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

Département d'Automatique, Télécommunication et d'Electronique

Projet de Fin d'Etudes

Pour l'obtention du diplôme de Master

Filière : Télécommunications

Spécialité : Réseaux et télécommunications

Thème

Mise en œuvre d'une solution de haute disponibilité (HSRP) pour un réseau local : cas pratique réseau LAN de CEVITAL agro-industrie.

Préparé par :

- Mlle Sendjakedine Ahlame
- Mlle Tissoukai Lydia

Dirigé par :

Mme GHERBI Meriem

Mr SLIMANI Mennad

Examiné par :

Mr BESSAAD Omar

Mme OUALI Kahina (P)

Année universitaire : **2023/2024**

Dédicaces

C'est avec un immense bonheur, un cœur débordant d'affection et une joie indescriptible que je consacre ce travail humble mais significatif :

À **mes parents** bien-aimés, et plus particulièrement à ma très chère **maman**, dont la patience, l'amour, le soutien et les sacrifices ont été le pilier de mes études. Aucun hommage ne saurait égaler l'amour incommensurable qu'ils me prodiguent sans cesse. Que Dieu leur accorde une santé robuste et une vie longue et prospère.

À mes frères adorés, **Akli** et **Walid**, dont l'amour et la compréhension ont été une source constante d'inspiration. Ils ont toujours été des modèles exemplaires pour moi.

À ma sœur chérie **Meriem**, une présence douce et constante dans ma vie, à son mari **Kamel** dévoué qui est pour moi comme un frère, et à mon neveu **Atmane**, une source inépuisable de joie et de bonheur, vous occupez tous une place irremplaçable dans mon cœur.

À l'ensemble de ma famille, dont le soutien inébranlable a été un phare tout au long de mon voyage d'études. Merci d'être toujours là pour moi.

À ma précieuse binôme et meilleure amie **Lydia** sa loyauté et son amitié ont été une source d'inspiration et de force tout au long de ce parcours. Son soutien indéfectible et sa présence constante ont été un pilier de ma vie, ainsi qu'à sa famille.

À tous mes amis, qui ont enrichi ma vie de manière inestimable.

Et à tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce travail. Leur aide a été précieuse et je leur en suis profondément reconnaissante.

S.Ahlame

C'est avec un immense bonheur, un cœur débordant d'affection et une joie indescriptible que je consacre ce travail humble mais significatif :

À ma famille aimante et inspirante, à **mes parents**, mes frères **Ahcene, Amine** et **Islam**, ainsi qu'à ma sœur **Kenza**, vous êtes mes piliers et ma source de soutien inconditionnel. Votre amour et votre encouragement ont été les fondations de mon parcours académique, et je vous suis infiniment reconnaissante pour cela.

À ma chère cousine **Baya**, tu es comme une sœur pour moi, et ta présence constante a apporté de la joie.

À mon grand-père Nadir, mes oncles **Nadjim** et **A.Kader**, et **mes tantes**, vous avez toujours été là pour moi, m'encourageant à poursuivre mes rêves et me prodiguant des conseils précieux. Je vous suis reconnaissante pour votre amour et votre soutien inconditionnels.

À la mémoire de mon oncle bien-aimé, **Azzeddine**, dont la présence aimante et le soutien inébranlable continuent de m'inspirer même en son absence.

À ma précieuse binôme, **Ahlame**, notre collaboration a été une expérience enrichissante tout au long de ce projet. Ta perspicacité et ton dévouement m'ont inspirée et je suis fière de ce que nous avons accompli ensemble.

À mes chères amies **Yasmine**, **Roza, Kenza et Wafa**, vous avez été mes compagnons de route pendant ces années d'études. Votre amitié sincère et votre soutien indéfectible ont rendu ce parcours encore plus mémorable.

À tous mes amis, vous avez été présents à mes côtés, partageant les hauts et les bas de ce voyage académique.

Et à tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce travail. Leur aide a été précieuse et je leur en suis profondément reconnaissante.

T.Lydia

Remerciements

Un grand merci à Dieu pour nous avoir guidés et inspirés tout au long de ce projet.

Nous tenons à exprimer notre profonde gratitude aux personnes qui ont contribué à son aboutissement et qui nous ont soutenus tout au long de notre parcours.

Tout d'abord, nous remercions chaleureusement notre encadrante Mme M.GHERBI, pour sa confiance, ses précieux conseils et son suivi rigoureux tout au long de l'élaboration de ce mémoire. Sa disponibilité et ses encouragements ont été d'une grande importance pour nous.

Nous exprimons notre sincère gratitude envers le groupe CEVITAL, notamment envers Mr M.SLIMANI et Mr Y.ARAB, pour leur accueil chaleureux et leur soutien pendant notre stage. Leur bienveillance nous a permis de mettre en pratique nos compétences dans un environnement professionnel stimulant, enrichissant ainsi notre expérience.

Nous sommes également reconnaissants envers les membres du jury Mr O.BESSAAD et Mme K.OUALI, pour l'honneur qu'ils nous font en acceptant d'évaluer notre travail. Nous apprécions leur expertise et leur regard critique, qui nous permettront d'améliorer notre mémoire.

Nous tenons également à remercier tous les enseignants qui nous ont transmis leur savoir et qui nous ont accompagnés tout au long de notre formation. Leurs cours et leurs conseils ont été essentiels pour notre développement personnel et professionnel.

Un grand merci à nos familles et à nos amis pour leur soutien indéfectible, leur encouragement et leur patience tout au long de nos études.

Enfin, nous remercions toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce mémoire. Nous sommes conscients que ce travail n'aurait pas pu être accompli sans votre aide et votre soutien.

Nous vous remercions tous du fond du cœur.

Lydia & Ahlame

Table des matières

Chapitre II : Étude de l'existant

Chapitre III : La haute disponibilité d'un réseau LAN

Chapitre IV : Conception et Réalisation

La liste des figures

La liste des tableaux

Liste des abréviations

ACL : **A**ccess **C**ontrol **L**ist

ARP : **A**ddress **R**esolution **P**rotocol

BPDU : **B**ridge **P**rotocol **D**ata **U**nit

CSMA/CD : **C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **D**etection

DHCP : **D**ynamic **H**ost **C**onfiguration **P**rotocol

DMZ : **D**emilitarized **Z**one

DSI : **D**irection des **S**ystèmes d'**I**nformation

FHRP : **F**irst **H**op **R**edundancy **P**rotocol

GLBP : **G**ateway **L**oad **B**alancing **P**rotocol

HSRP : Hot **S**tandby **R**outer **P**rotocol

ICMP : **I**nternet **C**ontrol **M**essage **P**rotocol

IP : **I**nternet **P**rotocol

ISO : **I**nternational **O**rganization for **S**tandardization

LACP : **L**ink **A**ggregation **C**ontrol **P**rotocol

LAN : **L**ocal **A**rea **N**etwork

MAC : **M**edia **A**ccess **C**ontrol

MAN : **M**etropolitan **A**rea **N**etwork

MSTP : **M**ultiple **S**panning **T**ree **P**rotocol

OSI : **O**pen **S**ystems **I**nterconnection

OSPF : **O**pen **S**hortest **P**ath **F**irst

PAGP : **P**ort **A**ggregation **P**rotocol

PAN : **P**ersonal **A**rea **N**etwork

RPO : **R**ecovery **P**oint **O**bjective

RSTP : **R**apid **S**panning **T**ree **P**rotocol

RTO : **R**ecovery **T**ime **O**bjective

STP : **S**panning-**T**ree **P**rotocol

TCP : **T**ransmission **C**ontrol **P**rotocol

VLAN : **V**irtual **L**ocal **A**rea **N**etwork

VRRP : **V**irtual **R**outer **R**edundancy **P**rotocol

VTP : **V**LAN **T**runking **P**rotocol

WAN : **W**ide **A**rea **N**etwork

WiFi : **W**ireless **F**idelity

Introduction Générale

Dans un monde de plus en plus connecté, les réseaux informatiques jouent un rôle crucial au sein des entreprises et des organisations**.** Ces réseaux, qui servent de base à la communication et à l'échange d'informations, doivent être conçus et gérés de manière efficace pour répondre aux exigences croissantes en termes de performance et de disponibilité.

Ce projet de fin d'études s'articule autour de la mise en œuvre d'une solution de haute disponibilité (HSRP) pour un réseau local, visant à assurer la continuité du fonctionnement du réseau et à minimiser les temps d'arrêt en cas de pannes matérielles. L'étude s'appuie sur le cas concret de Cevital Agro-industrie, une entreprise majeure opérant dans divers secteurs en Algérie.

L'implantation d'une redondance matérielle aux couches cœur et distribution, couplée à l'utilisation du protocole HSRP, offre une solution efficace pour basculer rapidement vers un équipement de secours en cas de défaillance, réduisant ainsi les interruptions de service et préservant la productivité de l'entreprise.

Pour atteindre cet objectif, ce mémoire se compose de quatre chapitres distincts :

Le premier chapitre pose les bases théoriques en abordant les principes fondamentaux des réseaux informatiques : les architectures réseau, les différents types de réseaux, les protocoles de communication, les modèles OSI et TCP/IP, ainsi que l'adressage IP. Cette section fournit le socle de connaissances nécessaire à la compréhension des chapitres suivants.

Le deuxième chapitre se concentrera sur une étude de cas spécifique: le réseau de Cevital Agro-industrie. Nous examinerons l'infrastructure réseau existante de l'entreprise, ses composants, son architecture et ses caractéristiques. Cette analyse approfondie nous permettra de comprendre les défis et les exigences spécifiques auxquels est confrontée l'entreprise en matière de connectivité et de continuité des services.

Le troisième chapitre portera sur un aspect essentiel des réseaux informatiques : la haute disponibilité. Nous explorerons les stratégies et technologies permettant d'assurer la continuité des réseaux locaux (LAN), en utilisant une combinaison de protocoles tels que STP, HSRP et OSPF. Notre choix du HSRP comme protocole principal reflète notre engagement à maintenir

les services critiques de l'entreprise. Nous analyserons également les avantages et le fonctionnement de ces protocoles.

Enfin, le quatrième chapitre se concentrera sur la conception et la réalisation d'une solution de haute disponibilité pour le réseau LAN de Cevital. Nous présenterons les étapes de conception, ainsi que les configurations et les tests nécessaires pour mettre en œuvre efficacement cette solution. L'objectif principal sera d'assurer la continuité des opérations réseau de Cevital en fournissant une architecture résiliente capable de répondre rapidement aux pannes et de minimiser les interruptions de service.

En conclusion, ce projet de fin d'études vise à fournir une analyse approfondie des réseaux informatiques, en mettant en évidence l'importance de la haute disponibilité pour assurer le bon fonctionnement des entreprises modernes.

Chapitre I
Généralités sur les réseaux informatiques

I.1 Introduction

Pour réussir notre étude sur la haute disponibilité des réseaux locaux, il est indispensable de comprendre les principes fondamentaux des réseaux informatiques. Ce chapitre a pour objectif de présenter les concepts théoriques essentiels des réseaux informatiques afin de faciliter leur compréhension. Nous y aborderons toutes les notions nécessaires pour acquérir une connaissance approfondie de leur fonctionnement.

I.2 Définition d'un réseau informatique

Un réseau informatique est un regroupement d'appareils interconnectés permettant l'échange d'informations. Il peut inclure des ordinateurs, commutateurs et routeurs, facilitant ainsi la communication entre les divers nœuds du réseau. Ces réseaux sont catégorisés selon leur taille, topologie et architecture, afin de répondre aux besoins spécifiques de chaque utilisateur [1].

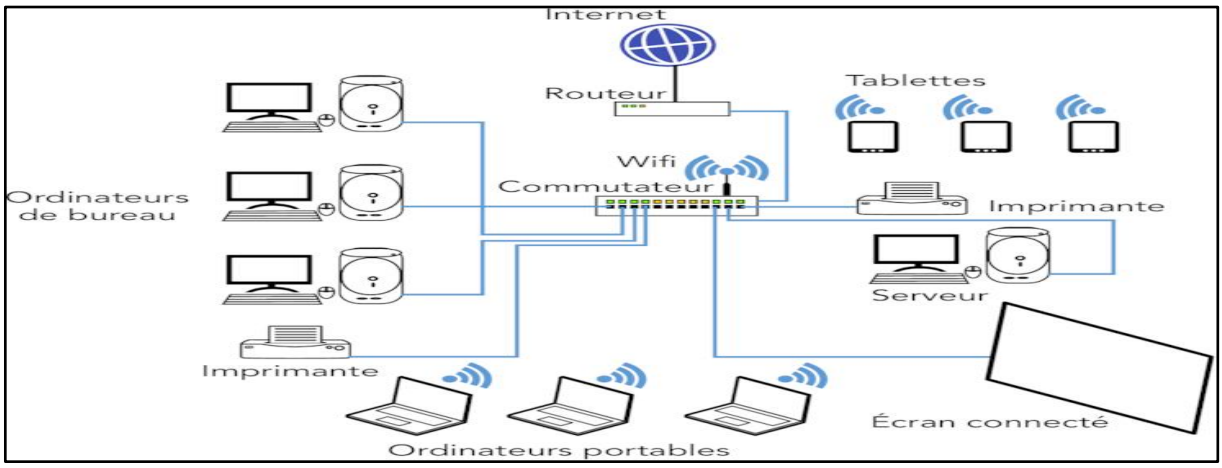


Figure I.1 : Organisation d'un réseau informatique [F1].

I.3 Classification des réseaux informatiques

Les réseaux informatiques peuvent être classés selon plusieurs critères :

I.3.1 Classification selon leur taille

On distingue quatre catégories de réseaux informatiques selon leur taille (nombre de machines et leur portée) :

a. Réseau personnel (PAN)

Un réseau PAN **(**Personal Area Network) est un réseau personnel de courte portée qui connecte des appareils personnels tels que des smartphones ou des ordinateurs portables dans un rayon de dizaine de mètres [2].

b. Réseau local (LAN)

Un réseau LAN (Local Area Network) désigne un réseau informatique limité géographiquement, généralement au sein d'un site d'entreprise. Il facilite l'interconnexion de tous les terminaux au sein de l'entreprise, assurant un débit élevé afin de favoriser des communications rapides entre les différents équipements [1].

c. Réseau métropolitain (MAN)

Un réseau MAN (Metropolitan Area Network**)** est un réseau informatique à large bande qui relie plusieurs LAN géographiquement à proximité. Les réseaux MAN sont souvent utilisés pour connecter plusieurs sites d'une même entreprise ou organisation situés dans une zone géographique relativement concentrée [2].

d. Réseau étendu (WAN)

Un réseau WAN (Wide Area Network) est un réseau informatique qui s'étend sur une grande distance géographique, couvrant souvent des zones nationales ou internationales, et permet la communication entre des sites distants situés dans différentes villes, régions ou pays [1].

I.3.2 Classification selon l'architecture des réseaux

On distingue deux types d'architectures de réseaux :

a. Réseau client/serveur

Ce modèle représente une architecture réseau où les clients et les serveurs communiquent entre eux via un protocole réseau. Le protocole définit les règles et les formats d'échange de données [3].

- Les clients : ces dispositifs informatiques sollicitent des services et des ressources à partir d'autres ordinateurs connectés au réseau.
- Les serveurs : ces machines dédiées à la fourniture de services et de ressources aux clients, répondent à leurs demandes et leur permettent d'accéder à diverses fonctionnalités et données.

b. Réseau poste à poste (peer to peer)

Le réseau poste à poste est un modèle d'architecture réseau dans lequel chaque ordinateur est à la fois client et serveur, il offre une solution simple et économique pour partager des ressources entre ordinateurs [3].

c. Comparaison entre les deux architectures

Chacun de ces modèles présentes des caractéristiques et des avantages distincts qui les rendent adaptés à des applications et des environnements spécifiques :

	Client-serveur	Peer to Peer
Définition	Un serveur spécifique est connecté à des clients spécifiques	Le client et le serveur effectuent des tâches distinctes. Chaque nœud agit en tant que client et serveur
Service	Le client sollicite le service et le serveur le fournit	Chaque nœud peut demander des services et peut également en fournir
La stabilité	plus stable et évolutif	Souffre si le nombre de pairs augmente dans le système
Le coût	Client-serveur est coûteux à implémenter	Sont moins chers à mettre en œuvre
côté serveur	Lorsque plusieurs clients demandent les services simultanément, un serveur peut être encombré	Comme les services sont fournis par plusieurs serveurs répartis dans le système Peer to Peer, un serveur n'est pas encombré
Les données	Les données sont stockées dans un serveur centralisé	Chaque pair a ses propres données

Tableau I.1 : Comparaison entre les deux architectures.

I.3.3 Classification selon leur topologie

La topologie des réseaux informatiques est essentielle pour comprendre leur structure et leur fonctionnement. Elle décrit la manière dont les appareils (ordinateurs, routeurs, etc.) sont interconnectés au sein d'un réseau. Voici les principales topologies de réseaux :

I.3.3.1 La topologie physique

La topologie physique d'un réseau informatique détermine la manière dont les données circulent entre les différents périphériques [4].

Nous avons cinq types de topologies (voir la figure I.2) :

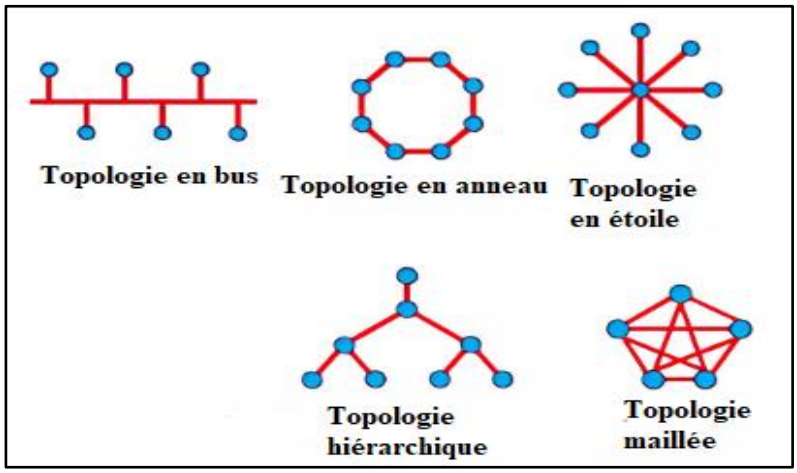


Figure I.2 : Les différentes topologies physiques [F2].

a. La topologie en bus

Un réseau en bus est une architecture réseau simple et économique où tous les ordinateurs sont connectés à un câble unique, appelé "bus". Ce câble central agit comme un canal de communication partagé, permettant aux ordinateurs d'échanger des données entre eux.

b. La topologie en anneau

Dans un réseau à topologie en anneau, les ordinateurs sont effectivement disposés en boucle fermée. La communication se déroule de manière ordonnée, chaque ordinateur ayant son tour pour transmettre des données.

c. La topologie en étoile

Dans une topologie en étoile, tous les ordinateurs sont connectés à un point central, appelé "switch". Ce point central est responsable de la communication entre les différents ordinateurs du réseau. Cependant, si le hub ou le switch venait à tomber en panne, le réseau tout entier ne pourrait plus communiquer.

d. La topologie en arbre

Dans La topologie en arbre, les périphériques sont organisés selon une hiérarchie, semblable à un arbre avec un nœud racine central. Ce dernier est relié à plusieurs niveaux de nœuds enfants, créant ainsi une structure hiérarchique bien définie.

e. La topologie maillée

La topologie en réseau maillé se caractérise par une interconnexion directe de tous les hôtes, sans hiérarchie centrale, formant ainsi une structure en forme de filet. Chaque nœud gère la réception, l'envoi et le relais des données, éliminant les points uniques de défaillance. En cas de panne d'un hôte, les données peuvent être acheminées par des chemins alternatifs via ses voisins :

- **Topologie maillée entièrement connectée** : tous les nœuds sont connectés les uns aux autres.
- **Topologie maillée partiellement connectée** : n'a pas tous les nœuds connectés les uns aux autres.

I.3.3.2 La topologie logique

La topologie logique décrit la manière dont les données circulent dans un réseau, en définissant les règles et les protocoles de communication. Elle est étroitement liée à la topologie physique [5].

a. Token Ring

Le protocole Token Ring est une technique de communication où les stations sont reliées en anneau physique et utilisent un jeton non adressé pour contrôler l'accès au réseau. Chaque station reçoit la trame de son prédécesseur et la transmet à son successeur, le jeton circulant de manière séquentielle dans un sens prédéfini [4].

b. Ethernet

Le protocole Ethernet, utilise une méthode d'accès appelée CSMA/CD (Carrier Sense Multiple Access with Collision Detection) où chaque appareil écoute le canal avant de communiquer. En cas de silence sur le réseau, l'appareil envoie ses données. Cependant, si plusieurs appareils tentent de transmettre simultanément, une collision se produit. Lorsqu'une collision se produit, chaque appareil concerné enregistre l'événement et attend temporairement avant de réessayer après un intervalle aléatoire. Bien que courantes, ces collisions ont un impact limité sur la vitesse de transfert [6].

I.4 Les équipements d'interconnexion

La mise en place d'un réseau nécessite l'utilisation de plusieurs équipements, dont la plupart sont des équipements d'interconnexion, chacun ayant un rôle spécifique à jouer [7].

I.4.1 Concentrateur

Le concentrateur est un appareil physique doté de plusieurs ports. C'est aussi un système de régénérateur du signal, son objectif est de connecter plusieurs ordinateurs entre eux. Il reçoit les données sur un port et les transmet à tous les autres ports.

I.4.2 Répéteur

Un répéteur est un dispositif utilisé pour amplifier le signal entre deux nœuds dans le but d'étendre la portée du réseau. Il est à noter qu'un répéteur peut être utilisé pour connecter deux types différents de supports de transmission.

I.4.3 Carte réseau

La carte réseau est l'interface physique entre l'ordinateur et le support de communication. Afin de mettre un ordinateur en réseau, il est nécessaire qu'il soit équipé d'une carte réseau.

I.4.4 Commutateur

Le commutateur (switch) est un équipement essentiel en réseaux et télécommunications. Il fonctionne au niveau 2 du modèle OSI. Il permet de connecter de manière efficace plusieurs équipements informatiques entre eux. Contrairement au hub, sa principale caractéristique est sa capacité à connaître l'adresse physique des machines connectées et à analyser les trames reçues pour les diriger vers la machine de destination.

I.4.5 Routeur

Un routeur est un élément essentiel d'un réseau informatique qui permet de relier plusieurs réseaux ou sous-réseaux**,** de gérer le trafic de données entre eux et assure le routage des paquets. Il fonctionne au niveau de la couche 3 du modèle OSI, la couche réseau.

I.4.6 Modem

Le modem ou le modulateur-démodulateur est un appareil permettant d'avoir accès à internet. En tant que communicant, le modem sert de relai entre le FAI**,** Fournisseur d'Accès à Internet et ses abonnés.

I.5 Les supports de transmissions

Les supports de transmission sont des moyens utilisés pour permettre la communication entre deux équipements informatiques. Il existe différents types de supports de transmission, notamment les câbles réseaux et les technologies sans fil [8].

I.5.1 Les câbles réseaux

Les câbles réseau sont des éléments essentiels pour la mise en place d'un réseau informatique performant et fiable, qu'il soit LAN ou WAN.

I.5.1.1 Câbles en cuivre

Un câble en cuivre est un dispositif utilisé pour transmettre de l'électricité ou des signaux de télécommunication. Il est composé de conducteurs en cuivre et peut prendre différentes formes selon les besoins de l'application.

a. Câble coaxial

Le câble coaxial est un type de câble utilisé principalement en télécommunications pour transmettre des signaux hauts fréquence. Il est composé d'un conducteur central entouré d'une gaine isolante et d'une tresse métallique pour la protection contre les interférences électromagnétiques.

b. Câble à paires torsadées

Les câbles à paires torsadées sont utilisés pour la transmission de signaux électriques ou de données. Ils sont composés de paires de fils conducteurs en cuivre torsadés ensemble pour réduire les interférences électromagnétiques.

I.5.1.2 Câble en fibre optique

Une fibre optique est un fil en verre ou en plastique très fin qui a la propriété de conduire la lumière et sert dans les transmissions terrestres et océaniques de données.

Les câbles en fibre optique se divisent en deux grands types selon le diamètre de leurs cœur et la longueur d'onde utilisé : les fibres multimodes et monomodes.

I.5.2 Les supports sans fils

Les supports sans fil transmettent des signaux ou des données via des ondes électromagnétiques, réduisant l'encombrement des câbles et offrant une plus grande liberté de mouvement.

Nous avons différents types de supports sans fils utilisés pour la transmission des données :

- **Infrarouge (IR) :** Utilisée pour les télécommandes et certains anciens protocoles de communication à courte portée.
- **Ondes radio :** utilisée pour les réseaux cellulaires tels que la 4G et la 5G et les réseaux sans fils (WIFI). Ils permettent la connectivité mobile et l'accès à Internet.

I.6 Modèle général de communication

On distingue deux modèles de communications, le modèle de référence OSI (Open System Interconnected) et le modèle TCP/IP (Transmission Control Protocol/Internet Protocol).

I.6.1 Le modèle OSI

Le modèle OSI est un modèle conceptuel qui définit sept couches pour la communication entre différents systèmes informatiques. Il a été normalisé en 1984 par l'ISO (Organisation internationale de normalisation) [9].

Chaque couche du modèle OSI a des fonctions spécifiques et est responsable de différents aspects de la communication entre les systèmes.

Modèle OSI	
Couche	Rôle
7-Application	Point d'accès aux services réseau
6-Présentation	Gère le chiffrement et le déchiffrement des données, convertit les données machine en données exploitables par n'importe quelle autre machine
5-Session	Communication Interhost, gère les sessions entre les différentes applications
4-Transport	Connexion de bout en bout, connectabilité et contrôle de flux ; notion de port (TCP et UDP)
3-Réseau	Détermine le parcours des données et l'adressage logique (adresse IP)
2-Liaison (link)	Adressage physique (adresse MAC)
1-physique	Transmission des signaux sous forme numérique ou analogique

Figure I.3 : les couches de modèle OSI [F3].

I.6.2 Le modèle TCP/IP

Le modèle TCP/IP est une approche pratique de la communication en réseau. Il est utilisé comme modèle de référence pour Internet. Contrairement au modèle OSI, le modèle TCP/IP ne comporte que quatre couches [10].

Le modèle TCP/IP tire son nom des deux protocoles majeurs qu'il utilise : TCP (Transmission Control Protocol) et IP (Internet Protocol). Ces protocoles sont responsables de la transmission des données sur Internet.

Voici les couches de modèle TCP/IP avec leurs rôles :

- **Couche Application** : Interface avec les applications utilisateur.
- **Couche Transport** : Assure la fiabilité de la communication.
- **Couche Internet** : Gère l'adressage et le routage des paquets.
- **Couche Accès au réseau** : Gère l'accès au support physique pour la transmission des données.

I.6.3 Comparaison entre le modèle OSI et le modèle TCP/IP

Les deux modèles OSI et TCP/IP ont des similitudes et des différences, notamment dans le nombre de couches et leur organisation, mais ils servent tous deux à normaliser les réseaux informatiques pour faciliter la communication entre les différents équipements et applications.

Voici une figure illustrant la différence entre le modèle OSI et le modèle TCP/IP :

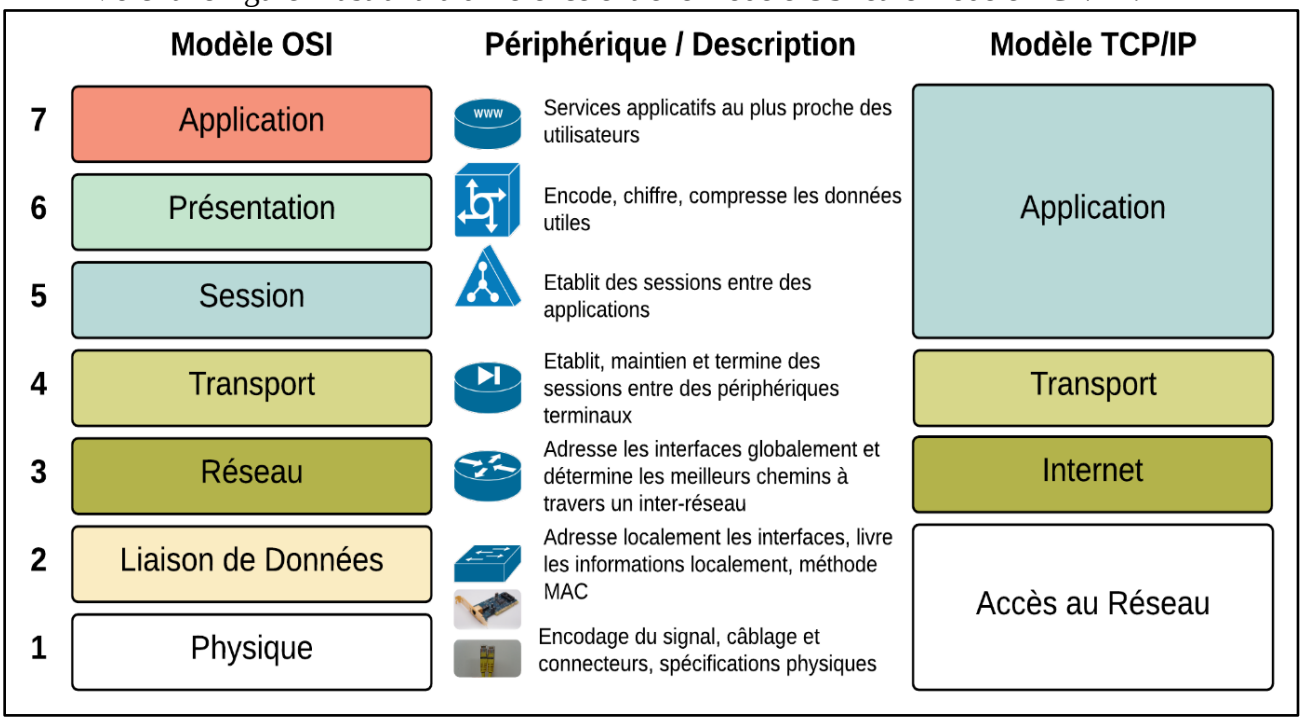


Figure I.4 : La différence entre les couches de modèle OSI - TCP/IP [F4].

I.7 Les protocoles réseaux

Les protocoles réseaux sont essentiels pour permettre la communication et le partage de ressources sur un réseau. Ils sont structurés en couches et utilisent différentes règles et conventions pour assurer une communication efficace entre les appareils [11].

I.7.1 Protocole IP

Le protocole IP (Internet Protocol) est un ensemble de règles régissant la communication entre les dispositifs sur un réseau IP. Il opère à la couche réseau du modèle OSI. Ce protocole est responsable de l'adressage, du routage et de la fragmentation des données en paquets afin d'assurer une transmission efficace. Toutefois, le protocole IP ne garantit pas que les paquets atteignent leur destination finale, car il ne dispose pas de mécanismes intégrés de vérification ou de correction des erreurs [12].

I.7.2 Protocole ICMP

Le protocole ICMP (Internet Control Message Protocol) est un protocole de la couche réseau du modèle OSI qui permet l'échange d'informations d'état et de messages d'erreur entre les nœuds des réseaux TCP/IP. Il est encapsulé dans les datagrammes du protocole IP et sert à informer les émetteurs des datagrammes en cas d'incident réseau.

De nombreux services réseau populaires, comme traceroute ou ping, reposent sur le protocole ICMP [12].

I.7.3 Protocole ARP

Le protocole ARP (Address Resolution Protocol) est un protocole de communication fonctionne entre la couche 2 (liaison de données) et la couche 3 (réseau) du modèle OSI.

Le protocole ARP est utilisé pour résoudre les adresses IP en adresses MAC dans un réseau local. Il permet aux appareils de communiquer en utilisant les adresses physiques (MAC) plutôt que les adresses logiques (IP), ce qui optimise l'utilisation de la bande passante [12].

I.7.4 Protocole DHCP

Le protocole DHCP (Dynamic Host Configuration Protocol) est un protocole réseau utilisé pour attribuer automatiquement des paramètres de configuration à des hôtes sur un réseau (l'adresse IP, masque sous réseau et la passerelle).

Le DHCP simplifie et automatise la configuration des paramètres réseau, ce qui permet une gestion efficace des adresses IP et réduit la charge administrative dans les réseaux informatiques.

I.7.5 Protocole VTP

Le VTP (VLAN Trunking Protocol**)** est un protocole propriétaire de Cisco utilisé pour synchroniser la configuration des VLANs sur les commutateurs d'un même domaine VTP [13]**.**

a. Architecture de VTP

Il existe plusieurs rôles que les commutateurs peuvent jouer. Voici les principaux rôles VTP :

- **Serveur VTP** : Le serveur VTP est le commutateur qui crée, modifie et supprime les VLANs. Il diffuse les informations sur les VLANs à tous les autres commutateurs dans le même domaine VTP. Les commutateurs en mode serveur peuvent également recevoir des mises à jour VTP des autres commutateurs.
- **Client VTP :** Les commutateurs en mode client VTP reçoivent les mises à jour VTP du serveur VTP, mais ils ne peuvent pas créer, modifier ou supprimer les VLANs. Toutes les modifications des VLANs doivent être effectuées sur le commutateur en mode serveur.
- **Transparent VTP :** Les commutateurs en mode transparent VTP ne participent pas activement à la gestion des VLANs. Ils ne créent pas, ne modifient pas et ne suppriment pas les VLANs. Cependant, ils transmettent les messages VTP qu'ils reçoivent sur leurs ports de trunking.

b. Fonctionnement de VTP

Le VTP fonctionne en désignant un commutateur en tant que serveur VTP, où les VLANs sont créés, modifiés ou supprimés. Les autres commutateurs sont des clients VTP qui se synchronisent automatiquement avec le serveur VTP, Cela facilite la configuration et la maintenance des VLANs dans un réseau de grande taille [13].

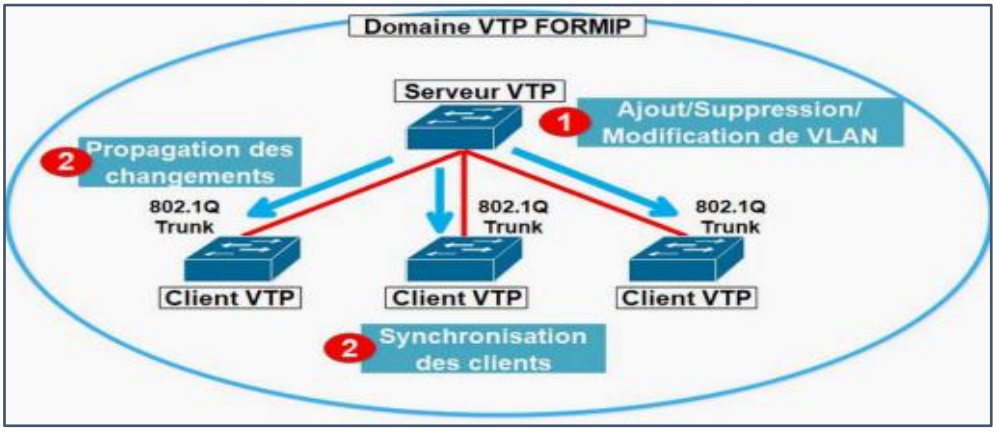


Figure I.5 : Fonctionnement de VTP [F5].

I.8 Un réseau local virtuel (VLAN)

I.8.1 Définition d'un VLAN

Un réseau local virtuel (VLAN) est un réseau logique qui fonctionne au niveau de la couche liaison de données du modèle OSI. Il permet la segmentation et l'isolation des appareils au sein d'un réseau local physique. Cela signifie que même s'ils sont physiquement répartis sur différents commutateurs réseau, ils peuvent appartenir au même VLAN et communiquer comme s'ils étaient sur le même réseau physique [14].

I.8.2 Agrégation de VLAN

L'agrégation de VLAN (trunking) est une technique utilisée dans les réseaux informatiques pour regrouper plusieurs VLANs sur un seul lien physique. Cette technique permet de transporter simultanément plusieurs VLANs sur un lien, ce qui facilite la gestion et l'optimisation du réseau.

I.8.3 Les avantages des VLANs

Les VLANs offrent de nombreux avantages, tels que :

- Les VLANs offrent une grande flexibilité pour la configuration et les modifications du réseau.
- Ils renforcent la sécurité en isolant les groupes d'utilisateurs.

- Ils réduisent la diffusion du trafic et améliorent la gestion des utilisateurs.
- Les VLANs permettent de créer des liens redondants pour améliorer la disponibilité du réseau en cas de panne d'un lien.
- Ils peuvent réduire les coûts en permettant de mutualiser des ressources physiques (câbles, commutateurs) entre plusieurs réseaux logiques.

I.9 L'adressage IP

L'adressage IP (Internet Protocol) joue un rôle crucial dans les réseaux informatiques en permettant l'identification unique de chaque appareil connecté à un réseau. Chaque appareil participant à un réseau informatique utilise une adresse IP, qui est un identifiant numérique attribué. Cette adresse IP est utilisée pour la communication en utilisant le protocole Internet (IP) et pour l'identification et l'adressage de localisation des appareils, et il existe différents types d'adresses IP, notamment les adresses IP publiques et les adresses IP locales [12].

I.9.1 Définition d'une adresse IPv4

Une adresse IPv4 est un identifiant unique attribué à un appareil connecté à un réseau utilisant le protocole Internet. Cette version d'IP, la plus couramment utilisée, se base sur des adresses de 32 bits. Elles sont formées de quatre nombres décimaux séparés par des points. Les adresses IPv4 permettent d'identifier et d'adresser les appareils sur les réseaux informatiques, en étant divisées en une partie réseau et une partie hôte pour distinguer le réseau et l'appareil spécifique [12].

I.9.2 Les classes d'adresse

Il existe plusieurs classes d'adresses IP. Elles sont citées dans le tableau suivant :

Classe	Bits de début	Première adresse	Dernière adresse	Masque de sous-réseau	Première adresse privée	Dernière adresse privée
A	0	0.0.0.0	127.255.255.255	255.0.0.0	10.0.0.0	10.255.255.255
B	10	128.0.0.0	191.255.255.255	255.255.0.0	172.16.0.0	172.31.255.255
C	110	192.0.0.0	223.255.255.255	255.255.255.0	192.168.0.0	192.168.22.255
D	1110	224.0.0.0	240.255.255.255			
E	1111	240.0.0.0	255.255.255.255			

Tableau I.2 : Les classes d'adresses IP et masque réseau.

I.9.3 Masque réseau

Le masque de réseau est utilisé pour séparer les parties réseau et hôte d'une adresse. L'adresse du réseau peut être obtenue en effectuant une opération logique ET bit à bit entre une adresse complète et le masque de réseau [11].

I.9.4 Masque générique

Le masque générique (wildcard), également connu sous le nom de masque inverse, est utilisé pour identifier un sous-réseau ou une plage d'adresses IP dans le contexte des listes de contrôle d'accès (ACL) et d'autres fonctionnalités réseau (protocole OSPF). Il est utilisé pour déterminer quelles parties d'une adresse IP doivent correspondre exactement et quelles parties peuvent être ignorées lors de la correspondance avec une règle de filtrage [12].

Quand on doit appliquer un masque inversé, il faut garder à l'esprit que :

- **Un bit avec une valeur de « 0 »** vérifie la correspondance de l'adresse.
- **Un bit avec une valeur de « 1 »** ignore la valeur correspondante de l'adresse.

I.9.5 Adresse de l'hôte

L'adresse d'hôte est une adresse que l'on distribue de manière manuelle ou automatique « DHCP » à un hôte sur un réseau afin qu'il puisse communiquer avec les autres hôtes du réseau ou ceux situant sur des réseaux distants.

Cette adresse doit être unique sur le réseau afin de ne pas avoir de conflit d'adresses avec les autres hôtes du réseau.

I.9.6 Adresse de diffusion

L'adresse de diffusion, ou adresse de broadcast, est une adresse IP spéciale permettant d'envoyer des informations à tous les appareils d'un réseau sans connaître leurs adresses individuelles. Chaque réseau a une adresse de diffusion réservée pour la diffusion à grande échelle. Cette adresse ne doit pas être attribuée à un appareil spécifique car elle est réservée à la diffusion uniquement [11].

I.9.7 Le choix d'une adresse IP

La sélection d'une adresse IP dépend principalement du contexte spécifique dans lequel elle sera utilisée [12].

- Pour une connexion locale : les adresses privées sont généralement utilisées, telles que les blocs 10.0.0.0/8, 172.16.0.0/12 et 192.168.0.0/16. Ces adresses ne sont pas directement accessibles depuis Internet, mais permettent aux appareils locaux de communiquer entre eux sur le même réseau local.
- Pour une connexion internet publique : une adresse IP publique est nécessaire pour qu'un ordinateur puisse se connecter à Internet. Il existe deux types principaux d'adresses IP publiques : statiques et dynamiques. Les fournisseurs d'accès à Internet attribuent souvent automatiquement des adresses IP dynamiques lorsque leurs clients se connectent à leurs services.

I.9.8 Les sous-réseaux

Les sous-réseaux sont utilisés pour diviser un réseau IP en segments plus petits, ce qui permet d'optimiser le trafic et d'améliorer l'efficacité de l'allocation des adresses IP. Chaque sous-réseau permet aux périphériques connectés de communiquer entre eux grâce à l'utilisation de routeurs. La taille du sous-réseau dépend des besoins de communication et de la technologie de réseau utilisée [12].

I.10 Conclusion

En maîtrisant les concepts fondamentaux des réseaux informatiques, nous sommes mieux équipés pour comprendre et analyser le réseau d'entreprise. Dans le prochain chapitre, nous allons présenter l'organisme d'accueil (Groupe CEVITAL).

Chapitre II
Étude de l'existant

II.1 Introduction

Dans ce chapitre, nous allons présenter l'entreprise CEVITAL, citer les différents départements qui la constituent et donnerons des informations utiles pour notre travail. Nous allons poser ainsi la problématique fondamentale sur laquelle repose notre projet.

II.2 Présentation de l'entreprise et de son historique

Figure II.1 : Logo Cevital [F6].

Cevital Agro-industrie est une filiale du groupe Cevital, faisant partie des entreprises algériennes qui ont émergé dès l'entrée de notre pays dans l'économie de marché. Fondée en 1998 par des fonds privés, elle est principalement détenue par M. ISSAD REBRAB et ses enfants. Le siège social de Cevital est situé à Garidi Kouba (Alger), tandis que le complexe étudié se trouve sur le nouveau quai de l'arrière-port de Bejaïa.

Cevital joue un rôle crucial dans la croissance du secteur agroalimentaire national. Grâce à ses prix compétitifs, son expertise, ses installations de production de pointe, son contrôle qualité rigoureux et son vaste réseau de distribution, elle propose des produits de premier ordre aux consommateurs et aux fabricants. En répondant aux demandes nationales, Cevital a transformé l'Algérie d'importateur en exportateur d'huiles, de margarines et de sucre. Leader de premier plan en Afrique et dans la région méditerranéenne, Cevital domine l'industrie du sucre et des huiles végétales. Ses produits d'exception sont distribués dans différents pays, notamment en Europe, au Maghreb, au Moyen-Orient et en Afrique de l'Ouest [15].

II.3 Situation géographique de Cevital

Cevital Agro-Industrie, le plus grand complexe privé en Algérie, est situé à Béjaïa, près du port et de la route nationale 26, à une distance avantageuse de 280 km d'Alger. Cette localisation stratégique facilite l'accès aux infrastructures clés telles que l'aéroport, le port et la zone industrielle d'Akbou, offrant ainsi à l'entreprise son propre quai privé. Outre ses installations à Béjaïa, le groupe possède des bureaux dans plusieurs autres villes algériennes. À

l'international, Cevital a étendu ses activités avec des bureaux et des installations dans divers pays, où ses filiales se concentrent principalement sur la distribution et la commercialisation des produits Cevital [15].

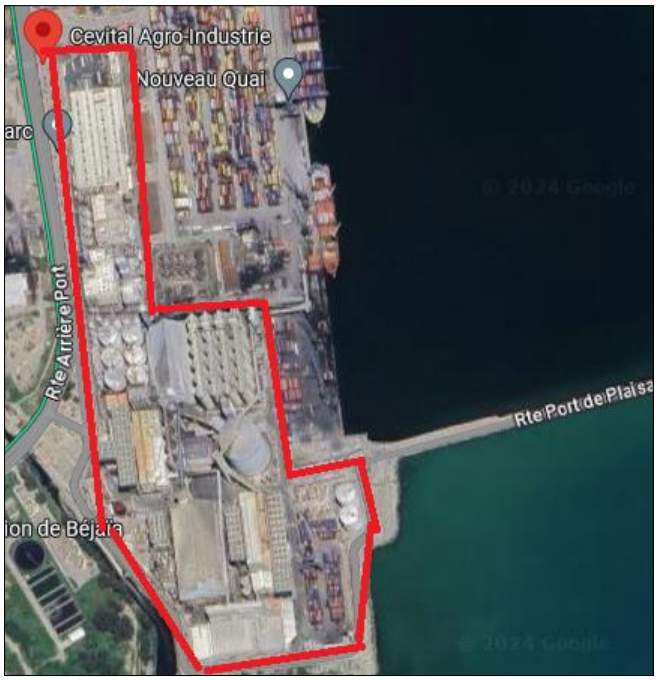


Figure II.2 : Vue satellitaire du Cevital Agro-Industrie [F7].

II.4 Organigramme de l'entreprise

L'entreprise géographique Cevital est composée de différentes directions, on cite [15] :

- **La direction des finances et de la comptabilité :** Cette direction a pour rôle de préparer et mettre à jour les budgets, de gérer la comptabilité, de préparer les états financiers et comptables, ainsi que de pratiquer le contrôle de gestion.

- **La direction commerciale :** cette direction est chargée de commercialiser l'ensemble des gammes de produits, de développer la base de clients de l'entreprise et de gérer la relation client.
- **La direction des ressources humaines :** la mission de cette direction est de fournir un soutien administratif à l'ensemble du personnel de CEVITAL, de superviser les activités sociales, d'apporter une assistance à la direction générale et à tous les responsables sur tous les aspects de la gestion des ressources humaines.

- **La direction industrielle :** cette direction est responsable du développement industriel des sites de production. En collaboration avec la direction générale, elle définit les objectifs et le budget de chaque site. Elle analyse les dysfonctionnements sur chaque site (équipements, organisations, etc.) et recherche des solutions techniques ou humaines pour améliorer en permanence la productivité, la qualité des produits et les conditions de travail. Elle anticipe également les besoins en équipements et supervise leurs achats.
- **La direction des systèmes d'information :** cette direction est responsable de la mise en place des outils et des technologies de l'information nécessaires pour soutenir et améliorer les activités, la stratégie et la performance de l'entreprise. Elle veille à la cohérence des moyens informatiques et de communication mis à la disposition des utilisateurs, à leur mise à niveau, à leur maîtrise technique, à leur disponibilité et à leur opérationnalité continue en toute sécurité.

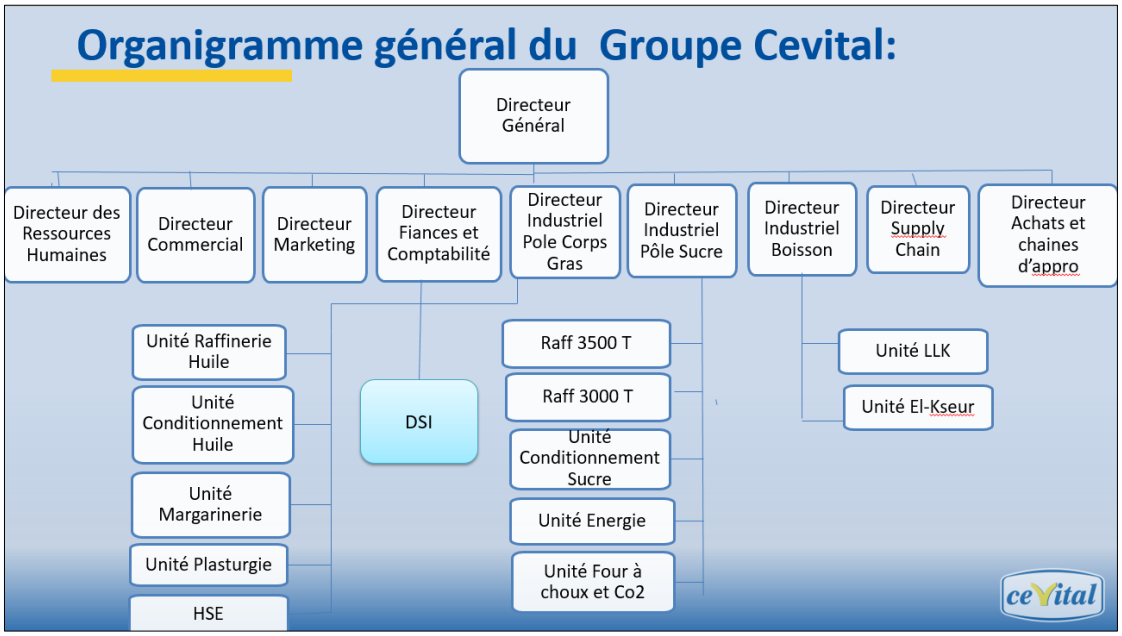


Figure II.3 : Organigramme général du Groupe Cevital [F8].

II.5 Valeurs du Groupe CEVITAL

Les quatre règles d'or (IRIS) à respecter sont les suivantes [15] :

- ✓ **Initiative :** Le collaborateur doit anticiper les problèmes potentiels et proposer des solutions innovantes grâce à sa connaissance du métier.

- ✓ **Respect :** Un principe primordial entre collaborateurs et avec les partenaires internes et externes.
- ✓ **Intégrité :** Une valeur fondamentale, les collaborateurs doivent adopter une éthique professionnelle irréprochable à travers leurs actions.
- ✓ **Solidarité :** Les collaborateurs doivent s'entraider mutuellement et partager leur expérience et leurs connaissances.

II.6 Présentation du service informatique

Le département Réseau et Télécom de la Direction des Systèmes d'Information (DSI) est une entité qui est chargée de mettre en œuvre les moyens et les technologies de l'information nécessaires pour améliorer l'activité, la stratégie et la performance de l'entreprise. Elle assure la cohérence des outils informatiques et de communication mis à la disposition des utilisateurs, garantissant leur maîtrise technique, leur disponibilité et leur opérationnalité continue, dans un environnement sécurisé [15].

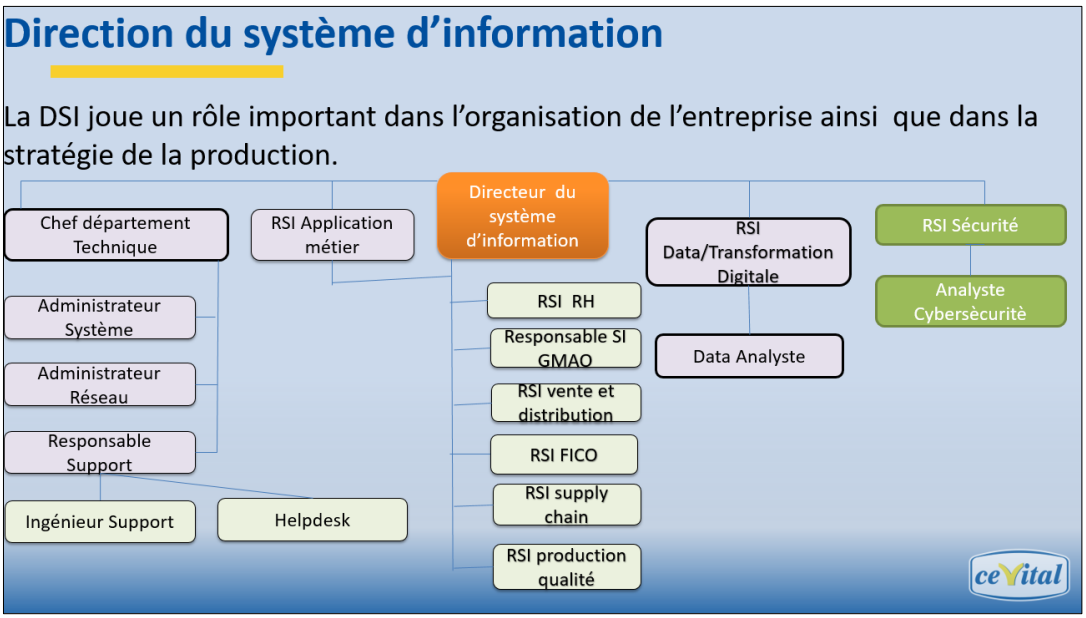


Figure II.4 : Direction du système d'information [F8].

Le département informatique est supervisé par des responsables spécialisés énumérés ci-dessous :

- ❖ **Directeur du système d'information :** Chargé de résoudre les problèmes de manière rentable et rapide, ce responsable choisit des solutions informatiques visant à améliorer la productivité de l'entreprise.

- **Administrateur réseau :** En charge de l'administration du réseau pour garantir une circulation optimale de l'information au sein de l'entreprise, ce professionnel veille à la qualité, à la continuité et aux performances des équipements et du réseau, tout en répondant aux besoins des utilisateurs.
- **Administrateur système :** Responsable de la conception, de l'installation et du bon fonctionnement de l'infrastructure informatique et du réseau de l'entreprise, il assure également la gestion et la maintenance des systèmes opérant sur le réseau.
- **Responsable support :** Assurant le contrôle à distance des postes, ce responsable fournit une assistance aux utilisateurs pour la prise en main de leur équipement et assure un support téléphonique interne.

II.7 Infrastructure de l'entreprise

CEVITAL Agro-industrie possède plusieurs unités de production ultramodernes, qui se présentent de la manière suivante [15] :

- Deux raffineries de sucre.
- Une unité de sucre liquide.
- Une raffinerie d'huile.
- Une margarinerie.
- Une unité de conditionnement d'eau minérale (située à Tizi-Ouzou).
- Une unité de fabrication et de conditionnement de boissons rafraîchissantes (site El-Kseur).
- Une conserverie.
- Des silos portuaires.

II.8 Architecture du réseau informatique de CEVITAL

Cevital bénéficie d'une infrastructure réseau interne étendue qui interconnecte les différents bâtiments, unités de production et directions du complexe. Cette infrastructure se décompose en plusieurs éléments : un backbone, un pare-feu, une zone démilitarisée (DMZ), une couverture WiFi, un routeur, des commutateurs (switches) et un centre de données (Datacenter) abritant les serveurs de l'entreprise.

Le réseau local du complexe est organisé en trois couches qui sont : la couche core (distribution), la couche d'accès et la couche en cascade.

- **La couche core (distribution) :** intègre un Switch Catalyst au data center, connecté au pare-feu, au routeur et aux Switchs d'accès pour garantir une connectivité rapide et fiable.
- **La couche d'accès :** est constituée de Switchs répartis sur les sites locaux, utilisant des VLANs pour gérer l'accès des utilisateurs par site.
- **La couche en cascade :** relie les Switchs entre eux et aux Switchs d'accès, permettant aux utilisateurs d'accéder aux services avec des VLANs dédiés à chaque département.

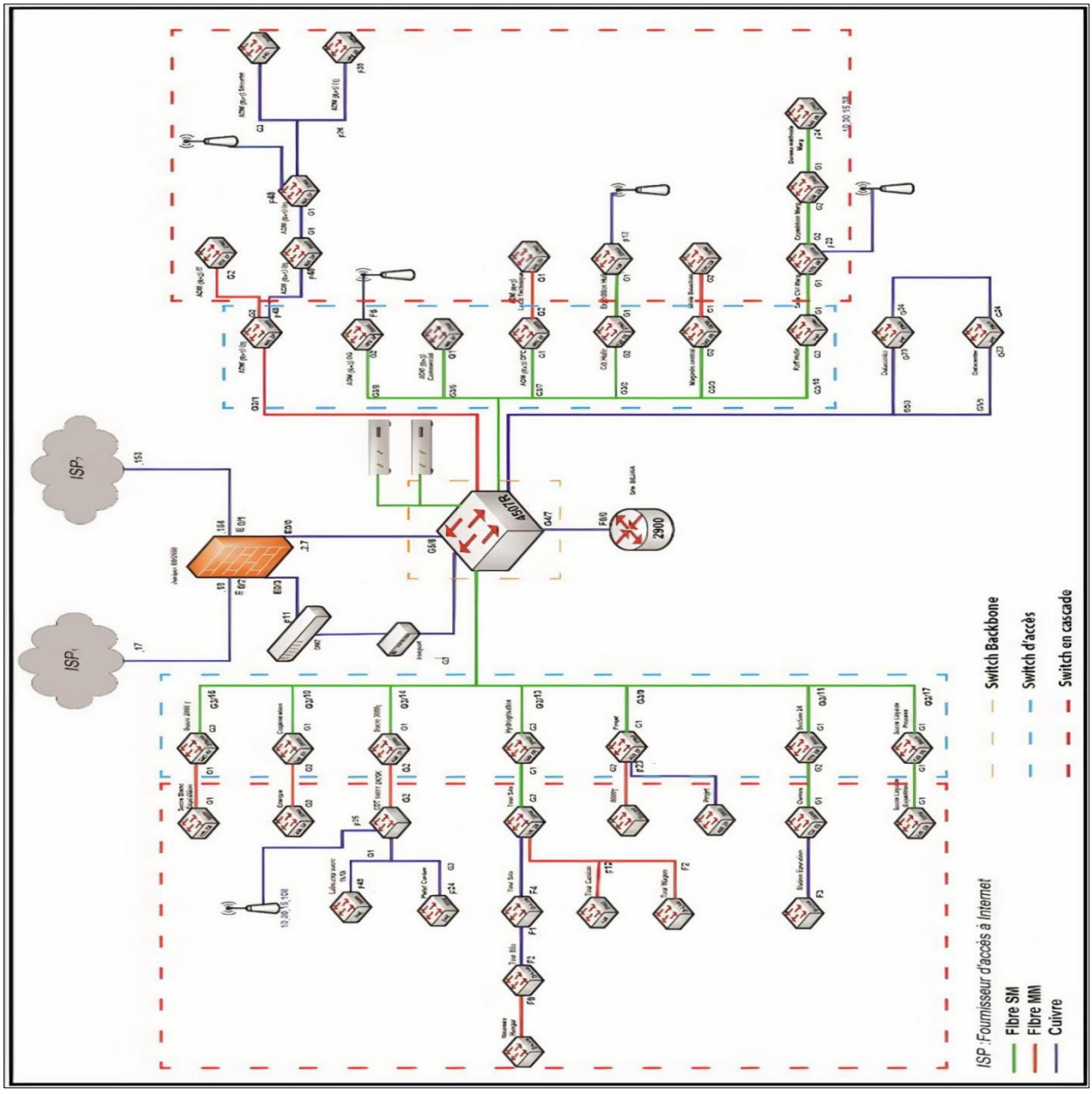


Figure II.5 : Architecture du réseau informatique du site Cevital-Bejaia [F8].

II.9 Matériel utilisé dans l'architecture existante

Le réseau est constitué de divers équipements, principalement des produits Cisco tels que les commutateurs Catalyst et le routeur, qui sont interconnectés via des liaisons en fibre optique ou en câble Ethernet torsadé [15].

- **Le Distributeur (Backbone) Cisco Catalyst 4507R**

C'est le pivot du réseau de CEVITAL, assurant la gestion du trafic de données crucial de l'entreprise. Il interconnecte les commutateurs d'accès, le pare-feu, les serveurs et les routeurs, jouant un rôle central dans le routage interVlan, l'accès Internet via le pare-feu et la fonction de serveur DHCP. Doté d'une architecture solide comprenant sept emplacements, ce commutateur peut accueillir divers moteurs de supervision et modules pour garantir une connectivité fiable et performante et une disponibilité optimale du réseau.

Figure II.6 : Switch Distributeur Cisco Catalyst 4507R [F9].

- **Routeur Cisco 2900**

Il facilite la gestion du routage entre les divers sites de l'entreprise.

Figure II.7 : Routeur Cisco 2900 [F10].

- **Switch d'accès, en cascade Cisco Catalyst 2960 et 2950**

Ils sont reliés au distributeur du réseau et déployés dans les divers secteurs de l'entreprise.

Figure II.8 : Switch d'accès Cisco Catalyst 2960 [F9].

- **Pare feu**

Le pare-feu est déployé pour garantir la sécurité du réseau, isoler des segments spécifiques, ainsi que surveiller et sécuriser l'accès à Internet.

Figure II.9 : Pare feu Fortinet [F11].

- **Point d'accès WIFI**

L'entreprise a mis en place plusieurs points d'accès Wi-Fi, établissant une connectivité sans fil dans des zones spécifiques du complexe pour assurer une couverture réseau étendue.

- **Le centre de données**

Le centre de données de CEVITAL est une zone sécurisée accessible uniquement aux responsables et techniciens de la DSI. Il dispose d'une climatisation et d'une alimentation électrique redondante pour garantir un fonctionnement continu. Ce centre héberge les serveurs, les Backbones, les pare-feu, les routeurs et le standard téléphonique de l'entreprise.

II.10 Codification des équipements de Cevital

- CEVWKS 1XXX : ordinateur de bureau
- CEVLAP 1XXX : ordinateur portable
- CEVSRV 1XXX : serveur
- CEVSWC 13XX : switch
- CEVAP 1XXX : point d'accès wifi
- CEVFW 1XXX : pare feu
- CEVRTR 1XXX : routeur.

II.11 Les VLANs de l'entreprise

Ci-dessous, un tableau détaillant les différents VLANs de l'entreprise, y compris leurs paramètres tels que le type de DHCP utilisé et les passerelles associées [15] :

Direction	VLAN	DHCP	Passerelle
DRH	VLAN10	Dynamique	10.30.10.254
Direction des Appro	VLAN11	Dynamique	10.30.11.254
DSI	VLAN12	Dynamique	10.30.12.254
Raff Huile	VLAN13	Dynamique	10.30.13.254
Raff sucre 3000T	VLAN14	Dynamique	10.30.14.254
Division utilités	VLAN15	Dynamique	10.30.15.254
Supply-chain	VLAN16	Dynamique	10.30.16.254
Unité margarinerie	VLAN17	Dynamique	10.30.17.254
Printer	VLAN18	Statique	10.30.18.254
Téléphone	VLAN20	Dynamique	10.30.20.254
Voice	VLAN21	Dynamique	10.30.21.254
Direction R&D	VLAN22	Dynamique	10.30.22.254
Performance industriel	VLAN23	Dynamique	10.30.23.254
Unité Cdt Huile	VLAN24	Dynamique	10.30.24.254
Management switch	VLAN 25	Statique	10.30.25.254
DFC	VLAN26	Dynamique	10.30.26.254
Commercial	VLAN27	Dynamique	10.30.27.254
Direction générale	VLAN28	Dynamique	10.30.28.254
Direction qualité et management système	VLAN29	Dynamique	10.30.29.254
Raff sucre 3500T	VLAN30	Dynamique	10.30.30.254
Cdt sucre	VLAN31	Dynamique	10.30.31.254
Caméra	VLAN32	Statique	10.30.32.254
Projets	VLAN33	Dynamique	10.30.33.254
Trituration	VLAN36	Dynamique	10.30.36.254

Tableau II.1 : Les VLANs de l'entreprise.

II.12 Liaison inter- sites (architecture WAN)

Afin d'assurer une communication fluide et un partage efficace des ressources, CEVITAL a établi des connexions entre son site de Bejaïa et plusieurs sites distants de l'entreprise, comprenant notamment [15] :

- Une liaison fibre optique point à point entre Bejaïa et Alger.
- Des liaisons par satellite (VSAT) entre Bejaïa et les sites d'El-Kseur (Cojek), Tizi-Ouzou (Lala Khadija) et El Kheroub (Constantine).

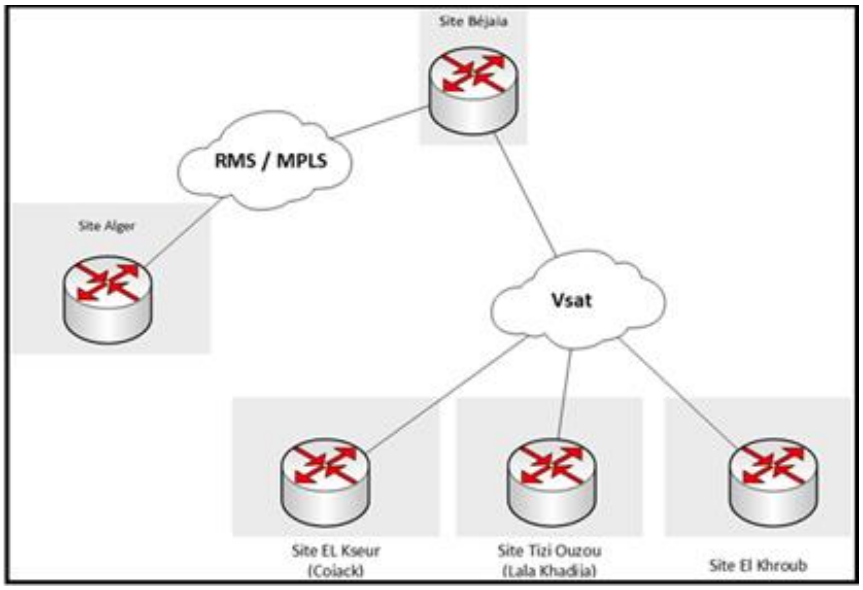


Figure II.10 : Schéma d'interconnexion réseaux WAN du Cevital [F8].

II.13 Critique de l'existant

Après une évaluation approfondie du réseau existant Cevital, plusieurs insuffisances ont été identifiées, mettant en évidence diverses contraintes fonctionnelles significatives. Le non-traitement adéquat de ces contraintes peut entraîner une détérioration des performances des réseaux existants et des interruptions fréquentes. Voici les constats résultants de notre étude par rapport au réseau existant :

- Utilisation d'un unique domaine de diffusion entraînant une surcharge du réseau.
- La liaison en cascade des switchs limite la bande passante du réseau, entraînant des ralentissements dans les applications et l'accès aux ressources.
- En cas de défaillance d'un switch connecté au switch principal, tous les utilisateurs connectés à ces switchs seront déconnectés du réseau.

II.14 Problématique

Dans le contexte des grandes entreprises telles que Cevital, la gestion et la maintenance des réseaux informatiques sont essentielles pour assurer la continuité des opérations et la productivité des employés. Les interruptions ou dysfonctionnements du réseau peuvent entraîner des perturbations majeures et compromettre les performances globales de l'entreprise. Dans ce contexte, une question essentielle mérite d'être posée :

Comment garantir une haute disponibilité du réseau local de Cevital afin d'assurer une continuité des services réseau et de minimiser les temps d'arrêt en cas de défaillance matérielle ?

II.15 Propositions

- Investir dans des équipements de pointe reconnus pour leur fiabilité et leurs performances optimales afin de répondre aux exigences croissantes du réseau.
- Implémenter une nouvelle topologie en arbre avec redondance matérielle au niveau des couches cœur et distribution pour assurer une disponibilité continue du réseau en cas de défaillance. Le protocole HSRP (Hot Standby Router Protocol) sera utilisé pour garantir une transition fluide vers les équipements de secours, préservant ainsi la continuité des services.
- Multiplier les liaisons d'interconnexion entre les périphériques afin de réduire l'impact de rupture de liaison.

II.16 Solution

Pour assurer la haute disponibilité du réseau local de Cevital, nous proposons de mettre en place une redondance matérielle dans les couches cœur et distribution, en utilisant le protocole HSRP pour garantir une disponibilité élevée en cas de défaillance matérielle.

En complément, l'intégration des protocoles STP (Spanning Tree Protocol) et OSPF (Open Shortest Path First) renforcera cette solution. STP préviendra les boucles de commutation en désactivant les liaisons redondantes inutiles, tout en maintenant des chemins de secours prêts à être activés, assurant ainsi la stabilité du réseau. OSPF fournira un routage dynamique et optimal, recalculant les routes en temps réel pour s'adapter aux changements du réseau et garantir que les données suivent toujours le chemin le plus efficace.

Cette combinaison de technologies minimisera les temps d'arrêt et améliorera la fiabilité globale du réseau, assurant une connectivité continue.

II.17 Conclusion

L'étude du réseau informatique actuel de Cevital à Béjaïa a permis d'évaluer son niveau de disponibilité élevée et de formuler des solutions tangibles pour renforcer cette capacité. La mise en œuvre de ces solutions visera à améliorer la disponibilité du réseau et à réduire les éventuels impacts des pannes sur les activités du groupe.

Chapitre III

La haute disponibilité d'un réseau LAN

III.1 Introduction

Après avoir exposé la structure de l'entreprise et les divers problèmes affectant leur réseau, nous allons définir, expliquer le fonctionnement et montrer comment garantir la haute disponibilité dans un réseau LAN d'une entreprise en utilisant les différents protocoles.

III.2 Définition de la haute disponibilité

La haute disponibilité d'un réseau LAN se réfère à la capacité d'un réseau informatique d'être toujours disponible et fonctionnel, 24/7. Cela implique la mise en place de mesures et de dispositions techniques pour garantir que l'infrastructure informatique reste opérationnelle.

La haute disponibilité est cruciale pour les entreprises, car un réseau fiable et disponible est essentiel à leur développement et leur fonctionnement. En cas d'indisponibilité, il y a des risques de pertes de productivité, de matériel, ainsi que des coûts supplémentaires liés aux pannes et aux ressources déployées [16].

III.3 Évaluation des risques

L'évaluation des risques d'un réseau LAN dans une entreprise est essentielle pour identifier les menaces potentielles et évaluer leur impact financier. Cela permet de prendre des mesures préventives et de planifier des mesures de continuité des activités en cas de dysfonctionnement [16]. Voici quelques-uns des risques courants :

- **Pannes matérielles :** Les défaillances des équipements réseau tels que les commutateurs, les routeurs ou les serveurs peuvent entraîner une interruption du réseau et une perte de connectivité pour les utilisateurs.
- **Problèmes de connectivité :** Les problèmes de connectivité, tels que les câbles endommagés ou les interférences électromagnétiques, peuvent entraîner des interruptions du réseau et une baisse de la productivité des utilisateurs.
- **Erreurs de configuration :** Des erreurs de configuration peuvent entraîner des problèmes de routage, des conflits d'adresses IP ou des incompatibilités entre les différents composants du réseau.
- **Surcharge du réseau** : Une évaluation des risques liés à la surcharge du réseau, tels que la congestion du trafic ou les problèmes de performances, s'avère nécessaire.
- **Environnement physique :** Des conditions telles que la température, l'humidité, et les risques d'incendie ou d'inondation peuvent affecter les équipements réseau, entraînant des pannes matérielles ou des dégradations de performance si elles ne sont pas correctement gérées.

III.4 Techniques améliorant la haute disponibilité

Il existe plusieurs techniques et technologies qui assurent la haute disponibilité des réseaux locaux tels que:

III.4.1 Redondance

La redondance consiste à avoir des composants en double pour assurer la disponibilité en cas de défaillance d'un élément [17].

- **La redondance matérielle :** Implique l'ajout d'un périphérique ou d'un composant en double dans le réseau. Cela intervient en cas de défaillance d'un périphérique ou d'un composant principal, dans le but de garantir un temps d'arrêt minimal.
- **La redondance réseau** : Consiste à dupliquer les chemins du réseau pour assurer une disponibilité continue en cas de panne. Cela signifie qu'il y a des équipements ou des liens de secours prêts à prendre le relais immédiatement si un élément du réseau tombe en panne, à l'aide de protocoles tels que STP et HSRP.

III.4.2 Répartition de charge

La répartition de charge est une technique utilisée pour distribuer de manière équilibrée les tâches de travail sur plusieurs serveurs ou ressources informatiques. Cela permet d'éviter la surcharge d'un composant du réseau et garantit une utilisation efficace des ressources disponibles [16].

III.4.3 Tolérance aux pannes

La tolérance aux pannes vise à maintenir la disponibilité constante d'un réseau malgré les défaillances matérielles ou logicielles. Elle détecte les erreurs, s'en remet rapidement et se rétablit sans intervention humaine. Elle repose sur des techniques telles que la redondance et le basculement automatique vers des composants de secours en cas de panne [16].

III.5 Critères de la haute disponibilité

- **Objectif de temps de reprise :** Le RTO (Recovery Time Objective) est le temps maximal acceptable pour lequel une ressource informatique peut être hors service après une interruption majeure de service, défini en fonction des besoins de production de l'entreprise [18].
- **Objectif de point de reprise :** Le RPO (Recovery Point Objective**)** définit la quantité maximale de données pouvant être perdue en cas d'incident [18].

III.6 Protocoles pour la redondance des liens

Diverses technologies et protocoles contribuent à la mise en place d'une infrastructure hautement disponible :

III.6.1 EtherChannel

EtherChannel est une technologie de liaison de ports qui permet de regrouper plusieurs liaisons physiques en une seule liaison logique pour obtenir un lien virtuel de meilleure capacité [19].

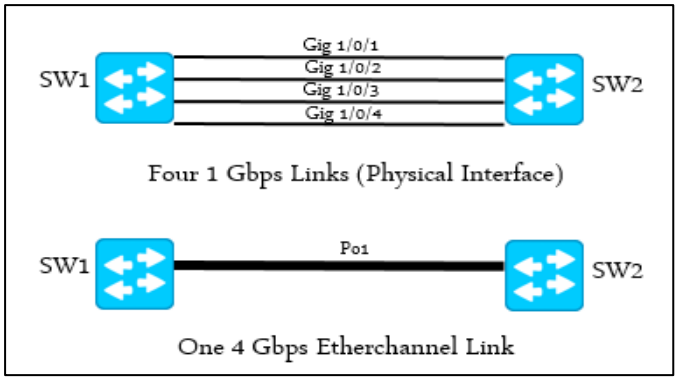


Figure III.1 : Illustration des performances d'EtherChannel [F12].

a. Protocoles d'agrégation de canaux

La négociation d'agrégation de liens est un élément crucial pour garantir une connectivité optimale et fiable. Deux protocoles dominent ce domaine [19] : PAGP (Port Aggregation Protocol) et LACP (Link Aggregation Control Protocol).

Les deux protocoles utilisent des mécanismes similaires pour négocier la création d'agrégations de liens. Ils définissent des modes de port qui déterminent le comportement du port dans le processus de négociation :

- **Actif (LACP) / Desirable (PAGP)** : Le port essaie activement de créer une agrégation de liens avec un port partenaire.
- **Passif (LACP)** / **Auto (PAGP)** : Le port attend qu'un port partenaire initie la création d'une agrégation de liens.
- PAgP et LACP ne peuvent pas fonctionner ensemble car ils sont incompatibles. Le mode "ON" crée un EtherChannel sans utiliser ces protocoles, mais nécessite une configuration cohérente de chaque côté. Sans configuration explicite, aucun EtherChannel n'est formé et les ports restent non agrégés.

b. Avantages d'EtherChannel

Voici les avantages d'EtherChannel :

- L'Etherchannel permet d'augmenter la bande passante disponible et il peut regrouper jusqu'à huit liens.
- La perte d'un lien n'impacte pas la connectivité grâce à la redondance d'EtherChannel.
- EtherChannel offre une redondance et une tolérance aux pannes améliorées.

III.6.2 Le protocole STP

Le protocole STP (Spanning-Tree Protocol) est un protocole de couche 2 utilisé dans les réseaux Ethernet pour garantir une topologie de réseau sans boucles en désactivant sélectivement les liens redondants [11].

Il existe différentes versions et variantes du STP, telles que le Rapid Spanning Tree Protocol (RSTP) et le Multiple Spanning Tree Protocol (MSTP)

a. Fonctionnement du STP

L'algorithme STP permet de créer une topologie logique sans boucle en désactivant les liens redondants et en ne laissant qu'un seul chemin actif entre les nœuds du réseau. Il utilise des messages BPDU (Bridge Protocol Data Unit) pour échanger des informations entre les commutateurs et détecter les boucles [20]. .

- **Élection du commutateur racine :** chaque commutateur annonce son identifiant de pont (Bridge ID), et celui avec le plus petit ID devient le commutateur racine, qui devient le point central du réseau.
- **Calcul des chemins les plus courts :** Chaque commutateur calcule le chemin le plus court vers le commutateur racine.
- **Désactivation des liens redondants :** Les liens redondants sont mis en état de blocage, sauf pour le chemin le plus court vers le commutateur racine.

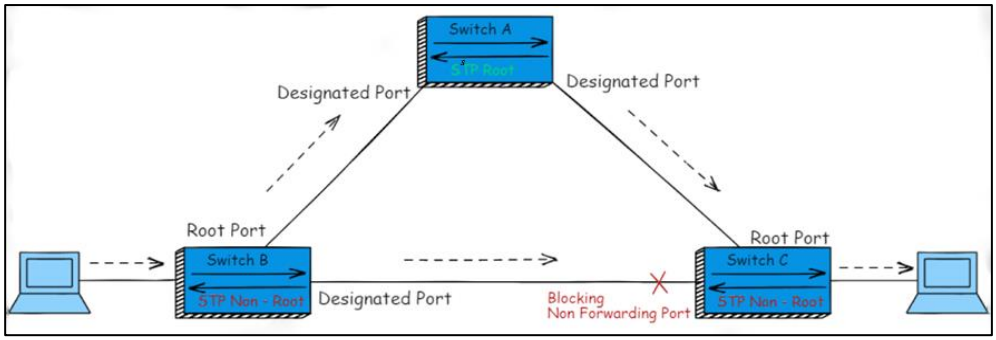


Figure III.2 : Exemple du concept du protocole STP [F13].

b. Les états des ports

Le protocole STP utilise différents états de port pour gérer la topologie du réseau et éviter les boucles de bouclage. Les principaux états de port sont [20]. :

- **Blocking (Bloqué) :** Le port n'est pas utilisé pour transmettre du trafic utilisateur, mais il écoute les messages BPDU pour surveiller la topologie du réseau.
- **Listening (Écoute) :** Le port commence à écouter les BPDU et prépare la transition vers l'état suivant.
- **Learning (Apprentissage) :** Le port commence à apprendre les adresses MAC des périphériques connectés.
- **Forwarding (Transfert) :** Le port est pleinement opérationnel et transfère le trafic utilisateur.

III.6.3 Protocole OSPF (Open Shortest Path First)

OSPF est un protocole de routage à état de liens (link-state) utilisé pour acheminer les paquets de données vers leur destination finale. OSPF est connu pour sa convergence rapide**,** sa fiabilité, sa **s**écurité et sa flexibilité, ce qui en fait un choix populaire pour les réseaux de toutes tailles [21].

a. Fonctionnement d'OSPF

Le OSPF fonctionne selon plusieurs points essentiels nous en citons :

- **Échange d'informations de routage :** Les routeurs OSPF partagent des informations détaillées sur la topologie du réseau entre eux, créant une base de données commune.
- **Calcul du meilleur chemin :** Chaque routeur utilise l'algorithme de Dijkstra pour calculer le chemin le plus court vers toutes les destinations possibles en se basant sur la base de données commune.
- **Tables de routage dynamiques :** Les routeurs OSPF peuplent leurs tables de routage avec les chemins les plus optimaux, garantissant un acheminement efficace des paquets.

b. Avantages d'OSPF

Voici quelques-uns de ses principaux avantages :

- Offrir une convergence rapide sans boucles et à chemins multiple.
- OSPF est adapté aux réseaux de grande taille grâce à sa structure hiérarchique et sa capacité à diviser le réseau en zones pour une gestion plus efficace.

- OSPF réagit rapidement aux changements de topologie du réseau, adaptant instantanément les tables de routage et garantissant une continuité de service.

III.7 Protocoles de mise en place de la haute disponibilité

Pour assurer une haute disponibilité dans un réseau, plusieurs protocoles sont utilisés. Parmi les protocoles couramment employés regroupés dans le groupe FHRP (First Hop Redundancy Protocol) se trouvent HSRP (Hot Standby Router Protocol), VRRP (Virtual Router Redundancy Protocol) et GLBP (Gateway Load Balancing Protocol) [22].

III.7.1 Protocole HSRP (Hot Standby Routing Protocol)

Le protocole HSRP est un protocole de redondance propriétaire de Cisco qui permet d'établir une passerelle par défaut tolérante aux pannes. Il peut être mis en place sur un routeur ou un switch de niveau 3 du modèle OSI. Il est un bon choix pour les réseaux Cisco qui n'ont pas besoin d'équilibrage de charge [23].

La taille du paquet HSRP varie en fonction de la version du protocole HSRP utilisée. En général, un paquet HSRP peut avoir une taille allant de 36 à 64 octets.

a. Fonctionnement de HSRP

Le HSPR fonctionne selon plusieurs points essentiels nous en citons [24] :

- Le HSRP permet à plusieurs routeurs de former un groupe HSRP, où un routeur est désigné comme routeur actif (active router) et les autres comme routeurs de secours (standby routers).
- Chaque routeur HSRP se voit attribuer une priorité, qui est un nombre compris entre 1 et 255.
- Le routeur avec la plus haute priorité devient le routeur actif. En cas d'égalité de priorité, le routeur avec l'adresse IP la plus élevée devient l'actif.
- Tous les routeurs du groupe HSRP partagent une adresse IP virtuelle et une adresse MAC virtuelle, qui agissent comme la passerelle par défaut pour les hôtes du réseau local.
- Le routeur actif est responsable de la transmission du trafic réseau, tandis que les routeurs de secours restent en attente et surveillent l'état du routeur actif.
- Les routeurs HSRP communiquent entre eux en envoyant des messages de type "hello" en multicast pour se tenir mutuellement informés de leur priorité et de leur état (actif ou de secours).

- Si le routeur actif devient inaccessible, l'un des routeurs de secours prend automatiquement le relais et devient le nouveau routeur actif, assurant ainsi une continuité de service sans interruption pour les hôtes du réseau.
- Le temps nécessaire pour qu'un routeur de secours prenne le relais en cas de défaillance du routeur actif, est généralement inférieur à 10 secondes. (Le Hold Timer est de 10 secondes, soit 3 * le Hello Timer + 1 seconde).

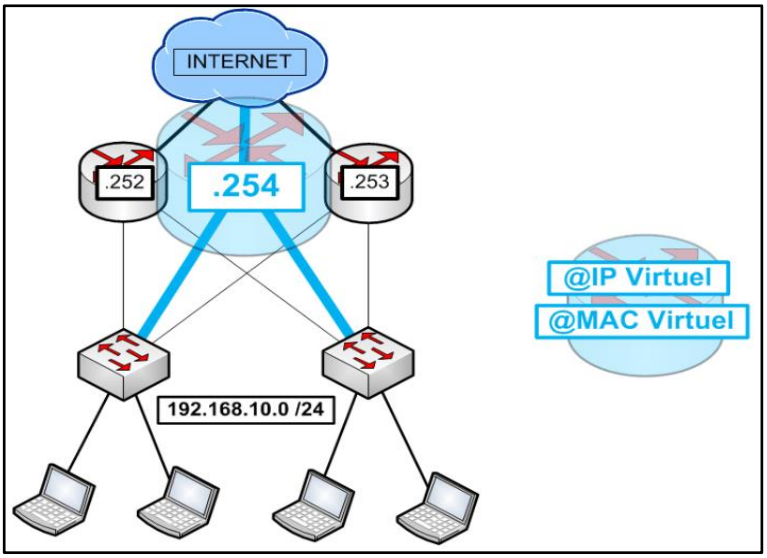


Figure III.3: Schéma physique ET virtuel d'un réseau HSRP [F14].

b. Les différents états d'un routeur HSRP

Après la configuration de HSRP, chaque routeur HSRP passera par plusieurs états avant de devenir un routeur actif ou de secours [25]. Voici le processus :

Initial	Cet état est atteint lorsqu'il y a un changement de configuration ou lorsqu'une interface devient disponible pour la première fois.
Learn	le routeur n'a pas encore appris son adresse IP virtuelle et n'a pas reçu de messages Hello du routeur actif. Le routeur est en attente d'un message du routeur actif.
Listen	Le routeur est en écoute des messages Hello du routeur actif pour déterminer son état au sein du groupe HSRP.
Speak	Le routeur envoie des messages Hello pour annoncer son état et sa priorité aux autres routeurs du groupe HSRP.
Standby	Le routeur est prêt à prendre le relais en cas de défaillance du routeur actif. Il reste en écoute des messages Hello du routeur actif.
Active	Le routeur est actuellement le routeur actif du groupe HSRP. Il est responsable de la distribution des paquets que les hôtes envoient à la passerelle virtuelle.

Tableau III.1 : Les différents états d'un routeur HSRP.

c. Étude de l'entête d'un paquet HSRP

L'analyse de la composition de l'en-tête d'un paquet HSRP est essentielle pour comprendre le fonctionnement du protocole HSRP [24].

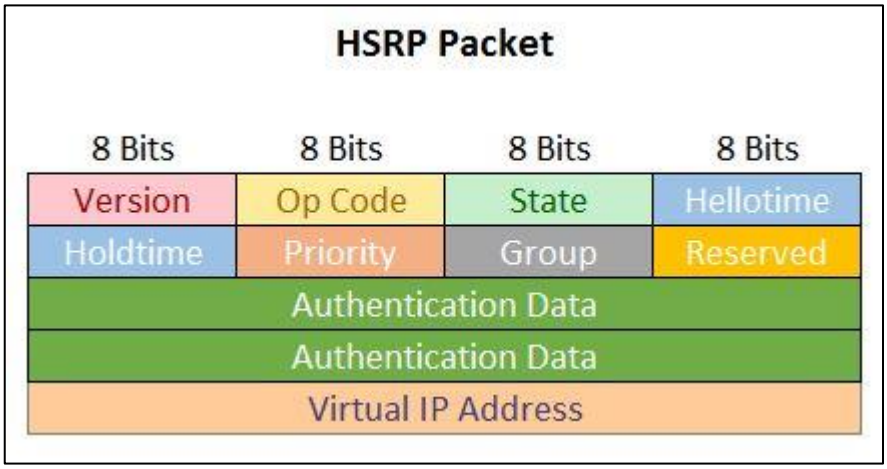


Figure III.4 : L'entête d'un paquet HSRP [F15].

L'en-tête d'un paquet HSRP contient plusieurs champs importants :

- **Version :** Indique la version du protocole HSRP utilisée.
- **Op Code :** Indique le type de message transmis par le paquet, trois types de messages distincts existent, chacun ayant une valeur et une signification propres:

  ➢ **0 - Hello :** Ce message est émis périodiquement par les routeurs Actif et Standby afin de maintenir la communication et de signaler leur présence au sein du groupe HSRP.

  ➢ **1 - Coup :** Ce message est envoyé par un routeur Standby qui souhaite prendre la relève en tant que routeur Actif. Il peut être déclenché par la détection d'une défaillance du routeur Actif ou par une décision manuelle de l'administrateur.

  ➢ **2 – Resign :** Ce message est transmis par un routeur Actif qui souhaite se décharger de ses responsabilités et céder la place à un autre routeur Standby.

- **State :** Indique l'état du routeur [voir le tableau III.1].
- **Hellotime :** Détermine l'intervalle de temps entre les messages Hello envoyés par les routeurs Actif et Standby.
- **Holdtime:** Définit le délai maximal après lequel un routeur est considéré comme inactif s'il n'a pas reçu de message Hello. Il doit être au moins trois fois supérieur à la valeur de Hellotime pour garantir une détection fiable des défaillances.
- **Priority :** Indique la priorité du routeur dans le groupe HSRP.

- **Group :** Indique le numéro du Standby Group, il permet de différencier plusieurs groupes HSRP coexistant sur le même réseau.
- **Authentication Data :** Contient des informations d'authentification pour garantir la sécurité du protocole HSRP.
- **Virtual IP Address :** Désigne l'adresse IP virtuelle attribuée au groupe HSRP.Cette adresse IP est utilisée par les clients pour accéder aux services du groupe, quelle que soit le routeur actif.

III.7.2 Protocole VRRP (Virtual Router Redundancy Protocol)

Le protocole VRRP est un protocole standard de l'industrie, ce qui signifie qu'il peut être utilisé avec des équipements de différents fabricants qui permet à plusieurs routeurs de travailler ensemble pour former un routeur virtuel. Le routeur virtuel créé par VRRP a une adresse IP virtuelle et une adresse MAC virtuelle, et il peut être utilisé comme passerelle par défaut pour les périphériques du réseau. VRRP ne prend pas en charge l'authentification, mais il peut hériter des valeurs de minuterie configurées sur le routeur maître [26].

III.7.3 Protocole GLBP (Gateway Load Blancing Protocol)

Le protocole GLBP est un protocole propriétaire Cisco utilisé pour créer une passerelle virtuelle haute disponibilité pour les routeurs redondants sur un réseau. Cela signifie qu'il permet de répartir le trafic sur plusieurs routeurs, améliorant ainsi les performances du réseau et sa tolérance aux pannes. Il ne répartit pas directement le trafic sur les routeurs comme des protocoles tels que HSRP ou VRRP [26].

III.8 Conclusion

Ce chapitre a présenté les divers outils utilisés pour garantir une haute disponibilité dans les réseaux locaux. Le chapitre suivant se concentrera sur la mise en œuvre d'une redondance matérielle au niveau des couches cœur et distribution.

Plus précisément, nous utiliserons les protocoles STP, HSRP et OSPF pour réaliser une redondance pratique sur l'architecture réseau LAN de Cevital.

Chapitre IV
Conception et Réalisation

IV.1 Introduction

Le réseau LAN de Cevital en pleine croissance doit répondre à des exigences de disponibilité et de performance élevées. La perte de connectivité, même brève, peut impacter la productivité et les opérations de l'entreprise**.**

Ce chapitre expose la conception et la mise en œuvre des solutions proposées pour notre projet visant à fournir un réseau hautement disponible pour Cevital. Nous avons appliqué les configurations nécessaires telles que les configurations des VLANs, VTP, STP, HSRP et OSPF en nous basant sur le simulateur Cisco Packet Tracer. Chaque étape sera détaillée, illustrée et accompagnée d'explications claires. La fiabilité de la solution sera ensuite testée pour valider son efficacité.

IV.2 Présentation du simulateur Cisco Packet Tracer 8.2.1

Cisco Packet Tracer est un simulateur de réseaux développé par Cisco Systems. Il offre un espace de test sécurisé nous permet d'expérimenter et de valider nos configurations sans aucun risque. Nous pouvons tester différentes configurations, étudier leur impact sur le réseau et résoudre des problèmes sans craindre d'interrompre un réseau réel [26].

Lors du lancement de Cisco Packet Tracer, l'interface suivante s'affiche, composée de plusieurs zones distinctes :

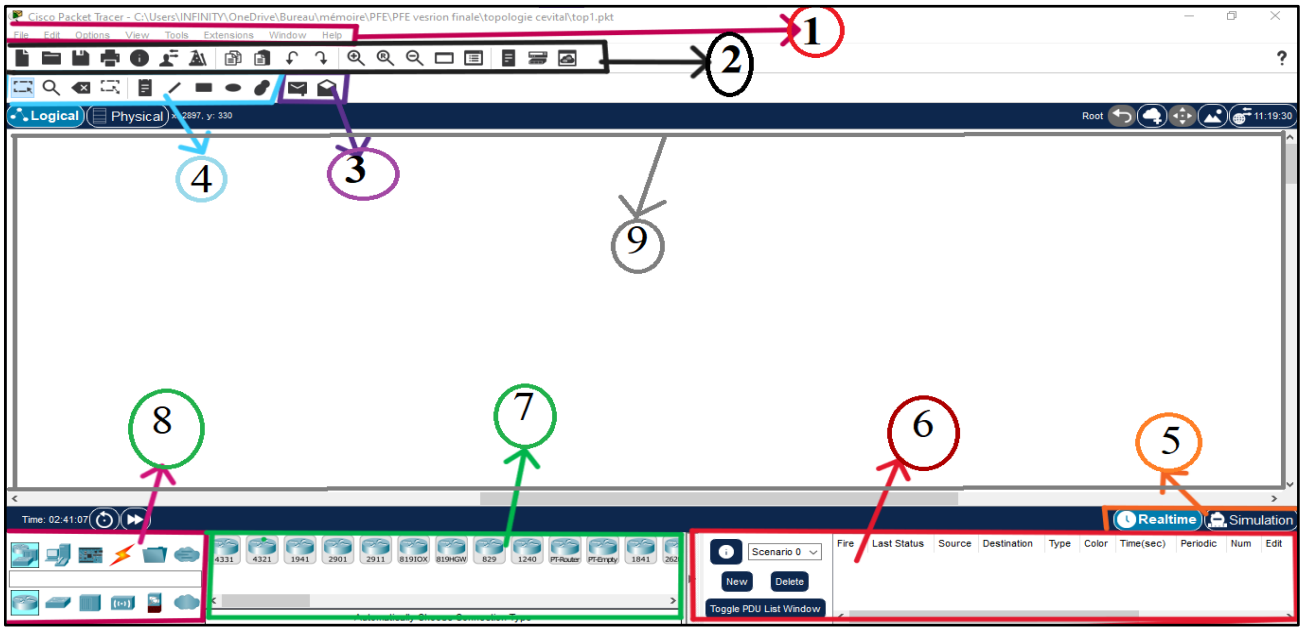


Figure IV.1 : Capture de l'interface Cisco Packet Tracer 8.2.1.

- **Zone 1 :** La barre de menu offre un accès aux fonctionnalités générales du logiciel, telles que la création de fichiers, l'édition de configurations et l'aide.
- **Zone 2 :** La barre d'outils principale regroupe des icônes pour les actions courantes, comme la création d'équipements, la simulation et la configuration.
- **Zone 3 :** L'espace de travail central est l'endroit où vous construisez votre réseau, visualisez les simulations et accédez à diverses informations et statistiques.
- **Zone 4 :** La barre d'outils secondaire contient des outils pour la sélection, le déplacement, l'édition et la suppression d'éléments, ainsi que pour l'inspection des équipements et la gestion des paquets.
- **Zone 5 :** Le panneau de configuration permet d'ajouter des annotations et de basculer entre les modes temps réel et simulation.
- **Zone 6 :** La zone de simulation affiche les détails des paquets transmis et reçus dans le réseau simulé.
- **Zone 7 :** Le panneau d'onglets présente les catégories d'équipements disponibles, facilitant la recherche et l'insertion d'éléments spécifiques dans votre réseau.
- **Zone 8 :** La zone de sélection d'équipement permet de choisir le type d'équipement à ajouter dans la catégorie sélectionnée.
- **Zone 9 :** Le panneau latéral affiche des informations contextuelles et des options de configuration spécifiques à l'équipement sélectionné.

IV.3 Nouvelle architecture du réseau Cevital

Pour le réseau de Cevital, une nouvelle architecture a été proposée afin d'assurer une haute disponibilité de son réseau LAN. Cette architecture hiérarchique est composée de trois couches : la couche Core, la couche distribution et la couche accès.

- **Couche Core** : dans cette couche, deux switches de niveau 3 sont utilisés. Elle est responsable de l'acheminement du trafic à haut débit à travers le réseau. Elle relie les différents équipements de distribution et assure une connectivité rapide et fiable entre eux.
- **Couche Distribution** : dans cette couche, deux switches de niveau 3 sont déployés. Elle agit comme une couche intermédiaire qui agrège le trafic provenant des commutateurs d'accès et le transmet vers les commutateurs de la couche Core.
- **Couche Accès** : C’est la couche la plus proche des utilisateurs finaux. Elle relie les appareils des utilisateurs aux commutateurs de la couche distribution.

Pour atteindre notre objectif, nous mettrons en œuvre plusieurs protocoles pour assurer la haute disponibilité du réseau. VTP et STP seront utilisés pour la gestion des VLAN et l'élimination des boucles. EtherChannel sera configuré entre les commutateurs de la couche de distribution pour améliorer la capacité et la résilience. HSRP assurera la redondance et la continuité du service au niveau de la couche de distribution. Enfin, OSPF sera utilisé pour le routage entre les commutateurs des couches core et distribution, garantissant un acheminement optimal du trafic.

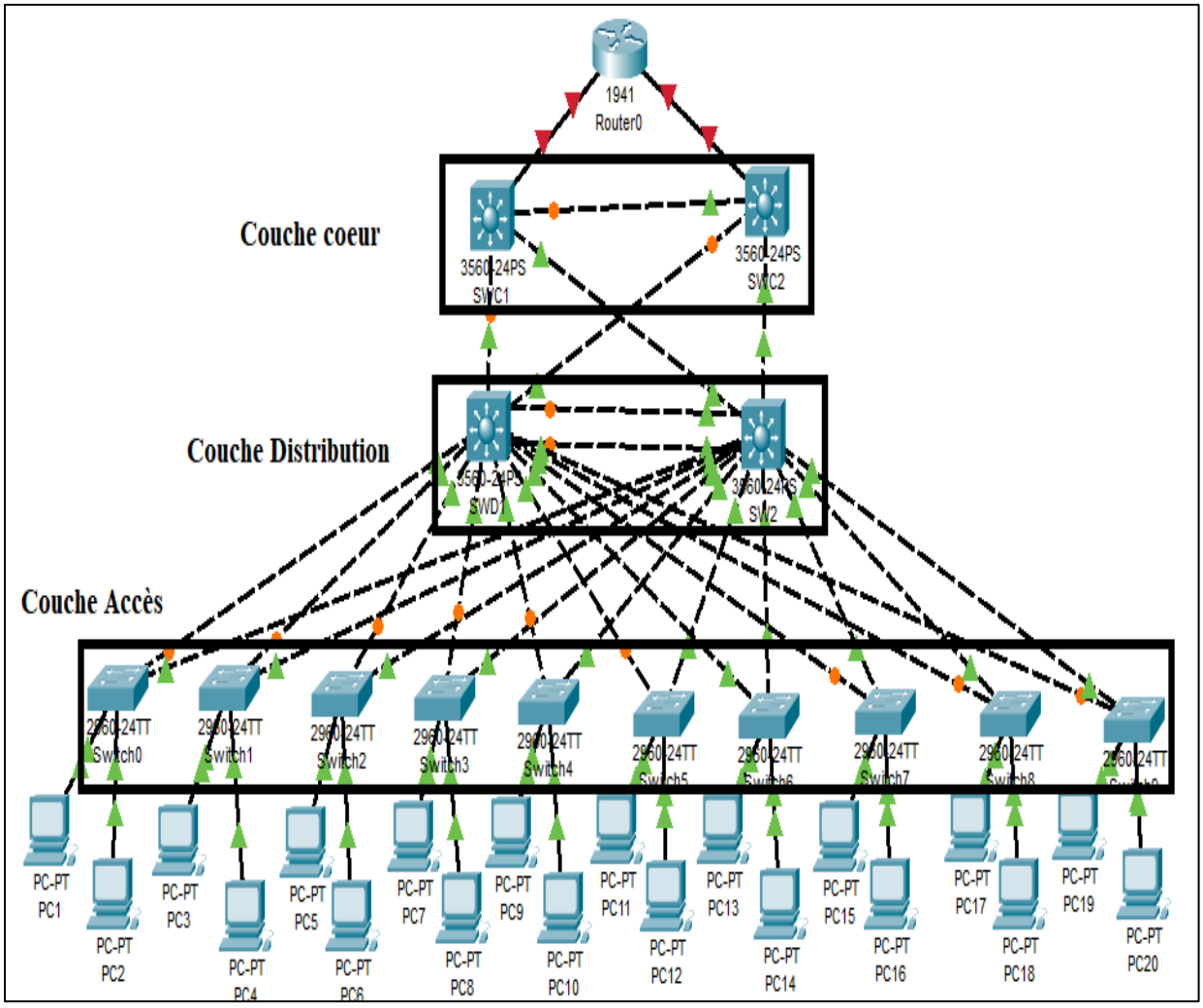


Figure IV.2 : Modèle d'architecture hiérarchique réseau Cevital.

IV.3.1 Présentation des équipements utilisés

Cevital a opté pour un réseau homogène en utilisant des équipements de la même marque pour garantir une compatibilité parfaite entre les protocoles, évitant ainsi les problèmes potentiels. Les détails des équipements réseau utilisés sont répertoriés dans le tableau IV.1, offrant une vue claire de la configuration.

	Modèle d'équipement	Nombre
Couche cœur	Switch cisco WS-C3560-24PS	02
Couche Distribution	Switch cisco WS-C3560-24PS	02
Couche d'accès	Switch Cisco WS-C2960-24TT	10
Routeur	Router Cisco 1941	01
PCs	PC-PT	20

Tableau IV.1 : Caractéristiques des équipements utilisés.

IV.3.2 Nomination des équipements

Pour une référence précise pour l'identification et le suivi de chaque équipement, des dénominations pertinentes ont été assignées aux équipements. Le tableau IV.2 détaille ces noms.

Couche Cœur	Couche Distribution	Couche d'Accès	PCs
SWC1 SWC2	SWD1 SWD2	$SWAccess_n$ n=1...10	PC_n n=1...20

Tableau IV.2 : Les nominations des équipements.

IV.3.3 Vlan de l'entreprise

L'adressage IP utilisé est de classe C et est segmenté en plusieurs sous-réseaux. Le réseau 10.30.0.0/24 est divisé en plusieurs sous-réseaux, un pour chaque VLAN. Chaque périphérique du réseau se voit attribuer une adresse IP dans le sous-réseau correspondant à son VLAN.

IV.4 Configuration de Hostname

Dans le cadre de la phase d'initialisation du projet, nous procéderons à la modification du nommage des équipements réseau. L'objectif est d'attribuer des noms significatifs et facilement reconnaissables à chaque élément afin d'en simplifier l'identification et la gestion. Prenons l'exemple d'un switch de distribution nommé "SWD1" :

```
Switch>enable
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SWD1
SWD1(config)#
```

Figure IV.3 : Exemple de configuration de Hostname.

IV.5 Configuration des Liens trunks

Nous allons établir des liaisons trunks entre les switches de distribution et les switches d'accès (niveau 2) pour permettre la communication et la transmission entre eux avec des VLANs configurés.

✧ La commande **interface range** permet de configurer plusieurs interfaces en une seule commande.

Les figures ci-dessous indiquent les commandes à saisir qui va nous permettre de configurer les différents commutateurs en mode trunk.

- Sur le SWD1 :

```
SWD1(config)#int range fa0/1-14
SWD1(config-if-range)#switchport trunk encapsulation dot1q
SWD1(config-if-range)#switchport mode trunk
```

Figure IV.4 : Exemple de configuration des liens trunks sur le SWD1.

- Sur les switches d'accès :

```
Switch(config)#int range fa0/1-2
Switch(config-if-range)#switchport mode trunk
```

Figure IV.5 : Exemple de configuration des liens trunks sur le Switch d'accès.

Après la configuration des liens trunks, la commande show interface trunk permet de vérifier l'état des trunks.

```
Switch>show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/2       on           802.1q         trunking      1
```

Figure IV.6 : Vérification des liens trunks sur Switch d'accès.

```
SWD1#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/2       on           802.1q         trunking      1
Fa0/3       on           802.1q         trunking      1
Fa0/4       on           802.1q         trunking      1
Fa0/5       on           802.1q         trunking      1
Fa0/6       on           802.1q         trunking      1
Fa0/7       on           802.1q         trunking      1
Fa0/8       on           802.1q         trunking      1
Fa0/9       on           802.1q         trunking      1
Fa0/10      on           802.1q         trunking      1
Fa0/11      on           802.1q         trunking      1
Fa0/12      on           802.1q         trunking      1
Fa0/13      on           802.1q         trunking      1
Fa0/14      on           802.1q         trunking      1
```

Figure IV.7 : Vérification des liens trunks sur le SWD1.

IV.6 Configuration d'un port EtherChannel

L'architecture réseau implémente une agrégation de liens FastEthernet entre les deux switches de distribution SWD1 et SWD2.

Pour ce faire, les deux ports FastEthernet ont été regroupés en un seul lien logique.

- La configuration suivante a été effectuée (Les figures IV.8 et IV.9 illustrent la configuration détaillée) :

✓ **Création d'un groupe de liens :**

- Les deux ports FastEthernet ont été assignés au même groupe.
- Le mode du groupe a été défini sur "ON".

✓ **Configuration du mode trunk.**

- Sur le SWD1 :

```
SWD1(config)#int range fa0/11-12
SWD1(config-if-range)#channel-group 1 mode on
SWD1(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINK-5-CHANGED: Interface Port-channel1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up

SWD1(config-if-range)#exit
SWD1(config)#int port-channel 1
SWD1(config-if)#switchport trunk encapsulation dot1q
SWD1(config-if)#switchport mode trunk
SWD1(config-if)#exit
```

Figure IV.8 : Configuration de l'EtherChannel sur le SWD1.

- Sur le SWD2 :

```
SWD2(config)#int range fa0/11-12
SWD2(config-if-range)#channel-group 1 mode on
SWD2(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINK-5-CHANGED: Interface Port-channel1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up

SWD2(config-if-range)#int port-channel 1
SWD2(config-if)#switchport trunk encapsulation dot1q
SWD2(config-if)#switchport mode trunk
```

Figure IV.9 : Configuration de l'EtherChannel sur le SWD2.

✧ La commande **show etherchannel summary** est utilisée pour vérifier la configuration d'un EtherChannel sur les switches SWD1 et SWD2 :

```
SWD1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


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

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

1      Po1(SU)           -      Fa0/11(P) Fa0/12(P)
SWD1#
```

Figure IV.10 : Vérification de la configuration d'Etherchannel sur le SWD1.

IV.7 Configuration des VLANs

En suivant les étapes décrites ci-dessus pour configurer des VLANs :

IV.7.1 Créations des Vlans

Pour créer les VLANs et leur attribuer des identifiants uniques, nous utiliserons l'interface de configuration du commutateur SWD1.

Voici les étapes à suivre :

➢ Accéder au mode configuration du commutateur.

➢ Créer un VLAN et lui attribuer un numéro d'identification.

- Nommer le VLAN pour une meilleure identification.

```
SWD1#enable
SWD1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
SWD1(config)#VLAN 10
SWD1(config-vlan)#Name DRH
SWD1(config-vlan)#VLAN 11
SWD1(config-vlan)#Name Direction-Appro
```

Figure IV.11 : Créations des Vlans.

Après avoir créé les 24 VLANs de l'entreprise, nous allons ensuite valider leur création en utilisant la commande **show vlan brief :**

```
SWD1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   DRH                              active
11   Direction-Appro                  active
12   DSI                              active
13   Raff-Huile                       active
14   Raff-sucre-3000T                 active
15   Division-utilits                 active
16   Supply-chain                     active
17   Unit-margarinerie                active
18   Printer                          active
20   Tlphone                          active
21   Voice                            active
22   Direction-R&D                    active
23   Performance-industrie            active
24   Unit-Huile                       active
25   Management-switch                active
26   DFC                              active
27   Commercial                       active
28   Direction-gnrale                 active
29   DQetMS                           active
30   Raff-sucre-3500T                 active
31   Cdt-sucre                        active
32   Camera                           active
33   Projets                          active
36   Trituration                      active
```

Figure IV.12 : Vérification de la Créations des Vlans.

IV.7.2 Configuration du VTP

Le protocole VTP permet de simplifier la gestion des VLANs en centralisant la configuration sur un serveur VTP. Pour profiter de ces avantages, nous allons configurer le switch SWD1 en tant que serveur VTP et les autres switches (SWD2 et les switches d'accès) en tant que clients VTP. Le nom de domaine VTP sera "cevital.com" et le mot de passe sera "cisco". En conséquence, nous allons suivre la procédure suivante :

✧ Configurer le switch SWD1 en tant que serveur VTP :

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

Figure IV.13 : Configuration de VTP serveur.

Après avoir configuré le protocole VTP, nous allons vérifier la configuration sur le switch SWD1 en exécutant la commande **show vtp status**.

```
SWD1#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : cevital.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 000C.CF4A.6300
Configuration last modified by 0.0.0.0 at 3-2-93 02:36:11
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          : 29
Configuration Revision            : 1
MD5 digest                        : 0x70 0x95 0x64 0xED 0x32 0x90 0xE1 0x47
                                    0x55 0x5B 0x04 0x9A 0x3E 0x8B 0xA0 0xB4
```

Figure IV.14 : Vérification de la configuration de VTP serveur.

✧ Configurer le SWD2 en mode VTP client :

```
SWD2(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWD2(config)#vtp domain cevital.com
Domain name already set to cevital.com.
SWD2(config)#vtp password cisco
Setting device VLAN database password to cisco
```

Figure IV.15 : Configuration de VTP client sur le SWD2.

Nous allons aussi vérifier la configuration sur le switch SWD2 en exécutant la commande **show vtp status**.

```
SWD2#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                       : 0001.970E.7E40
Configuration last modified by 0.0.0.0 at 2-28-93 23:00:00

Feature VLAN :
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 29
Configuration Revision            : 49
MD5 digest                        : 0xB8 0x23 0x21 0x0B 0x38 0x8C 0x7E 0x8E
                                    0x7B 0x70 0x59 0xE8 0xE2 0x8D 0x41 0x36
```

Figure IV.16 : Vérification de la configuration de VTP client sur le SWD2.

✧ Configurer les Switches d'accès en mode VTP client.

```
SWAccess1(config)#Vtp mode client
Device mode already VTP CLIENT.
SWAccess1(config)#Vtp domain cevital.com
Domain name already set to cevital.com.
SWAccess1(config)#Vtp password cisco
Setting device VLAN database password to cisco
```

Figure IV.17 : Exemple de configuration VTP client sur le SWAccess1.

Pour vérifier la configuration, nous utilisons également la commande show vtp status.

```
SWAccess1#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : cevital.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 000A.F34D.A700
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00

Feature VLAN :
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 29
Configuration Revision            : 97
MD5 digest                        : 0xD9 0xD0 0x43 0xAF 0x86 0x04 0x6F 0x90
                                    0xCA 0xD9 0x45 0xF9 0xE3 0x11 0x7A 0xA1
```

Figure IV.18 : Vérification de la configuration VTP client sur le SWAccess1.

Avant de finaliser la configuration du VTP, prenons l'exemple d'un switch en mode client pour vérifier que les VLANs sont bien propagés depuis SWD1 vers les autres switches en mode client.

```
SWAccess2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   DRH                              active
11   Direction-Appro                  active
12   DSI                              active
13   Raff-Huile                       active
14   Raff-sucre-3000T                 active
15   Division-utilits                 active
16   Supply-chain                     active
17   Unit-margarinerie                active
18   Printer                          active
20   Tlphone                          active
21   Voice                            active
22   Direction-R&D                    active
23   Performance-industrie            active
24   Unit-Huile                       active
25   Management-switch                active
26   DFC                              active
27   Commercial                       active
28   Direction-gnrale                 active
29   DQetMS                           active
30   Raff-sucre-3500T                 active
31   Cdt-sucre                        active
32   Camera                           active
33   Projets                          active
36   Trituration                      active
```

Figure IV.19 : Vérification de la propagation des VLANs.

IV.8 Configurations du protocole STP

Pour simplifier la création d'un cheminement logique sans boucle sur tout le réseau, nous prévoyons de configurer le protocole STP.

IV.8.1 Activation du Rapid Spanning Tree (RSTP) et configuration des ponts racines

1. Activation du Rapid Spanning Tree (RSTP) :

- La commande **spanning-tree mode rapid-pvst** est utilisée sur les commutateurs SWD1 et SWD2 pour activer le mode RSTP.
- Le RSTP permet une convergence plus rapide du STP après un changement de topologie réseau.

2. Configuration du pont racine :

Sur le SWD1 :

- La commande **spanning-tree vlan 10-22 root primary** définit SWD1 comme pont racine principal pour les VLANs 10 à 22. Cela signifie que SWD1 sera responsable de la gestion du STP pour ces VLANs.

- La commande **spanning-tree vlan 23-36 root secondary** définit SWD1 comme pont racine de secours pour les VLANs 23 à 36. Cela signifie que SWD1 prendra le relais en tant que pont racine pour ces VLANs si le pont racine principal (SWD2) rencontre un problème.

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

Figure IV.20 : Configuration du STP sur le SWD1.

Sur le SWD2 :

- La commande **spanning-tree vlan 23-36 root primary** définit SWD2 comme pont racine principal pour les VLANs 23 à 36.
- La commande **spanning-tree vlan 10-22 root secondary** définit SWD2 comme pont racine de secours pour les VLANs 10 à 22.

```
SWD2(config)#spanning-tree mode rapid-pvst
SWD2(config)#spanning-tree vlan 23-36 root primary
SWD2(config)#spanning-tree vlan 10-22 root primary
```

Figure IV.21 : Configuration du STP sur le SWD2.

Afin de vérifier cette configuration, nous allons utiliser la commande **show running-config** :

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

Figure IV.22 : Vérification du STP sur le SWD1.

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

Figure IV.23 : Vérification du STP sur le SWD2.

➢Pour afficher les informations relatives à la configuration du Spanning Tree pour chaque VLAN spécifique, nous allons utiliser la commande **show spanning-tree.**

```
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID     Priority    24586
              Address     00E0.B006.3410
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24586  (priority 24576 sys-id-ext 10)
              Address     00E0.B006.3410
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20
```

Figure IV.24 : Exemple d'instance STP Vlan 10.

IV.9 Configuration d'adresses IP virtuelles pour les VLANs sur SWD1 et SWD2

D'abord, nous allons activer la fonction de routage sur les switches SWD1 et SWD2 à l'aide de la commande **ip routing**. Ensuite, nous passerons à la configuration des SVI (Switch Virtual Interfaces). Nous attribuerons une adresse IP virtuelle à chaque VLAN sur les switches SWD1 et SWD2. Cela permettra aux switches de communiquer avec les périphériques du VLAN correspondant.

Sur le SWD1 :

Adresse IP virtuelle avec un masque de sous-réseau /24 et une partie machine de 252 pour chaque VLAN.

```
SWD1(config)#ip routing
SWD1(config)#int vlan 10
SWD1(config-if)#ip address 10.30.10.252 255.255.255.0
SWD1(config-if)#no shu
%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
```

Figure IV.25 : Exemple de la Configuration SVI (vlan 10) sur le SWD1.

Sur le SWD2 :

Adresse IP virtuelle avec un masque de sous-réseau /24 et une partie machine de 253 pour chaque VLAN.

```
SWD2(config)#ip routing
SWD2(config)#int vlan 10
SWD2(config-if)#ip address 10.30.10.253 255.255.255.0
SWD2(config-if)#no shu
SWD2(config-if)# exit
%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
```

Figure IV.26 : Exemple de la Configuration SVI (vlan 10) sur le SWD2.

Après avoir configuré les SVI de chaque vlan, nous allons vérifier la configuration de chaque interface SVI avec la commande **show running-config**. Cette vérification permettra de s'assurer que les adresses IP virtuelles sont correctement configurées et que le routage inter-VLAN est activé.

- Sur le SWD1

```
!
interface Vlan10
 mac-address 00e0.b006.3401
 ip address 10.30.10.252 255.255.255.0
!
interface Vlan11
 mac-address 00e0.b006.3402
 ip address 10.30.11.252 255.255.255.0
!
interface Vlan12
 mac-address 00e0.b006.3403
 ip address 10.30.12.252 255.255.255.0
!
interface Vlan13
 mac-address 00e0.b006.3404
 ip address 10.30.13.252 255.255.255.0
!
interface Vlan14
 mac-address 00e0.b006.3405
 ip address 10.30.14.252 255.255.255.0
!
interface Vlan15
 mac-address 00e0.b006.3406
 ip address 10.30.15.252 255.255.255.0
!
interface Vlan16
 mac-address 00e0.b006.3407
 ip address 10.30.16.252 255.255.255.0
!
interface Vlan17
 mac-address 00e0.b006.3408
 ip address 10.30.17.252 255.255.255.0
!
interface Vlan18
 mac-address 00e0.b006.3409
 ip address 10.30.18.252 255.255.255.0
```

```
!
interface Vlan20
 mac-address 00e0.b006.340a
 ip address 10.30.20.252 255.255.255.0
!
interface Vlan21
 mac-address 00e0.b006.340b
 ip address 10.30.21.252 255.255.255.0
!
interface Vlan22
 mac-address 00e0.b006.340c
 ip address 10.30.22.252 255.255.255.0
!
interface Vlan23
 mac-address 00e0.b006.340d
 ip address 10.30.23.252 255.255.255.0
!
interface Vlan24
 mac-address 00e0.b006.340e
 ip address 10.30.24.252 255.255.255.0
!
interface Vlan25
 mac-address 00e0.b006.340f
 ip address 10.30.25.252 255.255.255.0
!
interface Vlan26
 mac-address 00e0.b006.3411
 ip address 10.30.26.252 255.255.255.0
!
interface Vlan27
 mac-address 00e0.b006.3412
 ip address 10.30.27.252 255.255.255.0
!
interface Vlan28
 mac-address 00e0.b006.3413
 ip address 10.30.28.252 255.255.255.0
```

```
!
interface Vlan29
 mac-address 00e0.b006.3414
 ip address 10.30.29.252 255.255.255.0
!
interface Vlan30
 mac-address 00e0.b006.3415
 ip address 10.30.30.252 255.255.255.0
!
interface Vlan31
 mac-address 00e0.b006.3416
 ip address 10.30.31.252 255.255.255.0
!
interface Vlan32
 mac-address 00e0.b006.3417
 ip address 10.30.32.252 255.255.255.0
!
interface Vlan33
 mac-address 00e0.b006.3418
 ip address 10.30.33.252 255.255.255.0
!
interface Vlan36
 mac-address 00e0.b006.3419
 ip address 10.30.36.252 255.255.255.0
```

Figure IV. 27 : Vérification SVI sur le SWD1.

- Sur le SWD2

```
interface Vlan10
 mac-address 0060.4799.a401
 ip address 10.30.10.253 255.255.255.0
!
interface Vlan11
 mac-address 0060.4799.a402
 ip address 10.30.11.253 255.255.255.0
!
interface Vlan12
 mac-address 0060.4799.a403
 ip address 10.30.12.253 255.255.255.0
!
interface Vlan13
 mac-address 0060.4799.a404
 ip address 10.30.13.253 255.255.255.0
!
interface Vlan14
 mac-address 0060.4799.a406
 ip address 10.30.14.253 255.255.255.0
!
interface Vlan15
 mac-address 0060.4799.a407
 ip address 10.30.15.253 255.255.255.0
!
interface Vlan16
 mac-address 0060.4799.a408
 ip address 10.30.16.253 255.255.255.0
!
interface Vlan17
 mac-address 0060.4799.a409
 ip address 10.30.17.253 255.255.255.0
!
interface Vlan18
 mac-address 0060.4799.a40a
 ip address 10.30.18.253 255.255.255.0
```

```
interface Vlan20
 mac-address 0060.4799.a40b
 ip address 10.30.20.253 255.255.255.0
!
interface Vlan21
 mac-address 0060.4799.a40c
 ip address 10.30.21.253 255.255.255.0
!
interface Vlan22
 mac-address 0060.4799.a40d
 ip address 10.30.22.253 255.255.255.0
!
interface Vlan23
 mac-address 0060.4799.a40e
 ip address 10.30.23.253 255.255.255.0
!
interface Vlan24
 mac-address 0060.4799.a40f
 ip address 10.30.24.253 255.255.255.0
!
interface Vlan25
 mac-address 0060.4799.a410
 ip address 10.30.25.253 255.255.255.0
!
interface Vlan26
 mac-address 0060.4799.a411
 ip address 10.30.26.253 255.255.255.0
!
interface Vlan27
 mac-address 0060.4799.a412
 ip address 10.30.27.253 255.255.255.0
!
interface Vlan28
 mac-address 0060.4799.a413
 ip address 10.30.28.253 255.255.255.0
```

```
interface Vlan29
 mac-address 0060.4799.a414
 ip address 10.30.29.253 255.255.255.0
!
interface Vlan30
 mac-address 0060.4799.a415
 ip address 10.30.30.253 255.255.255.0
!
interface Vlan31
 mac-address 0060.4799.a416
 ip address 10.30.31.253 255.255.255.0
!
interface Vlan32
 mac-address 0060.4799.a417
 ip address 10.30.32.253 255.255.255.0
!
interface Vlan33
 mac-address 0060.4799.a418
 ip address 10.30.33.253 255.255.255.0
!
interface Vlan36
 mac-address 0060.4799.a419
 ip address 10.30.36.253 255.255.255.0
```

Figure IV. 28 : Vérification SVI sur le SWD2.

IV.10 Configuration du DHCP

Le protocole DHCP sera utilisé pour simplifier la gestion des adresses IP des hôtes et optimiser l'utilisation des ressources du réseau. Cela permettra une configuration dynamique des paramètres de chaque hôte. Cette configuration sera effectuée sur les commutateurs de distribution SWD1 et SWD2.

Pour éviter les conflits, la plage d'adresses de 128 à 254 sera exclue sur le SWD1, qui attribuera les adresses de 1 à 127. Le SWD2, quant à lui, attribuera les adresses de 128 à 251, excluant les plages d'adresses de 1 à 127 et 252 à 254.

Sur le SWD1

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

Figure IV.29 : Les adresses exclues 128-254 sur le SWD1.

Pour le SWD2, nous commencerons par exclure les adresses de 1 à 127, puis celles de 252 à 254.

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

Figure IV.30 : Les adresses exclues 1-127 sur le SWD2.

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

Figure IV.31 : Les adresses exclues 252-254 sur le SWD2.

- En utilisant la commande **show running-config**, nous pouvons vérifier les adresses exclues sur les switches SWD1 et SWD2, comme illustré dans les figures IV.32 et IV.33.

```
hostname SWD1
!
!
!
ip dhcp excluded-address 10.30.10.128 10.30.10.254
ip dhcp excluded-address 10.30.11.128 10.30.11.254
ip dhcp excluded-address 10.30.12.128 10.30.12.254
ip dhcp excluded-address 10.30.13.128 10.30.13.254
ip dhcp excluded-address 10.30.14.128 10.30.14.254
ip dhcp excluded-address 10.30.15.128 10.30.15.254
ip dhcp excluded-address 10.30.16.128 10.30.16.254
ip dhcp excluded-address 10.30.17.128 10.30.17.254
ip dhcp excluded-address 10.30.20.128 10.30.20.254
ip dhcp excluded-address 10.30.21.128 10.30.21.254
ip dhcp excluded-address 10.30.22.128 10.30.22.254
ip dhcp excluded-address 10.30.23.128 10.30.23.254
ip dhcp excluded-address 10.30.24.128 10.30.24.254
ip dhcp excluded-address 10.30.26.128 10.30.26.254
ip dhcp excluded-address 10.30.27.128 10.30.27.254
ip dhcp excluded-address 10.30.28.128 10.30.28.254
ip dhcp excluded-address 10.30.29.128 10.30.29.254
ip dhcp excluded-address 10.30.30.128 10.30.30.254
ip dhcp excluded-address 10.30.31.128 10.30.31.254
ip dhcp excluded-address 10.30.33.128 10.30.33.254
ip dhcp excluded-address 10.30.36.128 10.30.36.254
```

Figure IV.32 : Vérification des adresses exclues sur le SWD1.

```
hostname SWD2
!
!
!
ip dhcp excluded-address 10.30.10.1 10.30.10.127
ip dhcp excluded-address 10.30.11.1 10.30.11.127
ip dhcp excluded-address 10.30.12.1 10.30.12.127
ip dhcp excluded-address 10.30.13.1 10.30.13.127
ip dhcp excluded-address 10.30.14.1 10.30.14.127
ip dhcp excluded-address 10.30.15.1 10.30.15.127
ip dhcp excluded-address 10.30.16.1 10.30.16.127
ip dhcp excluded-address 10.30.17.1 10.30.17.127
ip dhcp excluded-address 10.30.20.1 10.30.20.127
ip dhcp excluded-address 10.30.21.1 10.30.21.127
ip dhcp excluded-address 10.30.22.1 10.30.22.127
ip dhcp excluded-address 10.30.23.1 10.30.23.127
ip dhcp excluded-address 10.30.24.1 10.30.24.127
ip dhcp excluded-address 10.30.26.1 10.30.26.127
ip dhcp excluded-address 10.30.27.1 10.30.27.127
ip dhcp excluded-address 10.30.28.1 10.30.28.127
ip dhcp excluded-address 10.30.29.1 10.30.29.127
ip dhcp excluded-address 10.30.30.1 10.30.30.127
ip dhcp excluded-address 10.30.31.1 10.30.31.127
ip dhcp excluded-address 10.30.33.1 10.30.33.127
ip dhcp excluded-address 10.30.36.1 10.30.36.127
```

Figure IV.33 : Vérification des adresses exclues sur le SWD2.

Notre prochaine étape consiste à établir un pool d'adresses IP pour chaque VLAN sur les deux switches de distributions, à l'exception du VLAN 18 (Printer), VLAN 25 (Management-switch) et VLAN 32 (Camera). Ensuite, nous définirons la passerelle par défaut pour chaque sous-réseau.

```
SWD1(config)#ip dhcp pool vlan10
SWD1(dhcp-config)#network 10.30.10.0 255.255.255.0
SWD1(dhcp-config)#default-router 10.30.10.254
SWD1(dhcp-config)#end
```

Figure IV.34 : Exemple de configuration de pool DHCP pour le vlan 10 sur le SWD1.

Nous procéderons à une vérification des pools DHCP en utilisant la commande **show running-config** pour confirmer leur création.

```
ip dhcp pool vlan10
 network 10.30.10.0 255.255.255.0
 default-router 10.30.10.254
ip dhcp pool vlan12
 network 10.30.12.0 255.255.255.0
 default-router 10.30.12.254
ip dhcp pool vlan11
 network 10.30.11.0 255.255.255.0
 default-router 10.30.11.254
ip dhcp pool vlan13
 network 10.30.13.0 255.255.255.0
 default-router 10.30.13.254
ip dhcp pool vlan14
 network 10.30.14.0 255.255.255.0
 default-router 10.30.14.254
ip dhcp pool vlan15
 network 10.30.15.0 255.255.255.0
 default-router 10.30.15.254
ip dhcp pool vlan16
 network 10.30.16.0 255.255.255.0
 default-router 10.30.16.254
ip dhcp pool vlan17
 network 10.30.17.0 255.255.255.0
 default-router 10.30.17.254
ip dhcp pool vlan20
 network 10.30.20.0 255.255.255.0
 default-router 10.30.20.254
ip dhcp pool vlan21
 network 10.30.21.0 255.255.255.0
 default-router 10.30.21.254
ip dhcp pool vlan22
 network 10.30.22.0 255.255.255.0
 default-router 10.30.22.254
```

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

Figure IV.35 : Vérification de la création des pools DHCP.

Après avoir configuré le DHCP, nous allons attribuer des ports pour les VLANs sur les switches d'accès, après nous mettrons en place la configuration des PCs sous le DHCP et nous vérifions le fonctionnement de ce dernier.

```
SWAccess1(config)#int fa0/3
SWAccess1(config-if)#switchport access vlan 10
SWAccess1(config-if)#int fa0/4
SWAccess1(config-if)#switchport access vlan 11
```

Figure IV.36 : Attribution des VLANs pour les ports de SWAcess1.

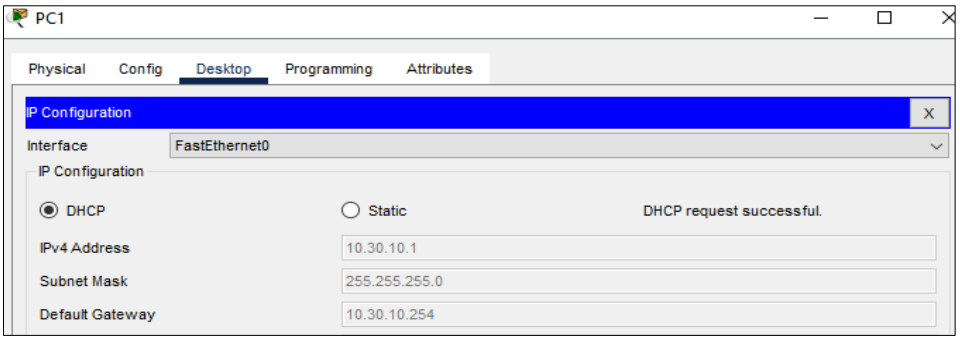


Figure IV.37 : Configuration de PC1 en mode DHCP.

IV.11 Configuration de protocole HSRP

Le protocole HSRP permet de garantir la haute disponibilité d'un routeur ou d'un switch de niveau 3 en cas de panne. Dans cette configuration, nous allons implémenter HSRP sur les deux switches de distribution, SWD1 et SWD2, pour garantir la redondance du routage pour les VLANs 10 à 36.Voici les étapes de la configuration :

- ✧ **Définition du groupe HSRP :** un groupe HSRP unique est créé, avec le même numéro sur les deux switches.
- ✧ **Configuration de la priorité standby priority :** La priorité détermine le switch qui deviendra le switch actif en cas de panne.

Voici comment nous allons configurer ces paramètres :

Sur le SWD1 :

- Nous attribuerons une priorité de 200 aux VLANs 10 à 22.
- Nous attribuerons une priorité de 150 aux VLANs 23 à 36.

```
SWD1(config)#Int vlan 10
SWD1(config-if)#Standby 10 ip 10.30.10.254
SWD1(config-if)#Standby 10 priority 200
SWD1(config-if)#Standby 10 preempt
SWD1(config-if)#Exit
```

Figure IV.38 : Exemple d'une configuration du HSRP (VLANs 10 à 22) sur le SWD1.

```
SWD1(config)#Int vlan 23
SWD1(config-if)#Standby 23 ip 10.30.23.254
SWD1(config-if)#Standby 23 priority 150
SWD1(config-if)#Standby 23 preempt
SWD1(config-if)#Exit
```

Figure IV.39 : Exemple d'une configuration du HSRP (VLANs 23à 36) sur le SWD1.

Sur le SWD2 :

- Nous attribuerons une priorité de 200 aux VLANs 23 à 36.
- Nous attribuerons une priorité de 150 aux VLANs 10 à 22.

```
SWD2(config)#Int vlan 10
SWD2(config-if)#Standby 10 ip 10.30.10.254
SWD2(config-if)#Standby 10 priority 150
SWD2(config-if)#Standby 10 preempt
SWD2(config-if)#Exit
```

Figure IV.40 : Exemple d'une configuration du HSRP (VLANs 10 à 22) sur le SWD2.

```
SWD2(config)#Int vlan 23
SWD2(config-if)#Standby 23 ip 10.30.23.254
SWD2(config-if)#Standby 23 priority 200
SWD2(config-if)#Standby 23 preempt
SWD2(config-if)#Exit
```

Figure IV.41 : Exemple d'une configuration du HSRP (VLANs 23à 36) sur le SWD2.

Ces configurations du HSRP permettront de déterminer quel switch sera l'actif en fonction des priorités attribuées à chaque groupe de VLANs.

Après avoir appliqué la configuration HSRP sur les switches SWD1 et SWD2, nous allons vérifier la configuration HSRP avec la commande **show standby brief**. Cette commande affiche un résumé des informations HSRP, y compris l'état du switch, le groupe HSRP et la priorité, nous permettant de confirmer que la configuration est correctement appliquée.

```
SWD1#show standby brief
%HSRP-6-STATECHANGE: Vlan28 Grp 28 state Speak -> Standby

                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
V110        10   200 P Active   local           10.30.10.253    10.30.10.254
V111        11   200 P Active   local           10.30.11.253    10.30.11.254
V112        12   200 P Active   local           10.30.12.253    10.30.12.254
V113        13   200 P Active   local           10.30.13.253    10.30.13.254
V114        14   200 P Active   local           10.30.14.253    10.30.14.254
V115        15   200 P Active   local           10.30.15.253    10.30.15.254
V116        16   200 P Active   local           10.30.16.253    10.30.16.254
V117        17   200 P Active   local           10.30.17.253    10.30.17.254
V118        18   200 P Active   local           10.30.18.253    10.30.18.254
V120        20   200 P Active   local           10.30.20.253    10.30.20.254
V121        21   200 P Active   local           10.30.21.253    10.30.21.254
V122        22   200 P Active   local           10.30.22.253    10.30.22.254
V123        23   150 P Standby  10.30.23.253    local           10.30.23.254
V124        24   150 P Standby  10.30.24.253    local           10.30.24.254
V125        25   150 P Standby  10.30.25.253    local           10.30.25.254
V126        26   150 P Standby  10.30.26.253    local           10.30.26.254
V127        27   150 P Standby  10.30.27.253    local           10.30.27.254
V128        28   150 P Standby  10.30.28.253    local           10.30.28.254
V129        29   150 P Standby  10.30.29.253    local           10.30.29.254
V130        30   150 P Standby  10.30.30.253    local           10.30.30.254
V131        31   150 P Standby  10.30.31.253    local           10.30.31.254
V132        32   150 P Standby  10.30.32.253    local           10.30.32.254
V133        33   150 P Standby  10.30.33.253    local           10.30.33.254
V136        36   150 P Standby  10.30.36.253    local           10.30.36.254
```

Figure IV.42 : Vérification du HSRP sur le SWD1.

```
SWD2#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
V110        10   150 P Standby  10.30.10.252    local           10.30.10.254
V111        11   150 P Standby  10.30.11.252    local           10.30.11.254
V112        12   150 P Standby  10.30.12.252    local           10.30.12.254
V113        13   150 P Standby  10.30.13.252    local           10.30.13.254
V114        14   150 P Standby  10.30.14.252    local           10.30.14.254
V115        15   150 P Standby  10.30.15.252    local           10.30.15.254
V116        16   150 P Standby  10.30.16.252    local           10.30.16.254
V117        17   150 P Standby  10.30.17.252    local           10.30.17.254
V118        18   150 P Standby  10.30.18.252    local           10.30.18.254
V120        20   150 P Standby  10.30.20.252    local           10.30.20.254
V121        21   150 P Standby  10.30.21.252    local           10.30.21.254
V122        22   150 P Standby  10.30.22.252    local           10.30.22.254
V123        23   200 P Active   local           10.30.23.252    10.30.23.254
V124        24   200 P Active   local           10.30.24.252    10.30.24.254
V125        25   200 P Active   local           10.30.25.252    10.30.25.254
V126        26   200 P Active   local           10.30.26.252    10.30.26.254
V127        27   200 P Active   local           10.30.27.252    10.30.27.254
V128        28   200 P Active   local           10.30.28.252    10.30.28.254
V129        29   200 P Active   local           10.30.29.252    10.30.29.254
V130        30   200 P Active   local           10.30.30.252    10.30.30.254
V131        31   200 P Active   local           10.30.31.252    10.30.31.254
V132        32   200 P Active   local           10.30.32.252    10.30.32.254
V133        33   200 P Active   local           10.30.33.252    10.30.33.254
V136        36   200 P Active   local           10.30.36.252    10.30.36.254
```

Figure IV.43 : Vérification du HSRP sur le SWD2.

IV.12 Configurations de Protocole OSPF

Dans cette configuration, nous allons implémenter l'OSPF sur les switches de distribution, cœur et le routeur pour établir une connectivité optimale entre les VLANs.

Les étapes de la configuration :

1. **Conversion des ports de couche 2 en couche 3 :** Les ports des switches doivent être convertis de la couche 2 (liaison de données) à la couche 3 (réseau) pour fonctionner comme des interfaces de routeur, avec la commande **no switchport**. Cette commande désactive la fonctionnalité de commutation sur le port et le configure comme une interface de routeur IP.
2. **Attribution d'une adresse IP et d'un masque de réseau :** Chaque interface de routeur doit avoir une adresse IP unique et un masque de réseau pour participer au routage OSPF.
3. **Configuration du routeur OSPF :** Définir l'ID du routeur OSPF et les paramètres de réseau.

Les figures ci-dessous illustrent la configuration des ports routés pour chaque switch (SWD1, SWD2, SWC1 et SWC2) et le routeur.

Sur le SWD1 :

```
SWD1(config)#Int fa0/13
SWD1(config-if)#no switchport
SWD1(config-if)#ip address 192.168.4.253 255.255.255.252
SWD1(config-if)#no shut
SWD1(config-if)#Exit
SWD1(config)#Int fa0/14
SWD1(config-if)#no switchport
SWD1(config-if)#ip address 192.168.1.254 255.255.255.252
SWD1(config-if)#no shut
SWD1(config-if)#Exit
```

Figure IV.44 : La configuration des ports routés sur le SWD1.

Sur le SWD2 :

```
SWD2(config)#Int fa0/13
SWD2(config-if)#no switchport
SWD2(config-if)#ip address 192.168.2.254 255.255.255.252
SWD2(config-if)#no shut
SWD2(config-if)#Exit
SWD2(config)#Int fa0/14
SWD2(config-if)#no switchport
SWD2(config-if)#ip address 192.168.3.253 255.255.255.252
SWD2(config-if)#no shut
SWD2(config-if)#Exit
```

Figure IV.45 : La configuration des ports routés sur le SWD2.

Sur le SWC1 :

```
SWC1(config)#Int fa0/1
SWC1(config-if)#no switchport
SWC1(config-if)#Ip address 192.168.2.253 255.255.255.252
SWC1(config-if)#no shut
SWC1(config-if)#Exit
SWC1(config)#Int fa 0/2
SWC1(config-if)#no switchport
SWC1(config-if)#Ip address 192.168.1.253 255.255.255.252
SWC1(config-if)#no shut
SWC1(config-if)#Exit
SWC1(config)#Int fa0/3
SWC1(config-if)#no switchport
SWC1(config-if)#Ip address 192.168.5.253 255.255.255.252
SWC1(config-if)#no shut
SWC1(config-if)#Exit
SWC1(config)#Int fa 0/4
SWC1(config-if)#no switchport
SWC1(config-if)#Ip address 192.168.6.253 255.255.255.252
SWC1(config-if)#no shut
SWC1(config-if)#Exit
```

Figure IV.46 : La configuration des ports routés sur le SWC1.

Sur le SWC2 :

```
SWC2(config)#Int fa0/1
SWC2(config-if)#no switchport
SWC2(config-if)#Ip address 192.168.4.254 255.255.255.252
SWC2(config-if)#no shut
SWC2(config-if)#Exit
SWC2(config)#Int fa 0/2
SWC2(config-if)#no switchport
SWC2(config-if)#Ip address 192.168.3.254 255.255.255.252
SWC2(config-if)#no shut
SWC2(config-if)#Exit
SWC2(config)#Int fa0/3
SWC2(config-if)#no switchport
SWC2(config-if)#Ip address 192.168.5.254 255.255.255.252
SWC2(config-if)#no shut
SWC2(config-if)#Exit
SWC2(config)#Int fa 0/4
SWC2(config-if)#no switchport
SWC2(config-if)#Ip address 192.168.7.253 255.255.255.252
SWC2(config-if)#no shut
SWC2(config-if)#Exit
```

Figure IV.47 : La configuration des ports routés sur le SWC2.

Sur le routeur :

```
Router(config)#int g0/0
Router(config-if)#Ip address 192.168.6.254 255.255.255.252
Router(config-if)#No shu

Router(config-if)#Exit
Router(config)#int g0/1
Router(config-if)#Ip address 192.168.7.254 255.255.255.252
Router(config-if)#No shu
```

Figure IV.48 : La configuration des ports routés sur le routeur.

Les figures ci-dessous illustrent la configuration d'OSPF pour chaque switch (SWD1, SWD2, SWC1 et SWC2) et le routeur :

Sur le SWD1 :

```
SWD1(config)#Router ospf 1
SWD1(config-router)#Network 192.168.1.252 0.0.0.3 area 0
SWD1(config-router)#Network 192.168.4.252 0.0.0.3 area 0
SWD1(config-router)#Network 10.30.10.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.11.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.12.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.13.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.14.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.15.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.16.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.17.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.18.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.20.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.21.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.22.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.23.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.24.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.25.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.26.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.27.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.28.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.29.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.30.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.31.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.32.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.33.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.30.36.0 0.0.0.255 area 0
SWD1(config-router)#exit
```

Figure IV.49 : La configuration de l'OSPF sur le SWD1.

Sur le SWD2 :

```
SWD2(config)#Ip routing
SWD2(config)#Router ospf 1
SWD2(config-router)#Network 192.168.3.252 0.0.0.3 area 0
SWD2(config-router)#Network 192.168.2.252 0.0.0.3 area 0
SWD2(config-router)#Network 10.30.10.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.11.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.12.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.13.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.14.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.15.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.16.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.17.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.18.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.20.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.21.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.22.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.23.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.24.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.25.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.26.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.27.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.28.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.29.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.30.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.31.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.32.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.33.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.30.36.0 0.0.0.255 area 0
SWD2(config-router)#exit
```

Figure IV.50 : La configuration de l'OSPF sur le SWD2.

Sur le SWC1 :

```
SWC1(config)#Ip routing
SWC1(config)#Router ospf 1
SWC1(config-router)#Network 192.168.1.252 0.0.0.3 area 0
SWC1(config-router)#Network 192.168.2.252 0.0.0.3 area 0
SWC1(config-router)#Network 192.168.5.252 0.0.0.3 area 0
SWC1(config-router)#Network 192.168.6.252 0.0.0.3 area 0
SWC1(config-router)#exit
```

Figure IV.51 : La configuration de l'OSPF sur le SWC1.

Sur le SWC2 :

```
SWC2(config)#Ip routing
SWC2(config)#Router ospf 1
SWC2(config-router)#Network 192.168.4.252 0.0.0.3 area 0
SWC2(config-router)#Network 192.168.3.252 0.0.0.3 area 0
SWC2(config-router)#Network 192.168.5.252 0.0.0.3 area 0
SWC2(config-router)#Network 192.168.7.252 0.0.0.3 area 0
SWC2(config-router)#Exit
```

Figure IV.52 : La configuration de l'OSPF sur le SWC2.

Sur le routeur :

```
Router(config)#Ip routing
Router(config)#Router ospf 1
Router(config-router)#Network 192.168.6.252 0.0.0.3 area 0
Router(config-router)#Network 192.168.7.252 0.0.0.3 area 0
```

Figure IV.53 : La configuration de l'OSPF sur le routeur.

Et nous pouvons vérifier avec la commande **Show IP route :**

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

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 24 subnets
O       10.30.10.0/24 [110/3] via 192.168.6.253, 00:01:40, GigabitEthernet0/0
                      [110/3] via 192.168.7.253, 00:01:40, GigabitEthernet0/1
O       10.30.11.0/24 [110/3] via 192.168.6.253, 00:01:40, GigabitEthernet0/0
                      [110/3] via 192.168.7.253, 00:01:40, GigabitEthernet0/1
O       10.30.12.0/24 [110/3] via 192.168.6.253, 00:01:40, GigabitEthernet0/0
                      [110/3] via 192.168.7.253, 00:01:40, GigabitEthernet0/1
O       10.30.13.0/24 [110/3] via 192.168.6.253, 00:01:40, GigabitEthernet0/0
                      [110/3] via 192.168.7.253, 00:01:40, GigabitEthernet0/1
O       10.30.14.0/24 [110/3] via 192.168.6.253, 00:01:40, GigabitEthernet0/0
                      [110/3] via 192.168.7.253, 00:01:40, GigabitEthernet0/1
O       10.30.15.0/24 [110/3] via 192.168.6.253, 00:01:40, GigabitEthernet0/0
                      [110/3] via 192.168.7.253, 00:01:40, GigabitEthernet0/1
O       10.30.16.0/24 [110/3] via 192.168.6.253, 00:01:40, GigabitEthernet0/0
                      [110/3] via 192.168.7.253, 00:01:40, GigabitEthernet0/1
O       10.30.17.0/24 [110/3] via 192.168.6.253, 00:01:40, GigabitEthernet0/0
                      [110/3] via 192.168.7.253, 00:01:40, GigabitEthernet0/1
O       10.30.18.0/24 [110/3] via 192.168.6.253, 00:01:40, GigabitEthernet0/0
                      [110/3] via 192.168.7.253, 00:01:40, GigabitEthernet0/1
O       10.30.20.0/24 [110/3] via 192.168.6.253, 00:01:40, GigabitEthernet0/0
                      [110/3] via 192.168.7.253, 00:01:40, GigabitEthernet0/1
O       10.30.21.0/24 [110/3] via 192.168.6.253, 00:01:40, GigabitEthernet0/0
                      [110/3] via 192.168.7.253, 00:01:40, GigabitEthernet0/1
O       10.30.22.0/24 [110/3] via 192.168.6.253, 00:01:40, GigabitEthernet0/0
```

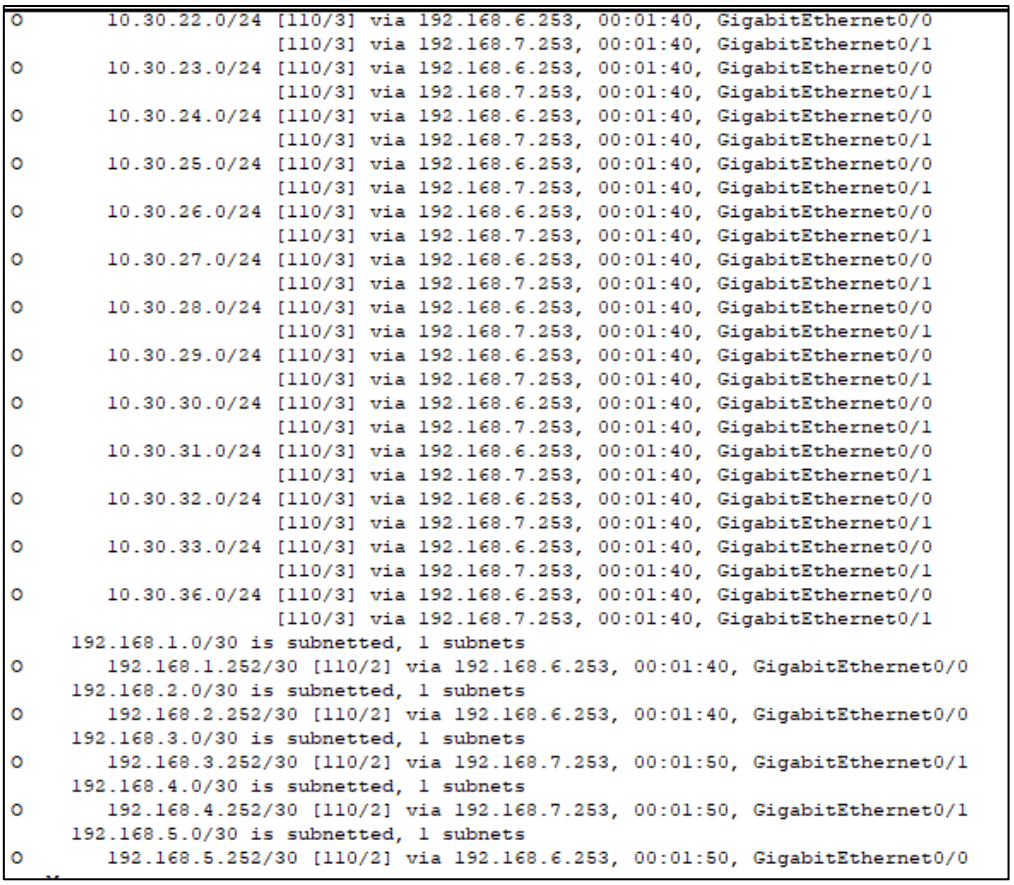


Figure IV.54 : Vérification de l'OSPF.

IV.13 La nouvelle approche d'architecture en haute disponibilité

Cette nouvelle approche d'architecture en haute disponibilité à trois couches intègre plusieurs protocoles pour assurer la continuité des services réseau et minimiser les temps d'arrêt en cas de panne.

Les protocoles VTP, STP, EtherChannel, DHCP, HSRP, et OSPF sont utilisés ensemble pour créer une infrastructure résiliente et efficace. Cette approche assure une gestion simplifiée des VLAN, l'élimination des boucles, une capacité accrue et une meilleure résilience du réseau grâce à l'agrégation des liens. La redondance et la continuité du service sont garanties par HSRP, tandis qu'OSPF optimise le routage entre les couches core et distribution.

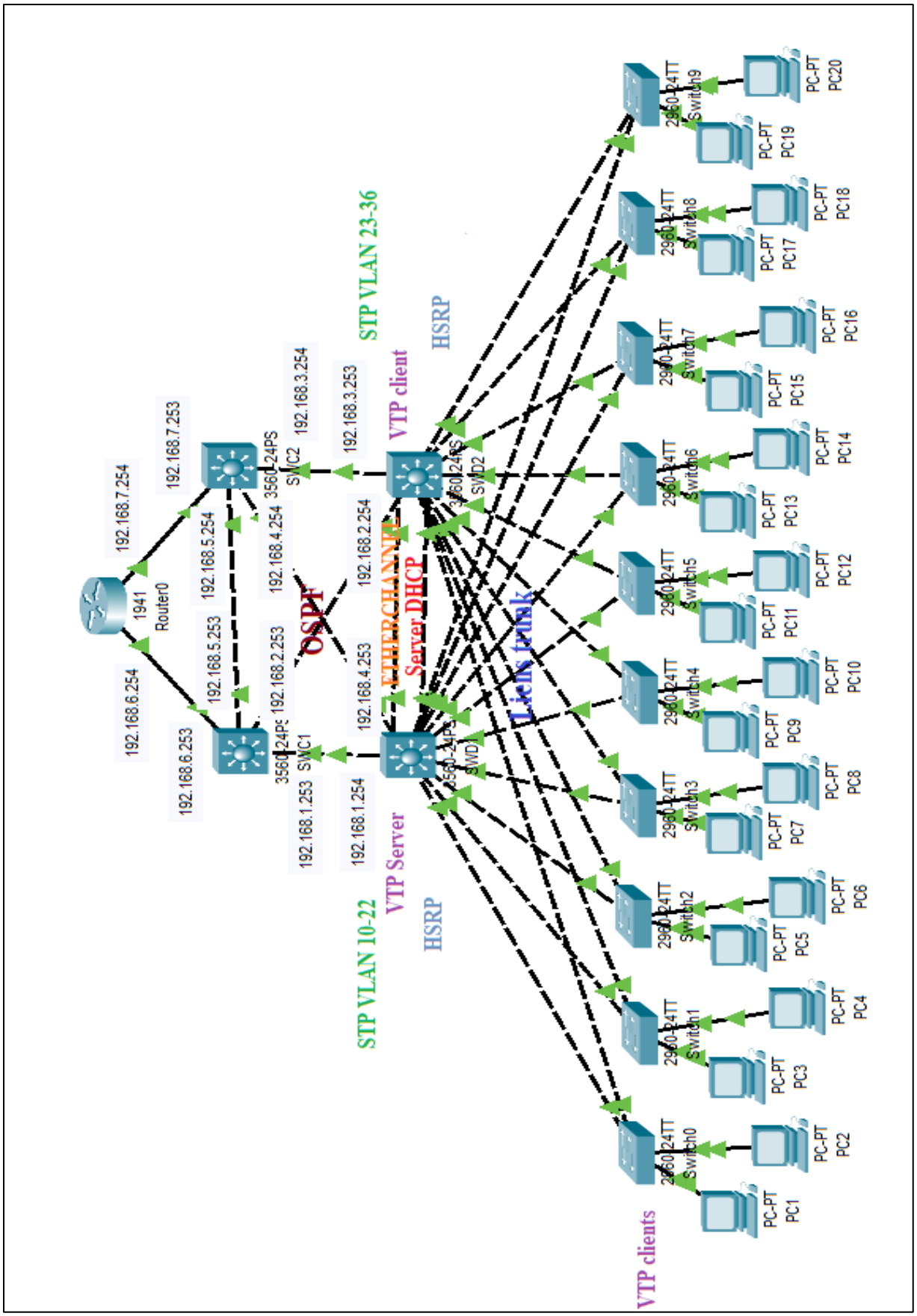


Figure IV.55 : La nouvelle approche de l'architecture en haute disponibilité.

IV.14 Tests de la haute disponibilité

Afin de garantir la disponibilité et la performance de notre réseau LAN, nous mettrons en place une série de tests rigoureux :

- **Test de ping continu :** Un ping continu sera effectué entre un VLAN et une autre interface afin de surveiller la latence et la connectivité.
- **Simulation de panne :** La route principale sera mise en **shutdown** pour simuler une panne et observer le comportement du réseau.
- **Vérification du basculement :** Le basculement vers une route secondaire sera observé et analysé pour garantir la continuité du service en cas de panne.
- **Rétablissement de la route principale :** La route principale sera remise en service pour garantir la reprise automatique du trafic.

IV.14.1 Test de connectivité entre VLANs au niveau de la couche distribution

Ce test vise à vérifier la connectivité entre deux PC appartenant à des VLANs distincts.

- Un ping continu est effectué depuis le PC1 du VLAN 10 vers le PC3 du VLAN 12.

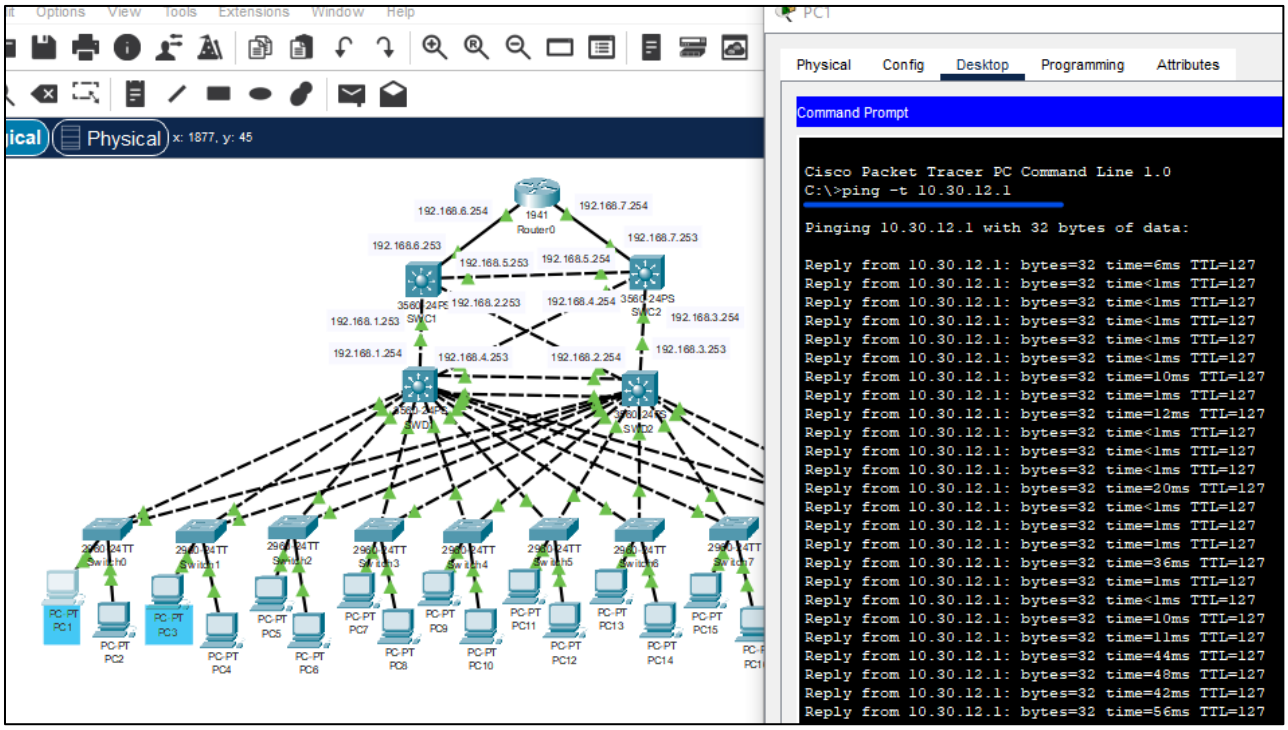


Figure IV.56 : Test de connectivité inter-VLAN.

Résultats :

- Le test a été réalisé avec succès (comme le montre la figure IV.56). Le ping continu entre les deux PC n'a rencontré aucune interruption, confirmant ainsi la connectivité optimale entre les VLANs 10 et 12.

Maintenant nous visons à simuler une panne de la route principale du VLAN 10 et à observer le comportement du protocole STP en cas de basculement vers la route secondaire :

- **Simulation de la panne :** Mettre hors service la route principale (liaison rouge sur la figure IV.57) en la désactivant.

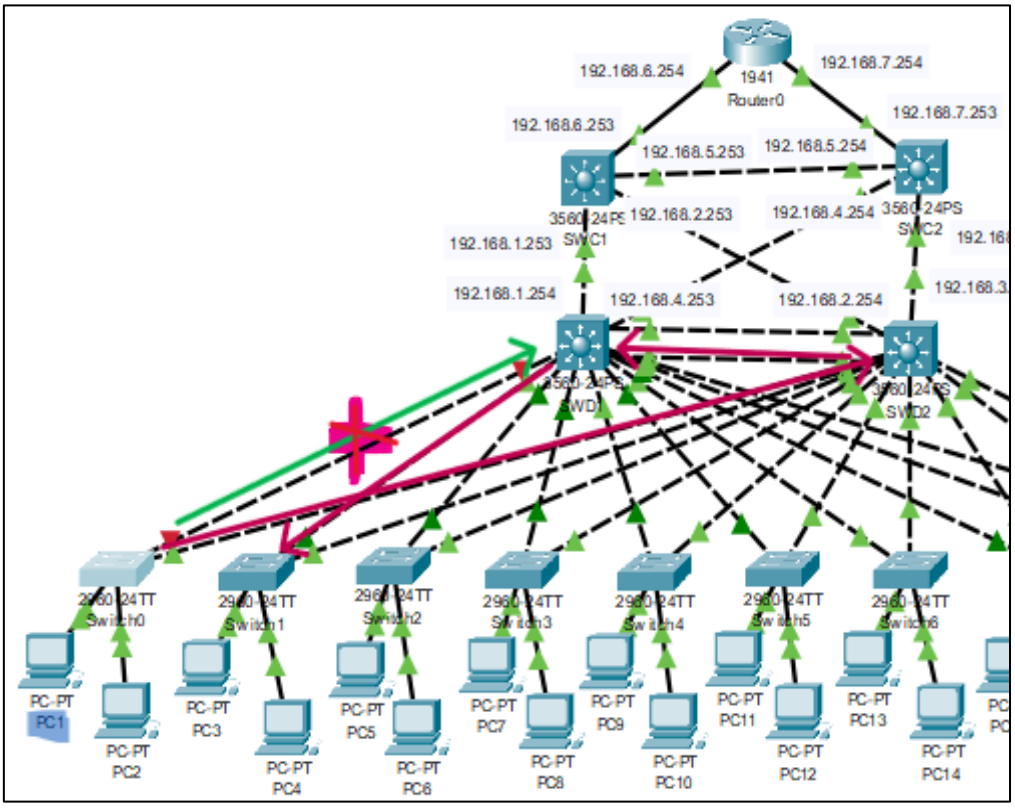


Figure IV.57 : simulation d'une panne sur la route principale d'un VLAN.

- **Observation du comportement du réseau :** Surveiller le ping en cours entre les deux PC des VLANs 10 et 12 et Observer le basculement vers la route secondaire et la reprise du trafic.

```
C:\>ping -t 10.30.12.1

Pinging 10.30.12.1 with 32 bytes of data:

Reply from 10.30.12.1: bytes=32 time=35ms TTL=127
Reply from 10.30.12.1: bytes=32 time=222ms TTL=127
Reply from 10.30.12.1: bytes=32 time=2ms TTL=127
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 10.30.12.1: bytes=32 time<1ms TTL=127
Reply from 10.30.12.1: bytes=32 time=11ms TTL=127
Reply from 10.30.12.1: bytes=32 time<1ms TTL=127
Reply from 10.30.12.1: bytes=32 time=21ms TTL=127
Reply from 10.30.12.1: bytes=32 time<1ms TTL=127
Reply from 10.30.12.1: bytes=32 time<1ms TTL=127
Reply from 10.30.12.1: bytes=32 time=4ms TTL=127
Reply from 10.30.12.1: bytes=32 time<1ms TTL=127
Reply from 10.30.12.1: bytes=32 time=10ms TTL=127
```

Figure IV.58 : Conséquences d'une panne sur la route principale du VLAN 10.

Résultats :

Lors d'une panne sur la route principale du VLAN 10, le protocole STP entre en action pour garantir la continuité du service. Il redirige le trafic vers le commutateur non racine (SWD2), qui devient alors la passerelle temporaire pour ce VLAN.

Ce chemin alternatif n'est pas optimal et peut entraîner une légère baisse des performances du réseau. Une perte de connectivité temporaire se produise durant le basculement vers le chemin secondaire, le temps que le STP reconfigure le réseau.

- **Réactivation de l'interface principale**

  Ce test vise à réactiver l'interface principale (liaison rouge sur la figure IV.57) :

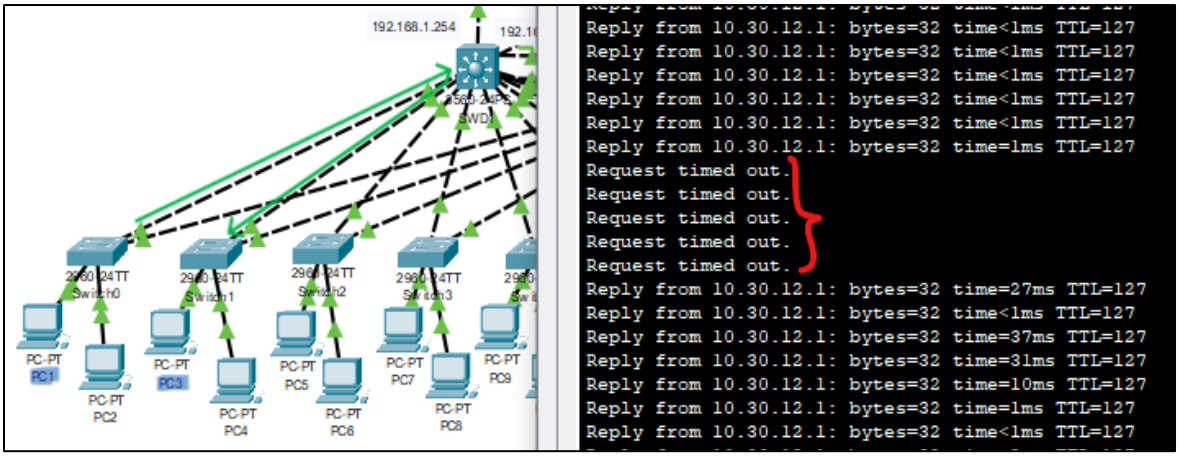


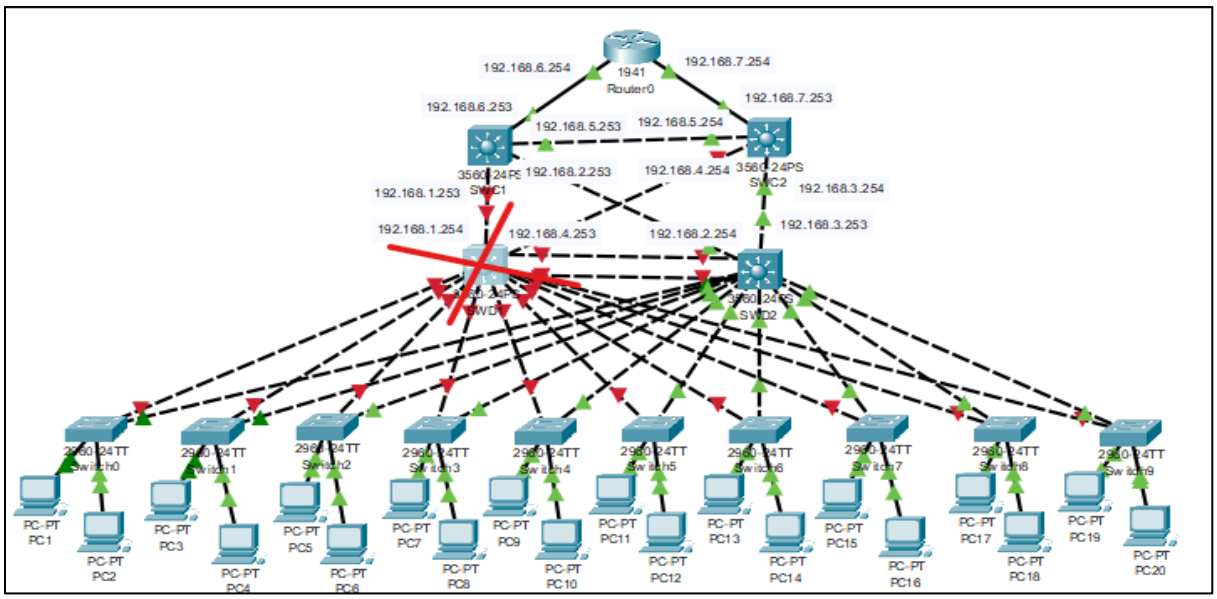
Figure IV.59 : Réactivation de la route principale du VLAN 10.

Résultats :

Le test a été réalisé avec succès. La réactivation de l'interface principale a provoqué une interruption temporaire du ping car Lorsque la route principale du VLAN 10 est réparée et remise en service, le protocole STP va automatiquement la détecter et basculer le trafic vers elle.

IV.14.2 Test de niveau 2

La simulation a été réalisée en provoquant une panne matérielle sur le switch SWD1, qui est le switch principal du VLAN 10.




```
C:\>ping -t 10.30.12.1

Pinging 10.30.12.1 with 32 bytes of data:

Reply from 10.30.12.1: bytes=32 time=68ms TTL=127
Reply from 10.30.12.1: bytes=32 time=887ms TTL=127
Reply from 10.30.12.1: bytes=32 time<1ms TTL=127
Reply from 10.30.12.1: bytes=32 time=13ms TTL=127
Reply from 10.30.12.1: bytes=32 time=1ms TTL=127
Reply from 10.30.12.1: bytes=32 time<1ms TTL=127
Reply from 10.30.12.1: bytes=32 time=128ms TTL=127
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 10.30.12.1: bytes=32 time=11ms TTL=127
Reply from 10.30.12.1: bytes=32 time=95ms TTL=127
Reply from 10.30.12.1: bytes=32 time<1ms TTL=127
Reply from 10.30.12.1: bytes=32 time<1ms TTL=127
Reply from 10.30.12.1: bytes=32 time<1ms TTL=127
Reply from 10.30.12.1: bytes=32 time=37ms TTL=127
Reply from 10.30.12.1: bytes=32 time<1ms TTL=127
Reply from 10.30.12.1: bytes=32 time<1ms TTL=127
Reply from 10.30.12.1: bytes=32 time<1ms TTL=127
Reply from 10.30.12.1: bytes=32 time<1ms TTL=127
```

Figure IV.60 : Simulation d'une panne sur SWD1 et impact sur la connectivité.

Résultats :

La simulation de la panne a provoqué une interruption temporaire du ping. Le switch SWD2, ayant la deuxième priorité HSRP la plus élevée, a pris le relais en tant que switch principal du VLAN 10. Le processus de basculement a entraîné une perte de 5 à 6 paquets pendant la période nécessaire pour que le switch standby prenne le relais.

✧ **Réactivation du switch principal et test du preemption HSRP :**

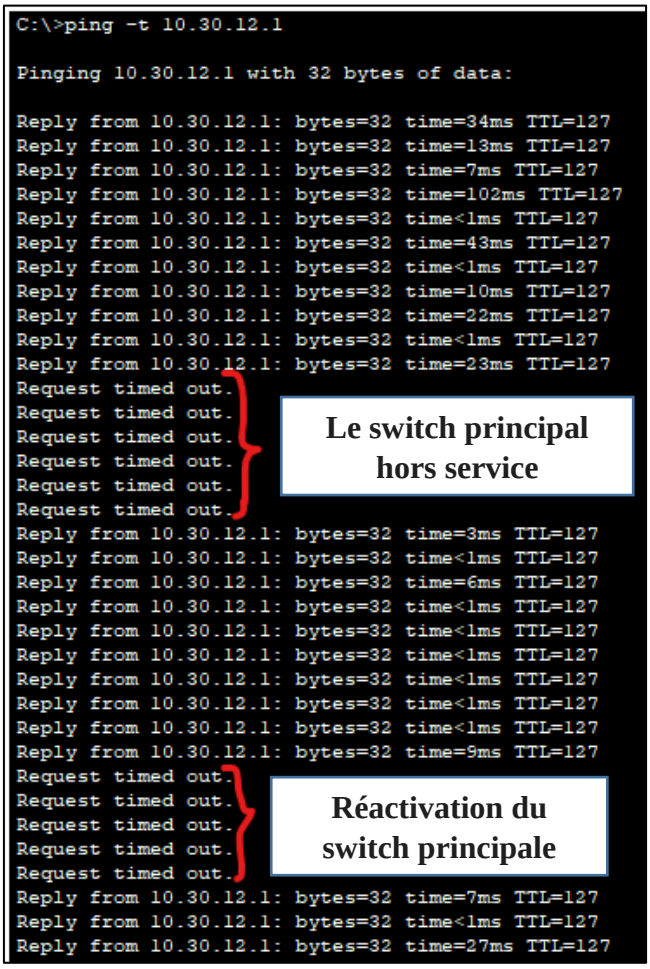


Figure IV.61 : Observation du comportement du trafic réseau pendant les simulations.

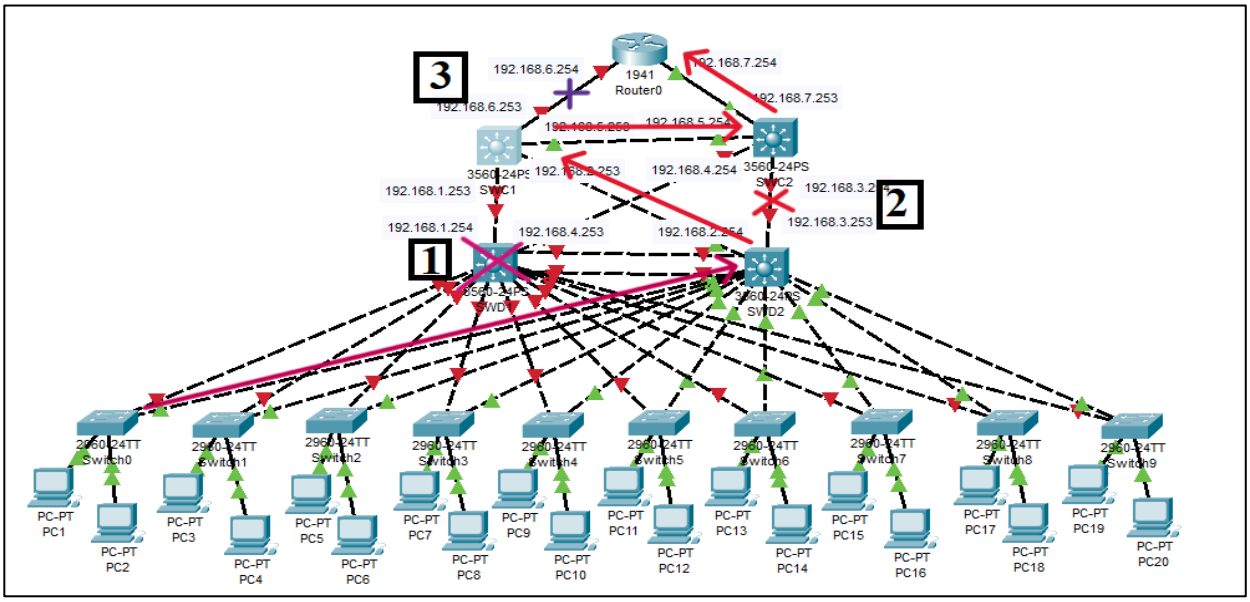
Résultats :

Le test a été réalisé avec succès. Quand le switch principal a été remis en service, une interruption temporaire du ping a été observée, mais le HSRP a rapidement effectué la préemption et SWD1 est redevenu le switch principal du VLAN 10. Le ping a ensuite repris sans interruption.

IV.14.3 Test de niveau 3

Nous avons évalué la capacité du réseau local de Cevital à maintenir la connectivité et les services en cas de défaillances critiques. Pour cela, nous avons suivi les étapes suivantes :

- ✧ Configuration d'un test de ping continu depuis un PC du VLAN 10 vers l'adresse 192.168.7.254 (une interface du routeur).
- ✧ Simulation de pannes :
  1. Panne du switch de distribution SWD1 (root bridge du VLAN 10).
  2. Panne du lien Fa0/14 sur le switch SWD2.
  3. Panne du lien Fa0/4 sur le switch SWC2.




```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping -t 192.168.7.254

Pinging 192.168.7.254 with 32 bytes of data:

Reply from 192.168.7.254: bytes=32 time=14ms TTL=253
Reply from 192.168.7.254: bytes=32 time<1ms TTL=253
Reply from 192.168.7.254: bytes=32 time=184ms TTL=253
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.                                      1
Reply from 192.168.7.254: bytes=32 time=53ms TTL=253
Reply from 192.168.7.254: bytes=32 time<1ms TTL=253
Reply from 192.168.7.254: bytes=32 time<1ms TTL=253
Reply from 192.168.7.254: bytes=32 time<1ms TTL=253
Reply from 192.168.7.254: bytes=32 time<1ms TTL=253
Request timed out.
Request timed out.                                      2
Reply from 192.168.7.254: bytes=32 time<1ms TTL=253
Reply from 192.168.7.254: bytes=32 time<1ms TTL=253
Reply from 192.168.7.254: bytes=32 time<1ms TTL=253
Reply from 192.168.7.254: bytes=32 time<1ms TTL=253
Reply from 192.168.7.254: bytes=32 time<1ms TTL=253
Reply from 192.168.7.254: bytes=32 time<1ms TTL=253
Reply from 192.168.7.254: bytes=32 time<1ms TTL=253
Request timed out.
Request timed out.                                      3
Reply from 192.168.7.254: bytes=32 time=66ms TTL=252
Reply from 192.168.7.254: bytes=32 time<1ms TTL=252
Reply from 192.168.7.254: bytes=32 time=20ms TTL=252
Reply from 192.168.7.254: bytes=32 time<1ms TTL=252
Reply from 192.168.7.254: bytes=32 time=10ms TTL=252
Reply from 192.168.7.254: bytes=32 time<1ms TTL=252
Reply from 192.168.7.254: bytes=32 time=9ms TTL=252
Reply from 192.168.7.254: bytes=32 time<1ms TTL=252
```

Figure IV.62 : Schéma du scénario de test.

Résultats :

Le test a permis de constater que :

✧ **Le HSRP a fonctionné correctement :** Le trafic réseau a basculé vers le switch de secours en cas de panne du switch principal.

✧ **OSPF a fonctionné correctement :** Les routes OSPF ont été mises à jour en cas de panne de lien. Le trafic réseau a continué à circuler malgré la panne des liens.

IV.15 Conclusion

Ce chapitre s'est concentré sur la mise en œuvre d'un réseau LAN hautement disponible pour Cevital. En s'appuyant sur des protocoles éprouvés tels que STP, HSRP et OSPF, la méthodologie employée a permis de garantir une disponibilité continue des services critiques pour l'entreprise.

Conclusion générale

Dans un contexte où la dépendance au numérique s'accroît de manière exponentielle, garantir la haute disponibilité d'un réseau local (LAN) est devenu un enjeu crucial pour la continuité opérationnelle et la compétitivité des entreprises.

Ce projet de fin d'études a été consacré à la mise en œuvre d'une solution de haute disponibilité pour le réseau local de Cevital Agro-industrie. À travers les différents chapitres de ce mémoire, nous avons parcouru un chemin allant des principes fondamentaux des réseaux informatiques à la réalisation concrète d'une architecture réseau résiliente, capable de répondre aux besoins croissants en termes de performance et de disponibilité.

Sur la base de cette analyse détaillée, une architecture réseau LAN redondante utilisant une combinaison de protocoles tels que STP, HSRP et OSPF a été conçue et implémentée pour Cevital. La solution proposée a été rigoureusement évaluée par le biais de simulations complètes sur Cisco Packet Tracer, en s'attardant sur les performances et la disponibilité du réseau.

Les résultats obtenus démontrent clairement l'efficacité du HSRP pour garantir la haute disponibilité du réseau LAN de Cevital. La redondance apportée par le protocole a permis de minimiser considérablement les temps d'indisponibilité, assurant ainsi une continuité opérationnelle quasi-parfaite. En cas de défaillance matérielle, le basculement automatique vers un routeur de secours se fait de manière transparente, minimisant ainsi les interruptions de service et garantissant une expérience utilisateur fluide.

En conclusion, ce mémoire a permis de confirmer l'intérêt et l'efficacité du HSRP pour garantir la haute disponibilité d'un réseau LAN. Les résultats obtenus et les leçons apprises serviront de base à de futures recherches pour améliorer encore les performances et la résilience des réseaux informatiques dans les environnements industriels exigeants.

Annexes

Equipement local	Equipement(s) distant(s)	Interface local	Interface(s) distante(s)
Router	SWC1	G0/0	Fa0/4
Router	SWC2	G0/1	Fa0/4
SWC1	SWC2	Fa0/3	Fa0/3
SWC1	SWD1	Fa0/2	Fa0/14
SWD1	SWD2	Fa0/1	Fa0/13
SWC2	SWD1	Fa0/1	Fa0/13
SWC2	SWD2	Fa0/2	Fa0/14
SWD1	SWC1	Fa0/14	Fa0/2
SWD1	SWC2	Fa0/13	Fa0/1
SWD1	SWD2	Fa0/12-Fa0/11	Fa0/12-Fa0/11
SWD1	SW d'accès1-10	Fa0/1-10	Fa0/1
SWD2	SW d'accès1-10	Fa0/1-10	Fa0/2

Equipement	Interface	Addresse IP
SWD1	Fa0/14	192.168.1.254/30
SWD1	Fa0/13	192.168.4.253/30
SWD2	Fa0/14	192.168.3.253/30
SWD2	Fa0/13	192.168.2.254/30
SWC1	Fa0/1	192.168.2.253/30
SWC1	Fa0/2	192.168.1.253/30
SWC1	Fa0/3	192.168.5.253/30
SWC1	Fa0/4	192.168.6.253/30
SWC2	Fa0/1	192.168.4.254/30
SWC2	Fa0/2	192.168.3.254/30
SWC2	Fa0/3	192.168.5.254/30
SWC2	Fa0/4	192.168.7.253/30
Router	G0/0	192.168.6.254/30
Router	G0/1	192.168.7.254/30

Vlan	Adressage					
Id	**Switch principal**	**Type**	**Réseau**	**SVI sur SWD1**	**SVI sur SWD2**	**Passerelle**
10	SWD1	DHCP	10.30.10.0/24	10.30.10.252	10.30.10.253	10.30.10.254
11	SWD1	DHCP	10.30.11.0/24	10.30.11.252	10.30.11.253	10.30.11.254
12	SWD1	DHCP	10.30.12.0/24	10.30.12.252	10.30.12.253	10.30.12.254
13	SWD1	DHCP	10.30.13.0/24	10.30.13.252	10.30.13.253	10.30.13.254
14	SWD1	DHCP	10.30.14.0/24	10.30.14.252	10.30.14.253	10.30.14.254
15	SWD1	DHCP	10.30.15.0/24	10.30.15.252	10.30.15.253	10.30.15.254
16	SWD1	DHCP	10.30.16.0/24	10.30.16.252	10.30.16.253	10.30.16.254
17	SWD1	DHCP	10.30.17.0/24	10.30.17.252	10.30.17.253	10.30.17.254
18	SWD1	statique	10.30.18.0/24	10.30.18.252	10.30.18.253	10.30.18.254
20	SWD1	DHCP	10.30.20.0/24	10.30.20.252	10.30.20.253	10.30.20.254
21	SWD1	DHCP	10.30.21.0/24	10.30.21.252	10.30.21.253	10.30.21.254
22	SWD1	DHCP	10.30.22.0/24	10.30.22.252	10.30.22.253	10.30.22.254
23	SWD2	DHCP	10.30.23.0/24	10.30.23.252	10.30.23.253	10.30.23.254
24	SWD2	DHCP	10.30.24.0/24	10.30.24.252	10.30.24.253	10.30.24.254
25	SWD2	statique	10.30.25.0/24	10.30.25.252	10.30.25.253	10.30.25.254
26	SWD2	DHCP	10.30.26.0/24	10.30.26.252	10.30.26.253	10.30.26.254
27	SWD2	DHCP	10.30.27.0/24	10.30.27.252	10.30.27.253	10.30.27.254
28	SWD2	DHCP	10.30.28.0/24	10.30.28.252	10.30.28.253	10.30.28.254
29	SWD2	DHCP	10.30.29.0/24	10.30.29.252	10.30.29.253	10.30.29.254
30	SWD2	DHCP	10.30.30.0/24	10.30.30.252	10.30.30.253	10.30.30.254
31	SWD2	DHCP	10.30.31.0/24	10.30.31.252	10.30.31.253	10.30.31.254
32	SWD2	statique	10.30.32.0/24	10.30.32.252	10.30.32.253	10.30.32.254
33	SWD2	DHCP	10.30.33.0/24	10.30.33.252	10.30.33.253	10.30.33.254
36	SWD2	DHCP	10.30.36.0/24	10.30.36.252	10.30.36.253	10.30.36.254

Bibliographie

[1] : Claude Servin., *Réseaux et télécoms*, 2003, éditeur Dunod, p54-55, p162-168.

[2] : Guy Pujolle, *Cours réseaux et télécoms*, édition Eyrolles 2004.

[4] : Jean-François P, Fabrice L. *Tout sur les Réseaux et internet*, 4éme édition 2015, Editeur Dunod, p78-80.

[6] : ATELIN, Philippe et DORDOIGNE, José. *Réseaux informatiques : Notions fondamentales Normes, Architecture, Modèle OSI, TCP/IP, Ethernet, Wi-Fi*, éditions ENI 2006.

[7]: Soumia chelihi, *Les équipements d'interconnexion*, Mémoire master Département Informatique, université de Guelma.2015.

[8]: Support de Cours.*Réseau Fst Chapitre 4: supports de transmission*, édition 2014.

[9]:G. Valet, *Modèle OSI et TCP/IP*, édition Novembre 2010.

[10]: PUJOLLE, Eric. *Réseau TCP/IP*, édition ENI 2009.

[12] : Christian Bulfone. *Le protocole IP*, édition 2015

[14] : Belgacem JARRAY, *Réseaux informatique*, éditions 2015.

[15] : Source interne de CEVITAL.

[16] : Carthern, & Rivera, N. *Introduction to Availability*. Cisco Networks, édition 2021.

[19] : R. Jurnal et al, ANALISA *DAN IMPLEMENTASI VTP DENGAN ETHERCHANNEL TYPE LACP*, édition 2018.

[20] : David Bombal, *Designing and Implementing Cisco Networks*, édition 2019.

[21] : Jessica H. Fong et al, *Better Alternatives to OSPF Routing*, édition 2005.

[22] : Diane E. Baker et David S, *Perkins.Réseaux de campus Cisco*, édition 2016.

Webographie

[3] : https://www.geonov.fr/architecture-client-serveur/, consulté le 21 mars 2024.

[5] : https://fr.scribd.com/document/655255386/Cours-Topologie, consulté le 23 mars 2024.

[11] : https://pandorafms.com/blog/fr/protocoles-de gestion-reseau/, consulté le 15 mars 2024.

[13] : https://www.connecthostproject.com/vtp.html, consulté le 01 mars 2024.

[17] : https://www.silicon.fr/avis-expert/equilibrage-des-charges-lincontournable-dune-infrastructure-haute-disponibilite, consulté le 01 avril 2024.

[18] : https://fr.slideshare.net/EliorBoukhobza/haute-disponibilit-et-tolrance-de-panne, Consulté le 10 mars 2024.

[23] : https://www.it-connect.fr/mise-en-place-du-protocole-hsrp/, consulté le 03 mars 2024.

[24] : https://ciscotracer.wordpress.com/2014/03/13/hsrp-hot-standby-routing protocol/, consulté le 05 mars 2024.

[25] : https://www.networklab.fr/hsrp/, consulté le 28 mars 2024.

[26] : https://abcxperts.com/fr/hsrp-vrrp-glbp-entendiendo-los-protocolos-clave-para-la-redundancia-en-redes/, consulté le 01avril 2024.

[F1] : https://www.assistancescolaire.com/eleve/3e/technologie/reviser-une-notion/3_tec_18

[F2] :http://robert.cireddu.free.fr/SNIR/Cours%20sur%20la%20topologie%20des%20reseaux.

[F3] : https://www.numerique-sciences-informatiques.fr/coursReseaux

[F4] : https://cisco.goffinet.org/ccna/fondamentaux/modeles-tcp-ip-osi/

[F5] : https://www.formip.com/pages/blog/dtp-dynamic-trunking-protocol

[F6] : https://www.novojob.com/algerie/entreprise/groupe-cevital/presentation

[F7] : https://www.google.com/maps/place/Cevital+Agroindustrie/

[F8] : Document édité par l'organisme d’accueil cevital agro-industrie.

[F9] : https://www.cisco.com/c/fr_ca/support/routers/2900-series-integrated-services-routers-isr/series.html

[F10] : https://www.router-switch.com/ws-c4507r-e-p-516.html

[F11] : https://m.indiamart.com/proddetail/fortinet-firewall-13387367930.html

[F12] : https://networkel.com/etherchannel-explained/

[F13] : https://afrozahmad.com/blog/stp-spanning-tree-protocol-explained-in-detail/

[F14] : https://www.it-connect.fr/mise-en-place-du-protocole-hsrp/

[F15] : https://www.networklab.fr/hsrp/

Résumé

Ce document fait partie de notre projet de fin d'études en vue de l'obtention du diplôme de master en Télécommunications, avec une spécialisation en Réseaux et télécommunications à l'université ABDERRAHMANE Mira de Béjaïa. Il relate notre expérience lors de notre stage au sein de Cevital Agro-Industrie.

Ce mémoire se concentre sur la mise en œuvre d'une solution de haute disponibilité (HSRP) pour un réseau LAN, en se basant sur l'exemple du réseau local de Cevital Agro-Industrie. Après avoir analysé l'infrastructure existante et identifié ses lacunes, nous avons proposé des solutions pratiques pour améliorer sa fiabilité. En utilisant une combinaison de protocoles tels que STP, OSPF et HSRP, nous avons conçu un réseau LAN robuste. Notre choix final du HSRP comme protocole principal reflète notre engagement à assurer la continuité des services critiques de l'entreprise. De plus, nous avons utilisé le logiciel Cisco Packet Tracer pour simuler et tester les configurations réseau, garantissant ainsi une mise en œuvre efficace. En résumé, ce mémoire offre une contribution significative à l'amélioration de la résilience et de la fiabilité du réseau local de Cevital Agro-Industrie.

Mots clés : Haute disponibilité, Réseau local, Cevital Agro-Industrie, STP, OSPF, HSRP, Cisco Packet Tracer, Infrastructure réseau, Fiabilité, Redondance matérielle.

Abstract :

This document is part of our final study project with a view to obtaining a master's degree in Telecommunications, with a specialization in Networks and telecommunications at the ABDERRAHMANE Mira University of Béjaïa. It relates our experience during our internship within Cevital Agro-Industrie.

This thesis focuses on the implementation of a high availability (HSRP) solution for a LAN, based on the example of the local network of Cevital Agro-Industrie. After analyzing the existing infrastructure and identifying its shortcomings, we proposed practical solutions to improve its reliability. Using a combination of protocols such as STP, OSPF, and HSRP, we designed a robust LAN. Our final choice of HSRP as the primary protocol reflects our commitment to ensuring the continuity of the company's critical services. Additionally, we used Cisco Packet Tracer software to simulate and test network configurations, ensuring effective implementation. In summary, this thesis makes a significant contribution to improving the resilience and reliability of the local network of Cevital Agro-Industrie.

Keywords : High availability, Local network, Cevital Agro-Industrie, STP, OSPF, HSRP, Cisco Packet Tracer, Network infrastructure, Reliability, Hardware redundancy.