République Algérienne Démocratique et Populaire
Ministére de l'Enseignement Supérieur et de la Recherche Scientifique

Université A. Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

MÉMOIRE DE MASTER

En Informatique

Option
Administration et Sécurité des Réseaux

Thème

Étude et mise en place de protocoles de haute disponibilité HSRP et GLBP, cas : CEVITAL

Présenté par :
M^{elle} *OUCHIHA Asma*
M^{elle} *MERSEL Nadjet*

Soutenu le 25 Juin 2023 devant le jury composé de :

Présidente	**Dr YESSAD Samira**	**U.A.MIRA-BÉJAIA**
Examinatrice	**Dr HOCINI Kenza**	**U.A.MIRA-BÉJAIA**
Encadrant	**Dr BENNAI Yani-Athmane**	**U.A.MIRA-BÉJAIA**
Co-encadrant	**Mr BERAZA Abderrahmane**	**U.A.MIRA-BÉJAIA**

Béjaia, Juin 2023.

⁕ *Remerciements* ⁕

A l'issue du cycle de notre formation nous tenons à remercier dieu le tout puissant.

Nous souhaitons également exprimer notre profonde gratitude envers notre encadrant ***Dr. BENNAI Yani-athmane****, ainsi que notre co-encadrant* ***Mr. BERAZA Abderrahmane****, pour leur encadrement infaillible, leurs conseils précieux, leur suivi attentif et surtout leur disponibilité tout au long de notre travail. Leur expertise et leur soutien ont été essentiels à notre réussite.*

Nous tenons à remercier chaleureusement notre encadrant de stage ***Mr. SLIMANI Mennad****, pour le temps précieux qu'il nous a consacré malgré ses propres responsabilités et préoccupations.*

Nos vifs remerciements vont également aux membres du jury qui ont accepté d'évaluer notre travail présenté.

Nous exprimons également notre gratitude envers tous les enseignants qui ont contribué à notre formation et nous ont transmis leurs connaissances.

Enfin, nous tenons à remercier sincèrement toutes les personnes qui, de près ou de loin, ont participé à la réalisation de ce mémoire. Votre contribution a été précieuse et nous vous en sommes profondément reconnaissants.

Que toutes les personnes impliquées dans notre formation soient sincèrement remerciées.

⁕ *Dédicaces* ⁕

Je dédie ce modeste travail
À l'homme qui est l'amour de ma vie, mon exemple éternel, celui qui s'est toujours sacrifié pour me voir réussir, je dédie ces mots à toi, mon cher père KHERREDDINE.
À ma chère mère FADILA, je souhaite exprimer mon amour pour elle, ainsi que ma reconnaissance pour les sacrifices qu'elle a consentis, sa confiance et sa tendresse immense.
À mes chers frères DANI, AOMAR et SAMOU, mes piliers qui m'ont toujours soutenu, je vous adresse mes remerciments sincères.
À ma jolie fleur, ma petite soeur adorée IMENE, je veux te dire combien tu compte pour moi.
À tous mes amis et camarades, en particulier LYDIA, ZAHOU, SARAH, TOTO, SONIA, IDIR et SELMA. Je garde en souvenir les bons moments et tout ce que nous avons vécu ensemble.
À mon cher biñome NADJET, celle qui m'a accompagné tout au long de notre parcours, je t'exprime ma gratitude.
À toute ma famille et à tous ceux qui ont contribué de près ou de loin à la réalisation de ce modeste travail, je leurs adresse mes profonds remerciments.

Asma

⁂ *Dédicaces* ⁂

Merci Allah de m'avoir donné la capacité d'écrire et de réflichir, la force d'y croire, la patience d'aller jusqu'au bout de mes rêves.

Je dédie ce modeste travail à celle qui m'a donné la vie, le symbole de tendresse, qui s'est sacrifiée pour mon bonheur et ma réussite, à ma mère NADIA.

A mon père ZAHIR, école de mon enfance, qui a veillé tout au long de ma vie à m'encourager, à me donner l'aide et à me protéger.

A mon cher frère BILLAL, mes chères soeurs KENZA et MARIA et ma chère tante MIRA, mes piliers qui m'ont toujours soutenu, je vous adresse mes remerciements sincères.

A mes chères grands parents je leurs souhaite une longue vie nchallah.

A tous mes ami(e)s, camarades, cousines et cousins qui ont été à mes cotés à tout moment, je garde en souvenir les bons moments et tout ce que nous avons vécu ensemble.

A mon cher binôme ASMA, celle qui m'a accompagné tout au long de notre parcours, je t'exprime ma gratitude.

A toute ma famille et à tous ceux qui ont contribué de près ou de loin à la réalisation de ce modeste travail, je leurs adresse mes profonds remerciements.

Nadjet

Table des matières

Table des figures

Liste des abréviations

ADG : Administrateur Directeur Général.

ARP : Address Resolution Protocol.

AVF : Active Virtual Forwarder.

AVG : Active Virtual Gateway.

BGP : Border Gateway Protocol.

CRC : Cyclic Redundancy Check.

CSMA/CD : Carrier Sence Multiple Access with Collision Detect.

DFC : Direction Finances et Comptabilité.

DHCP : Dynamic Host Cofiguration Protocol.

DRH : Direction Des Ressources Humaines.

FDDI : Fiber Distributed Data Interface .

GLBP : Gateway Load Balancing Protocol.

HSRP : Host Standby Routing Protocol.

IP : Internet Protocol .

ISO : International Standards Organisation.

IT : Information Technology.

LAN : Local Area Network.

MAC : Media Acess Control.

MAU : Multistation Access Unit.

MAN : Metropolitains Area Network.

OSI : Open Systems Interconnection.

OSPF : Open Shortest Path First.

PAN : Personnel Area Network.

RIP : Routing Information Protocol.

STP : Spanning Tree Protocol.

TCP : Transmission Control Protocol.

UDP : User Datagram Protocol.

VLAN : Virtual Local Area Network.

VRRP : Virtual Router Redundancy Protocol.

VTP : Vlan Trunking Protocol.

WAN : Wide Area Network.

Introduction générale

Avec le développement de l'informatique, la complexité et la performance des systèmes matériels et logiciels augmentent de plus en plus pour répondre aux besoins des utilisateurs. Ils envahissent tous nos quotidiens et sont aujourd'hui indispensables dans la plupart des grands domaines de l'industrie et de la vie quotidienne. [35]

La haute disponibilité et la stabilité d'un réseau d'entreprise sont nécessaire. Celles ci permettent d'assurer la qualité de service et le bon fonctionnement de ce dernier, et cela en intégrant des technologies et des protocoles pour l'assurer. Elles sont essentielles au succès des entreprises. [25]

L'architecture hiérarchique du réseau de CEVITAL ne tolère aucune panne de ses équipements car si un appareil tombe en panne, l'ensemble du réseau fonctionnera mal, ce qui entraînera une défaillance dans le réseau de l'entreprise, pour cela nous avons comme objectif de trouver une solution afin de garder le réseau en marche même en cas de panne.

Le déploiement d'un seul équipement qui prend en charge tout le réseau d'une entreprise de taille grandiose tel que le réseau de l'entreprise CEVITAL rend le réseau très lent ce qui n'est pas apprécié ni par l'utilisateur ni par l'entreprise.

Notre travail a pour raison de remédier aux manques que rencontre le réseau de l'entreprise CEVITAL, en se concentrant spécifiquement sur les technologies de haute disponibilité qui sont la redondance de passerelle et l'équilibrage de charge.

Notre mémoire sera décomposé en quatre chapitres, dans le premier chapitre nous allons définir des généralités sur les réseaux, le deuxième sera consacré pour l'entreprise CEVITAL ainsi que la problématique posée . Dans le troisième nous allons éclaircir notre sujet et parler des protocoles de haute disponibilité. Enfin nous allons terminer par la conception et réalisation des solutions proposées.

Chapitre 1

Généralités sur les réseaux informatiques

1.1 Introduction

Aujourd'hui, il est pratiquement indispensable de connaitre les concepts de base des réseaux informatiques, car ils sont présents dans tous les domaines de la vie. Dans ce chapitre, nous allons présenter les concepts de réseau informatique ainsi quelques notions théoriques que nous utiliserons tout au long de notre étude pour mener à bien notre travail.

1.2 Définition d'un réseau informatique

Un réseau est un moyen de communication qui permet à des individus ou à des groupes de partager des informations et des services.

La technologie des réseaux informatiques constitue l'ensemble des outils qui permettent à des ordinateurs de partager des informations et des ressources.

Un réseau est constitué d'équipements appelés noeuds. Ces réseaux sont catégorisés en fonction de leur étendue et de leurs domaines d'application.

Pour communiquer entre eux, les noeuds utilisent des protocoles, ou langages compréhensibles par tous.[20]

1.3 Les catégories de réseau informatique

On distingue quatre catégories de réseaux informatiques selon leurs tailles et leurs étendus.[11,20,38]

1.3.1 Réseau personnel (Personal Area Network)

PAN est la plus petite étendue des réseaux informatiques, avec portée de connectivité allant jusqu'à 10 mètres, ce réseau peut inclure les claviers et les souris d'ordinateur sans fil, des écouteurs compatibles Bluetooth, des imprimantes sans fil etc.

1.3.2 Réseau local (Local Area Network)

De taille supérieure que le réseau personnel (PAN), avec une portée de connectivité de quelques dizaines à quelques centaines de mètres. Le Local Area Network(LAN), en français Réseau Local d'Entreprise (RLE). Il relie des ordinateurs, des serveurs, etc, il est généralement utilisé pour le partage de ressources communes comme des périphériques, des données ou des applications.

1.3.3 Réseau métropolitain (Métropolitain Area Network)

Le réseau métropolitain ou Metropolitain Area Network(MAN) est également nommé réseau fédérateur. Il assure des communications sur plus longues distances, interconnectant souvent plusieurs réseaux LAN. Il peut servir à interconnecter, par une liaison privée ou non, différents bâtiments distants de quelques dizaines de kilomètres.

1.3.4 Réseau étendu (Wide Area Network)

Les étendues de réseau les plus conséquents sont classés en Wide Area Network(WAN). Constitués de réseaux de type LAN, voir MAN, les réseaux étendus sont capables de transmettre les informations sur des milliers de kilomètres à travers le monde entier. Le WAN le plus célèbre est le réseau public Internet dont le nom provient de cette qualité : Inter Network ou interconnexion de réseaux.

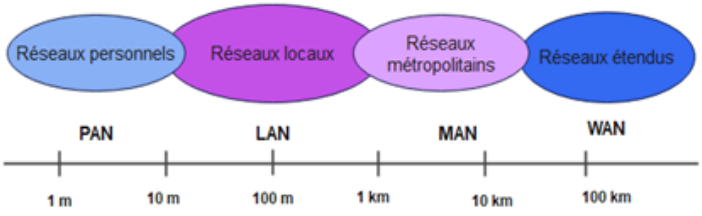

FIGURE 1.1 – Catégories des réseaux informatiques.[18]

1.4 Les topologies de réseau informatique

Les réseaux se distinguent par leurs structures, ou plus précisément par leurs topologies. La topologie d'un réseau décrit comment ses noeuds sont connectés. Il existe deux types de topologies :

1.4.1 Les topologies physiques

Elles décrient la manière dont les équipements du réseau sont connectés physiquement entre eux grâce à des lignes de communications (câbles réseaux) et des éléments matériels (cartes réseaux, etc). [11,14,20]
Il existe plusieurs topologies parmi eux nous citons :

1.4.1.1 Le bus

Une topologie en bus est la configuration la plus simple d'un réseau. En fait, dans une topologie en bus, tous les ordinateurs sont connectés à la même ligne de transmission par des câbles (généralement coaxiaux).

Le mot "bus" fait référence aux câbles physiques qui connectent les machines sur un réseau.

1.4.1.2 L'étoile

Dans un réseau en étoile, chaque noeud du réseau est connecté à un noeud central via des câbles RJ45. Ce noeud est un appareil qui reçoit un signal de données via l'une de ses entrées et transmet ce signal à votre ordinateur ou à chacune des autres entrées auxquelles votre ordinateur est connecté.

1.4.1.3 L'anneau

Une topologie en anneau relie chaque machine à la machine suivante. Les machines sont connectées à des répartiteurs appelés MAU (Multi Station Access Unit), ce dernier gère la communication entre différentes machines en allouant du temps de conversation à chacune.

1.4.1.4 L'arbre

Dans cette topologie, un appareil central, souvent appelé "noeud racine" ou "noeud central", est connecté à plusieurs appareils de niveau inférieur, qui à leur tour peuvent être connectés à d'autres appareils de niveau inférieur.

1.4.2 Les topologies logiques

Elles expliquent comment les différents éléments d'information (données) circulent à travers les lignes de communication pour atteindre leurs destinations, ou comment identifier où les collisions peuvent se produire. [13,19,30]
Parmi les topologies logiques les plus courantes nous citons :

1.4.2.1 Ethernet

C'est une norme LAN qui respecte les spécifications de la norme 802.3 et utilise la méthode CSMA/CD pour définir les réseaux locaux. Son principe est basé sur un bus physique (commun) comme support de transmission. C'est-à -dire que tous les éléments actifs sont connectés à un seul support de transmission. Les réseaux Ethernet communiquent via un protocole appelé CSMA/CD.

1.4.2.2 Token Ring

Token Ring est basé sur une topologie en anneau qui utilise la méthode d'accès par jeton. Avec cette technologie, seules les stations disposant de jetons ont des droits d'émettre. Si une station veut émettre, elle doit d'abord attendre jusqu'à la réception d'un jeton. Dans un réseau Token Ring, chaque noeud de réseau contient une unité d'accès multi-station (MAU) qui peut recevoir des connexions de stations. Un signal circulant est joué à partir de chaque MAU. La mise en place d'un réseau Token Ring est couteux en place et la défaillance d'une station MAU provoque un disfonctionnement total du réseau.

1.4.2.3 FDDI (Fibre Distributed Data Interface)

La technologie LANFDDI (Local Area Network Fibre Distributed Data Interface) est une technologie d'accès réseau utilisant des câbles fibre optique. Le FDDI se compose de deux anneaux : un anneau primaire et un anneau secondaire qui sert à rattraper les erreurs de l'anneau primaire. Le FDDI utilise un anneau à jeton qui sert à détecter et à corriger les erreurs. Ce qui fait que si une station MAU tombe en panne, le réseau continuera toujours son fonctionnement.

1.5 Le Modèle OSI (Open Système Interconnections)

Le modèle OSI est un modèle d'architecture de réseau standard à sept couches développé par l'organisation ISO en 1984. Les couches peuvent être regroupées en trois blocs fonctionnels.[20,22]

- Couches inférieures (1, 2 et 3) : assurent la transmission et le transfert d'informations sur les réseaux via les médias.
- Couches moyennes (4 et 5) : gèrent les communications et les ressources nécessaires pour échanger des messages entre les terminaux.

- Couches supérieures (6 et 7) : traitent les données échangées.

OSI est un modèle théorique, mais pour pouvoir identifier un protocole, un appareil ou des données à l'une de ses sept couches, nous devons savoir qu'il est essentiel dans notre interaction avec la communauté des réseaux.

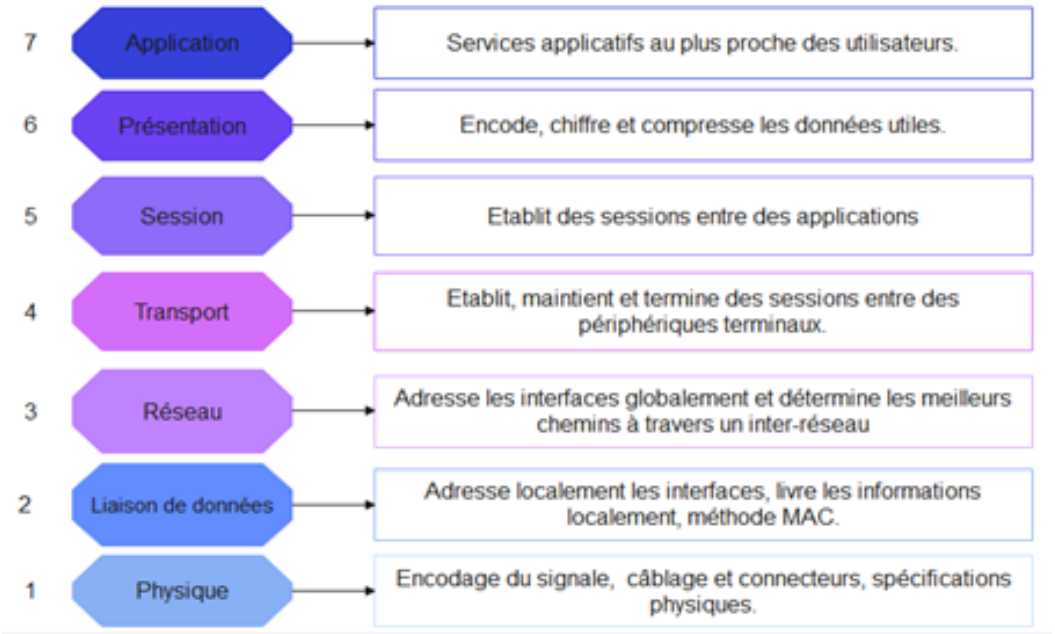

FIGURE 1.2 – Les couches du modèle OSI.[10]

Notre travail se base sur les trois couches inférieurs qui sont :

1.5.1 La couche physique

Elle a pour rôle la transmission bit à bit sur le support, entre l'émetteur et le récepteur, des signaux électriques ou lumineux qui codent des données numériques (0 ou 1).

Définissant le mode de propagation de signaux, elle gère au besoin les circuits physiques, des matériels comme les modems (modulateur/démodulateur), les répéteurs ou la connexion des cartes réseau, RJ45 par exemple, ce placent à ce niveau.

1.5.2 La couche liaison de données

Cette couche convertit les données numériques en signaux. Les bits de données sont organisés en trames.Elle crée un en-tête qui identifie l'expéditeur et le destinataire par adresse physique qui est également appelée Une adresse MAC, c'est un identifiant unique et propre à la carte réseau de l'ordinateur. A ce niveau de couche, certains problèmes de transmission sont détectés en utilisant

un code de redondance cyclique CRC (Cyclic Redundancy Check). A la transmission, le récepteur recalcule le CRC s'il est différent de celui envoyé, la trame sera rejetée.

1.5.3 La couche réseau

Lorsqu'il en existe plusieurs, le choix du meilleur chemin pour atteindre le destinataire est géré au niveau de cette couche. Alors que l'adresse physique sert à identifier un périphérique local, une adresse logique permet de référencer un composant de manière globale. Pour cela, certains protocoles identifient les périphériques du réseau en les référençant par un numéro de réseau, ainsi qu'un numéro de poste dans ce réseau.

Pour atteindre un destinataire, un coût est calculé qui peut dépendre de plusieurs paramètres (nombre de réseaux â traverser, durée du transport, coût de la communication, encombrement de la ligne,etc). C'est en comparant les différents coûts qu'un chemin peut étre qualifié de meilleur qu'un autre.

En fonction des protocoles, le bloc peut être nommé message, datagramme, cellule ou même paquet, comme dans Internet Protocol (IP).

1.6 Transmission Control Protocol/Internet Protocol (TCP/IP).

Définition

TCP/IP (Transmission Control Protocol/Internet Protocol). Cette désignation est tirée des noms des deux principaux protocoles de la suite, TCP et IP. c'est un ensemble de protocoles qui représente toutes les règles de communication sur Internet et repose sur le concept d'adressage IP, c'est-à-dire attribuer des adresse IP à toutes les machines du réseau pour pouvoir partager des paquets de donnée. [34]

La suite des protocoles TCP/IP est conçue d'assurer le routage, le contrôle d'erreurs de transmissions en utilisant un système d'adresse.

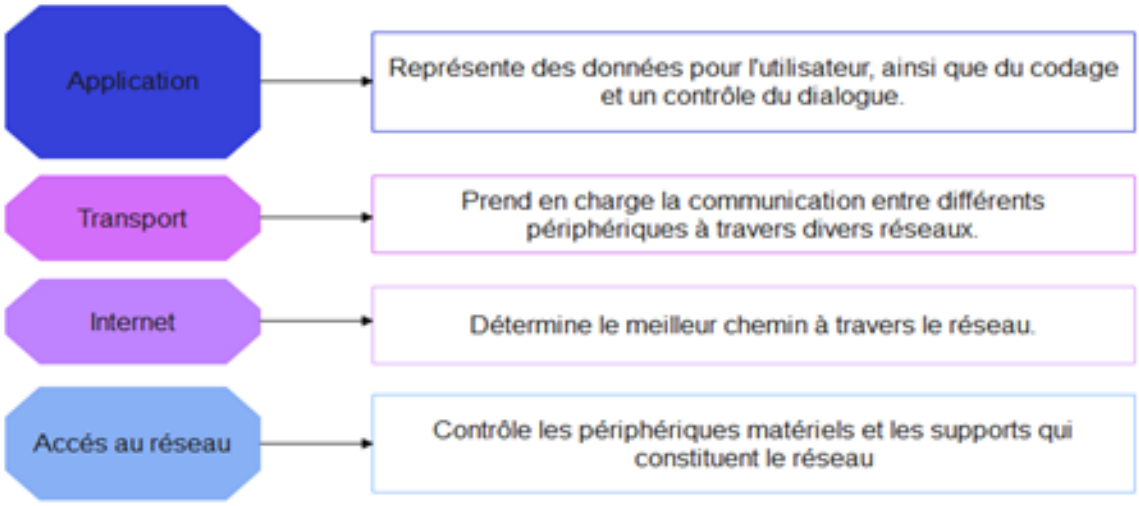

FIGURE 1.3 – Les quatre couches du modèle TCP/IP. [10]

1.7 La comparaison entre le modèle OSI et TCP/IP

Le modèle TCP/IP est une approche pratique dérivée du modèle OSI qui est un modèle théorique de référence. Par conséquent, le modèle TCP/IP est le plus utilisé dans les réseaux LAN. La différence que nous pouvons facilement observer entre les deux modèles est le nombre de couches, le modèle OSI se compose de sept couches et le modèle TCP/IP de quatre couches. La différence est par rapport au type de communications, orienté connexion ou sans connexion. Dans le modèle OSI, la couche réseau autorise les deux types de communication, mais la couche transport n'autorise que la communication orientée connexion. Le modèle TCP/IP n'a qu'un seul mode au niveau du réseau (sans connexion), mais au niveau du transport il offre les deux types de communications et le choix revient à l'utilisateur. C'est très important. Surtout pour les protocoles de requête/réponse très simples.[6]

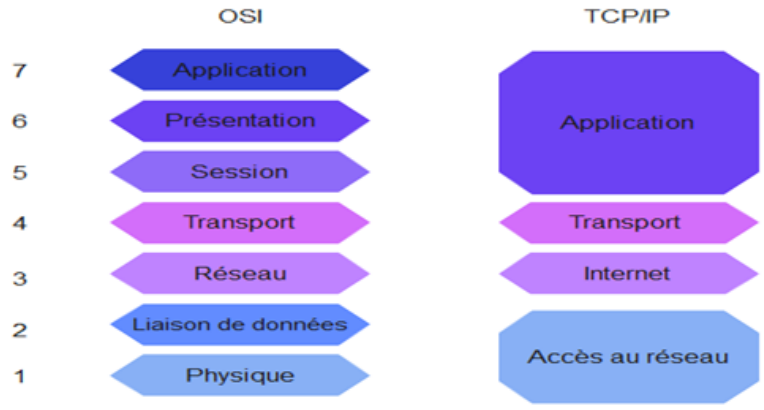

FIGURE 1.4 – La comparaison entre les couches du modèle OSI et TCP/IP.[10]

1.8 Les équipements d'un réseau

Les équipements d'un réseau informatique sont nombreux , parmi eux nous mentionnons : [34]

1.8.1 Le Hôte

Les hôtes sont des unités directement connectées à un segment de réseau, nous pouvons les retrouver sous forme d'ordinateurs, de serveurs, de scanners ou d'imprimantes.

1.8.2 Le commutateur (Switch)

Un commutateur est un équipement qui connecte plusieurs câbles ou fibres dans un réseau informatique ou un réseau de télécommunications, ils permettent de créer des circuits virtuels et d'envoyer des informations des destinations précises au sein d'un réseau. Les commutateurs aident à protéger les informations envoyées sur les réseaux.

1.8.3 Le routeur

Sont les machines clés d'internet, ils sont des dispositifs qui permettent de choisir le chemin qu'un message va emprunter. Votre poste de travail envoie la requête au routeur le plus proche (en général la passerelle du réseau) qui choisit la machine la plus proche à laquelle il va faire circuler la demande de telle façon que le chemin choisit soit le plus court.

Autres équipements :

- **La passerelle (Gateway)** : qui permet de relier des réseaux locaux de types différents.
- **Le répéteur :** qui permet de générer un signal.
- **Le concentrateur (hub) :** qui permet de connecter entre eux plusieurs hôtes.
- **Le pont (Bridge) :** qui permet de relier des réseaux locaux de même type.
- **Le B-routeur :** qui associe les fonctionnalités d'un routeur et d'un pont.

1.9 L'adressage

Dans les réseaux IP , chaque interface possède une adresse IP, soit définie par l'administrateur réseau, soit attribuée dynamiquement à l'aide d'un protocole tel que DHCP. [22,38]

1.9.1 Le IPv4

Une adresse IP est un numéro unique qui identifie chaque ordinateur connecté à un réseau. Ce nombre est divisé par 4 avec 8 bits allant de 0 à 255 séparés par des points. Une adresse IP se

compose de deux parties, une partie réseau et une partie hôte. Le premier identifie le réseau auquel la machine est connectée et le second identifie la machine connectée à ce réseau. Pour distinguer ces deux parties, chaque adresse est associée à un masque de sous-réseau, permettant de définir le réseau auquel appartient l'adresse.

FIGURE 1.5 – Les classes d'adresses.[18]

Les adresses IP sont découpées en plusieurs classes :

- Les adresses IP de classe A : 0 à 127.
- Les adresses IP de classe B : 128 à 191.
- Les adresses IP de classe C : 192 à 223.
- Les adresses IP de classe D : 224 à 239.
- Les adresses IP de classe E : 240 à 255.

Les adresses privées : Il existe des adresses privées, dans chaque classe

- 10.0.0.0 à 10.255.255.255.
- 172.16.0.0 à 172.31.255.255.
- 192.168.0.0 à 192.168.255.255.

Une adresse IP privée n'est pas visible sur internet, au contraire d'une adresse IP publique.

1.9.2 Le IPv6 :

IPv6 est une amélioration pour corriger tous les défauts de IPv4. Cette nouvelle version fournit un format d'en-tête simplifié avec un plan d'adressage étendu de 16 octets avec des possibilités d'extension, des fonctionnalités d'authentification et de confidentialité. L'adressage IPv6 est réparti en trois classes :

- La classe Unicast : utilisée pour l'envoi d'un datagramme vers un noeud unique.

- La classe Cluster : identifie un groupe de noeuds ayant en commun un préfixe d'adresse.
- La classe Multicast : utilisée pour l'envoi à tous les membres d'un groupe.

L'adresse Broadcast a été supprimée.

1.9.3 La comparaison entre les protocoles IPv4 et IPv6

Les adresses IPv6 sont plus longues et se présentent dans un format différent pour assurer plus de possibilités et de configurations uniques. L'IPv6 est un système 128 bits, les adresses se présentent sous la forme de séquences alphanumériques séparées par le signe des deux-points. De son coté l'IPv4 est basée sur une architecture 32 bits utilisant une chaine de nombres séparées entre eux par un point.[22]

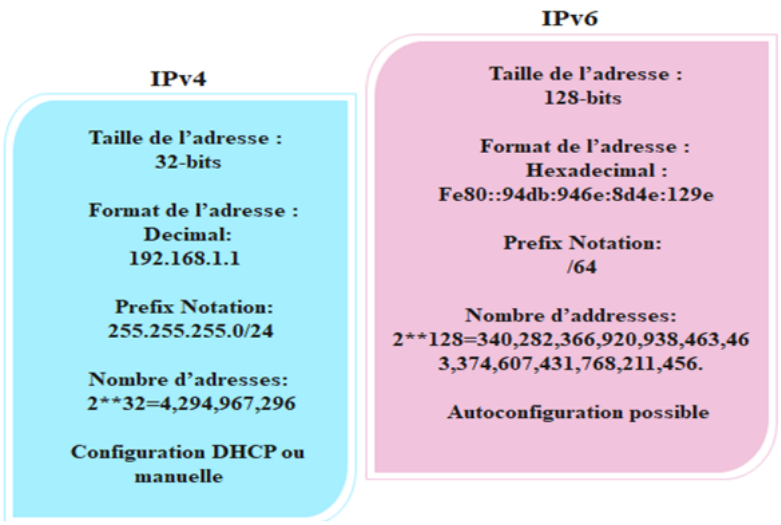

FIGURE 1.6 – La différence entre IPv4 et IPv6. [5]

1.10 Le routage

Le routage de paquets consiste à utiliser des adresses IP pour trouver le chemin vers une station de destination. Si un paquet envoyé d'une machine à sa destination n'est pas trouvé sur le réseau ou le sous-réseau local, il doit être transmis à un routeur qui le rapproche de sa destination. Par conséquent, chaque station du réseau doit avoir une adresse de routeur par défaut. L'ordinateur source applique un masque de sous-réseau (Netmask) pour savoir si un routage est nécessaire. Par conséquent, chaque routeur doit connaitre l'adresse du routeur suivant si la machine de destination n'est pas sur le réseau ou le sous-réseau auquel il est connecté. Un routeur associe au moins deux interfaces réseau avec une seule adresse IP sans connecter chaque réseau. Les tables de routage doivent être maintenues de manière statique ou dynamique. [17,22,37]

1.10.1 Le routage statique

Le routage consiste à configurer manuellement, dans chaque routeur d'un réseau, une liste des adresses de destination spécifiques et des chemins associés à ces adresses.

- L'interface de sortie ou l'adresse IP du prochain saut.
- Le cout associé.
- Eventuellement le masque de sous-réseau.

Ce type de routage est utile lors de la configuration de routeurs à la périphérie du réseau qui se connectent au coeur via un lien unique, mais il est difficile à utiliser dans les grands réseaux maillés en raison de la quantité de données à traiter. Dans la plupart des cas, il ne permet pas non plus aux routeurs de modifier le routage lorsqu'une défaillance de liaison est détectée. Les administrateurs réseau doivent apporter des modifications manuellement (ajouter ou supprimer des routes) sur chaque routeur.

1.10.2 Le routage dynamique

Contrairement au routage statique, dans le routage dynamique, en configurant le protocole adéquat, le remplissage de la table de routage se fait automatiquement, ce type de routage est utilisé dans les grands réseaux. Le routage dynamique permet également à la table de routage de changer automatiquement en cas de perte de connectivité au niveau du routeur. Il permet également de choisir le meilleur itinéraire disponible pour atteindre une destination.

1.10.3 Protocoles de routage

Un protocole de routage est un ensemble de règles qui spécifient comment les routeurs identifient et transmettent les paquets d'une source vers une destination. Il existe plusieurs protocoles de routage, nous citons :

1.10.3.1 OSPF (Open Shortest Path First)

Le protocole OSPF a pour but de trouver les chemins les plus courts pour atteindre différentes destinations dans un réseau IP. Pour cela, les routeurs OSPF communiquent entre eux en échangeant des messages contenant des informations sur les liens réseau, comme la bande passante, la charge, la fiabilité et le coût. Ces informations permettent de construire une représentation complète de la topologie du réseau. En se basant sur ces données, OSPF calcule les routes les plus efficaces et les plus rapides vers chaque destination.

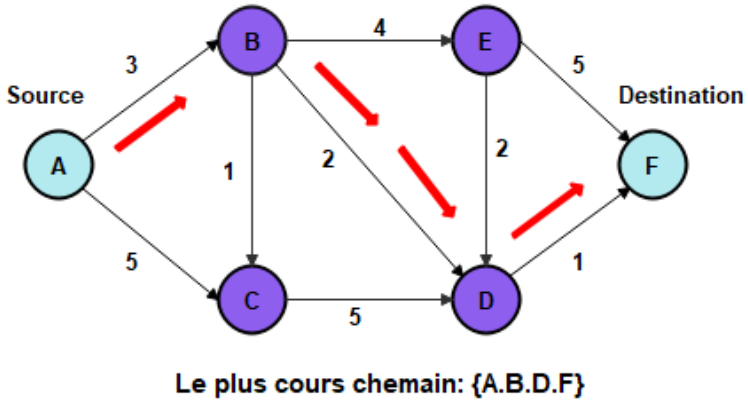

FIGURE 1.7 – schéma de principe de protocole OSPF.[27]

1.10.3.2 RIP (Routing Information Protocol)

C'est un protocole de vecteur à distance qui utilise des techniques de diffusion périodiques. Le transfert se fait par des datagrammes UDP envoyès toutes les 30 secondes, la distance est exprimèe en sauts exprimès sous la forme d'un entier compris entre 1 et 15, la distance infinie est exprimèe en 16. Si une route n'est pas annoncèe en au moins 3 minutes la distance correspondante devient infinie.

1.10.3.3 BGP (Border Gateway Protocol)

C'est un protocole de routage entre systèmes autonomes. Ce protocole permet d'empêcher les réseaux autonomes, même les plus courts, soient utilisés comme un passage par d'autres systèmes autonomes sans l'accord de l'opérateur privilégié.

1.10.4 Le STP (Spanning Three Protocol)

C'est un protocole réseau utilisé pour définir des topologies sans boucle dans les réseaux locaux commutés. STP est activé par défaut sur les commutateurs Cisco pour créer automatiquement des chemins sans boucle entre les commutateurs.[25]

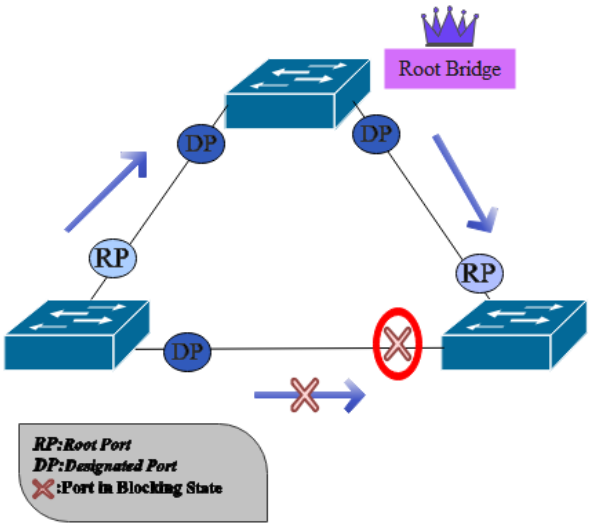

FIGURE 1.8 – Schéma de fonctionnement du protocole STP.[36]

1.11 Les Virtuals LAN (VLAN)

1.11.1 La définition

Un VLAN (Virtual Local Area Network) est un sous-réseau logique de périphériques au sein d'un domaine de diffusion. Ces réseaux sont apparus comme une nouvelle fonctionnalité de gestion de réseau avec le développement des commutateurs.[3,34,39]

La virtualisation LAN (VLAN) consiste à séparer l'infrastructure physique et les services de transmission à haut débit fournis par les commutateurs. L'idée de base des VLAN est de diviser un seul LAN en réseaux logiques complètement disjoints.

Cette technologie offre plusieurs nouvelles solutions pour la segmentation et la protection des réseaux locaux. Les VLAN sont normalisés selon la spécification IEEE 802.1Q.

1.11.2 Les types de VLANs

Les VLANs diffèrent selon les informations utilisées pour regrouper les stations. Il en existe trois modèles

1.11.2.1 Un VLAN de niveau 1 (port-based VLAN en anglais)

Les VLAN de niveau 1 également appelés VLAN par port, définissent des réseaux virtuels en fonction des commutateurs ou des ports connectés des commutateurs. Avec les VLANs basés sur les ports, la configuration de VLAN auquel appartient chaque port de commutateur se fait manuellement.

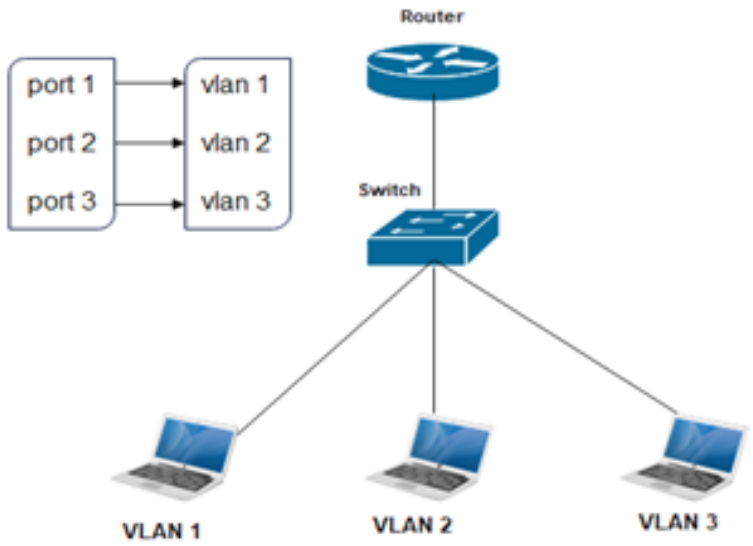

FIGURE 1.9 – Schéma montrant un VLAN du niveau 1.[39]

1.11.2.2 Un VLAN de niveau 2 (VLAN MAC, VLAN par adresse IEEE ou en anglais MAC Address-Based VLAN)

Un VLAN de niveau 2, est construit en définissant un réseau virtuel en fonction de l'adresse MAC de la station. Ce type de VLAN est beaucoup plus flexible que les VLAN par port car le réseau est indépendant de l'emplacement de la station.

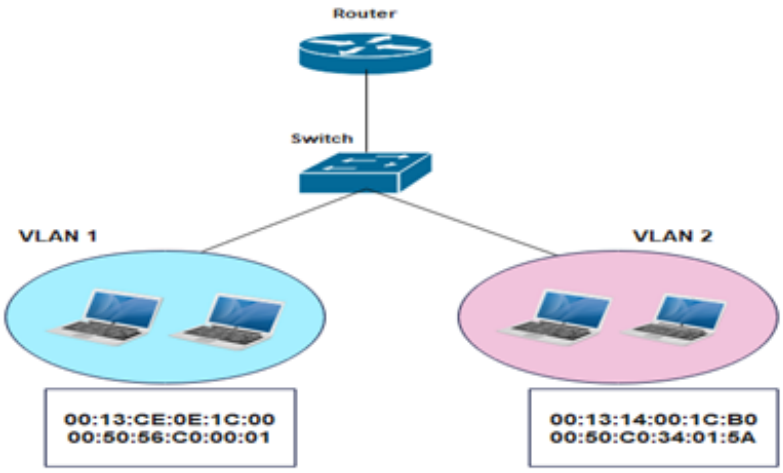

FIGURE 1.10 – Schéma montrant un VLAN du niveau 2.[39]

1.11.2.3 Un VLAN de niveau 3

VLAN de niveau 3 également appelé VLAN par adresse IP a le même principe que les VLANs de niveau 2 sauf que l'on indique les adresses IP (ou une plage d'IP) qui appartiennent à un VLAN

précis. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de changement de station.

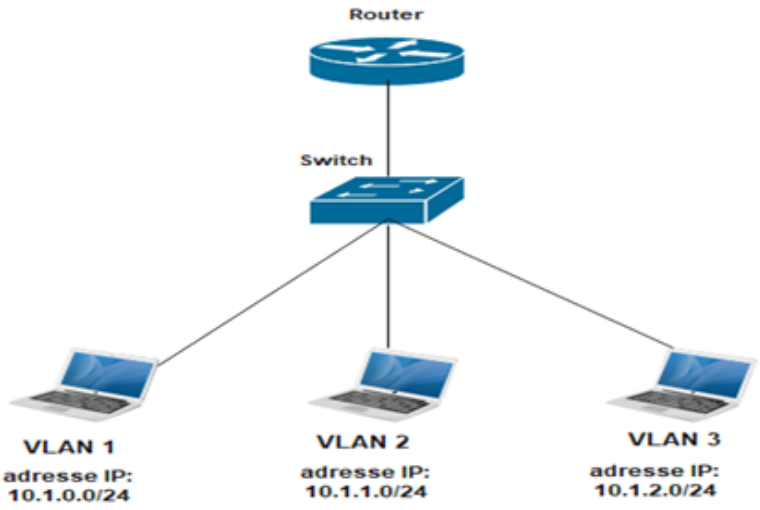

FIGURE 1.11 – Schéma montrant un VLAN du niveau 3.[38]

1.11.3 Les avantages des VLANs

Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants : Plus de souplesse pour l'administration et les modifications du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs , Gain en sécurité car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées ainsi que la réduction de la diffusion du trafic sur le réseau.

1.12 VTP (Vlan Trunking Protocol)

C'est un protocole client/serveur de la couche 2, qui permet de configurer des VLANs sur un commutateur en mode serveur pour propager automatiquement ces configurations à d'autres commutateurs en mode client du réseau. VTP assure la cohérence de la configuration VLAN en gérant l'ajout, la suppression et la modification des VLANs sur plusieurs commutateurs du réseau.[7,37]
Il existe trois modes de configuration possible :

1.12.1 Le mode serveur

Le commutateur propage les VLANs et leurs paramètres aux commutateurs en mode 'client' appartenant au même domaine VTP. Le serveur stocke les informations des VLANs dans sa NVRAM.

A ce niveau les VLANs peuvent être crées, supprimer ou modifier tout en propageant les changements à d'autres commutateurs en mode client.

1.12.2 Le mode client

Ne permet aucune modification par l'administrateur sur les VLANs, le commutateur traite les messages VTP reçus et les transmet aux voisins.

1.12.3 Le mode transparent

Le switch en mode transparent permet à l'administrateur de faire toute modification seulement sur les VLANs qui lui appartient sans les diffuser aux commutateurs voisins.

Le schéma suivant montre le fonctionnement de VTP serveur et VTP client.[Figure 1.12]

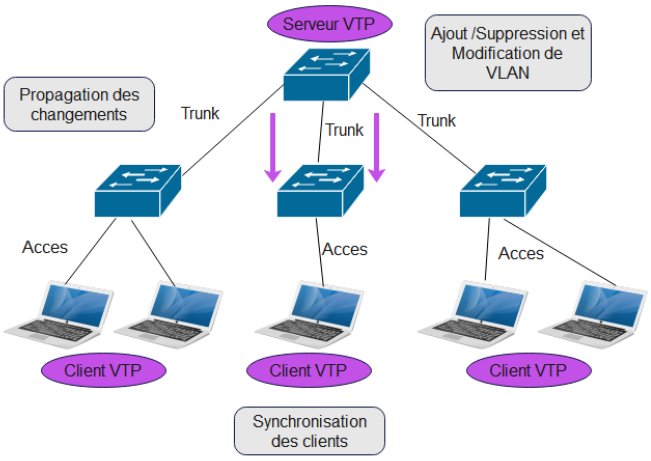

FIGURE 1.12 – Schéma de fonctionnement du protocole VTP

1.13 Conclusion

Dans ce chapitre nous avons présenté les notions de base d'un réseau informatique pour avoir une idée claire sur son ensemble de concepts et son fonctionnement, ce qui nous permettra d'aborder notre thème. Dans le chapitre suivant nous allons présenter l'organisme d'accueil.

Chapitre 2

Présentation de l'organisme d'accueil

2.1 Introduction

« *Voir grand, commencer petit et aller vite* », dite par le fondateur du groupe Cevital Mr. ISSAD REBRAB.

Le succès et le développement d'une entreprise dépendent de son histoire, de son organisation et des différentes personnes qui la dirigent.

Dans ce chapitre, nous présentons le groupe Cevital, les noms des différents départements qui composent cette entreprise, et quelques informations nécessaires que nous allons utiliser pour réaliser notre travail. En effet une problématique sera annoncée à la fin de ce chapitre.

2.2 Présentation de l'organisme d'accueil

Le groupe Cevital est une conglomération algérienne de l'agroalimentaire, de la grande distribution, de l'industrie et des services. Fondé en 1998 par l'entrepreneur Issad Rebrab, Cevital est le premier groupe privé algérien à l'implantation internationale et la troisième entreprise algérienne en chiffre d'affaires. Elle emploie 18 000 personnes. [26]

Cevital agro-industrie est le leader du secteur agro-alimentaire en algérie, elle couvre les besoins nationaux et a permis de faire passer l'Algérie du stade importateur á celui d'exportateur pour les huiles, les margarines et le sucre.

FIGURE 2.1 – Logo de l'entreprise. [8]

2.3 Historique et évolution du groupe Cevital

Cevital est un groupe familial basé sur une histoire, un parcours et les valeurs qui ont fait son succès et sa réputation. Elle a été la première entreprise privée algérienne à investir dans un large éventail d'activités, elle a affranchi des étapes historiques importantes pour atteindre sa taille et son prestige actuel. Industrie Agroalimentaire et Grande Distribution, Electronique et Electroménager, Sidérurgie, Industrie du Verre Plat, Construction Industrielle, Automobile, Services, Média, etc. Le Groupe Cevital s'est construit à travers des investissements fondés sur l'idée forte de constituer un ensemble économique.

Cette entreprise à traversé d'importantes étapes historiques pour atteindre la taille et la célébrité dont elle jouit aujourd'hui et ce tout en continuant à oeuvrer dans la création d'emplois et de richesses en Algérie. [26]

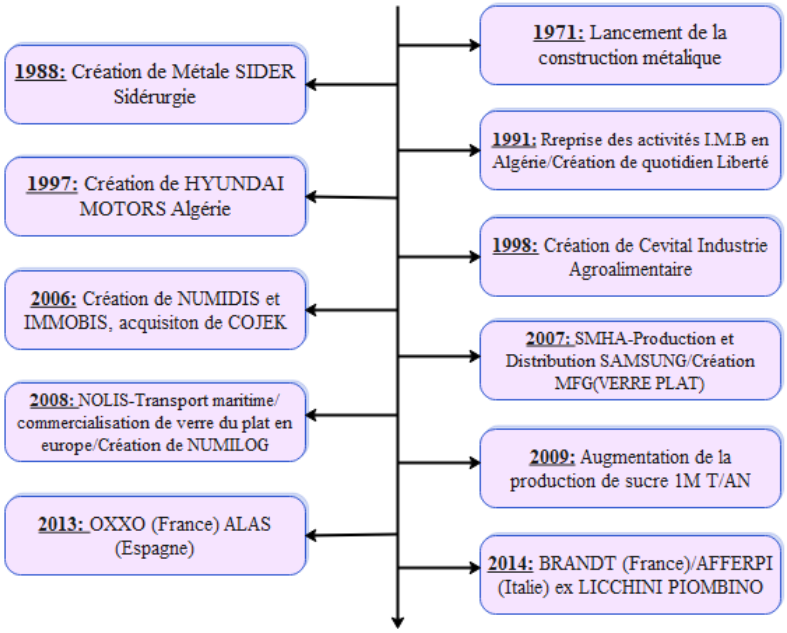

FIGURE 2.2 – L'évolution du groupe Cevital à travers le temps.[8]

2.4 Les valeurs du groupe Cevital

Cevital est un Groupe familial qui s'est bâti sur les valeurs suivantes[26] :

- Intégrité et transparence.
- Ecoute et respect.
- Solidarité et persévérance.
- Initiative et persévérance.

2.5 Infrastructure de groupe Cevital

Cevital agro-industrie dispose de plusieurs unités de production ultramodernes [26] :

- Deux raffineries de sucre.
- Une unité de sucre liquide.
- Une raffinerie d'huile.
- Une margarinerie.
- Une unité de conditionnement d'eau minérale (se situe à Tizi-Ouzou).
- Une unité de fabrication et de conditionnement de boissons.
- Rafraîchissantes (site EL-Kseur).
- Une conserverie.
- Silos portuaires.

2.6 Situation géographique

CEVITAL Agro-industrie se situe dans le nouveau quai du port de Bejaia, à 3km Sud-ouest de la ville, à proximité de la RN 26 et la RN 9. Cette situation géographique de l'entreprise lui profite bien étant donné qu'elle lui confère l'avantage de la proximié économique.

En effet, elle se situe très proche du port et de l'aéroport de Bejaia. Le complexe s'étend sur une superficie de 45 000 m2 (le plus grand complexe privé en Algérie). Il a une capacité de stockage de 182 000 tonnes/an (Silos portuaire), et un terminal de déchargement portuaire de 200 000 tonnes/heure (réception de matière première). Comme elle possède un réseau de distribution de plus de 52 000 points de vente sur tout le territoire national

FIGURE 2.3 – Vue satellitaire du complexe Cevital.[9]

2.7 L'architecture de réseau Cevital

Un réseau informatique local a été mis en place pour faciliter les échanges d'informations entre les différents départements, unités et services administratifs. Cevital dispose d'un réseau interne assez étendu pour relier les différents départements, unités de production et directions du complexe.

Il peut être divisé en plusieurs parties telles que le backbone du réseau, le pare-feu, la DMZ (zone démilitarisée), la couverture Wifi, les routeurs, les commutateurs et les centres de données (oú résident les serveurs de l'entreprise).

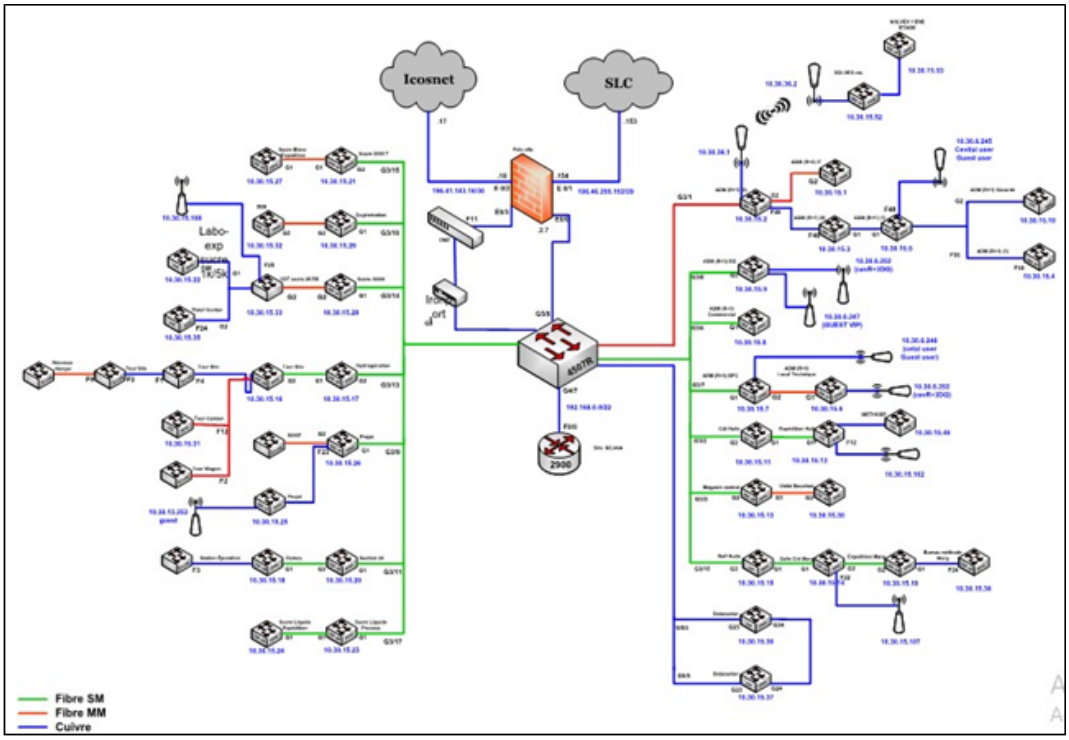

FIGURE 2.4 – L'architecture générale du réseau Cevital.

Le réseau local de complexe se divise en trois couches, qui sont :

2.7.1 Couche Core (Distribution)

L'épine dorsale se compose de commutateurs Catalyst situés dans le centre de données du bâtiment, connectés aux pare-feu et aux routeurs via des câbles RJ45, et connectés aux commutateurs d'accès via la fibre optique, augmentant le débit á diverses stations. Cette partie est la plus sensible car elle est connectée à tous les périphériques du réseau.

2.7.2 Couche d'accès

Cette couche se compose de commutateurs répartis à divers emplacements locaux dans le bâtiment. Le gestionnaire de réseau de Cevital utilise des VLANs pour partager l'accès aux utilisateurs, en s'assurant que chaque site local (étage du bâtiment) contient un ou plusieurs VLAN.

2.7.3 Couche en cascade

Au niveau de cette couche, les commutateurs sont interconnectés et connectés aux commutateurs d'accès pour fournir un accès aux utilisateurs. Au sein du commutateur, les VLANs vous permettent de définir plusieurs sous-réseaux pour différents services de l'entreprise.

2.8 L'organigramme de Cevital

L'organigramme ci-dessous donne un aperçu des différentes institutions du complexe Cevital. Le Complexe Cevital est composé de 13 services principaux dont la mission est de veiller à la bonne exécution de leurs missions.

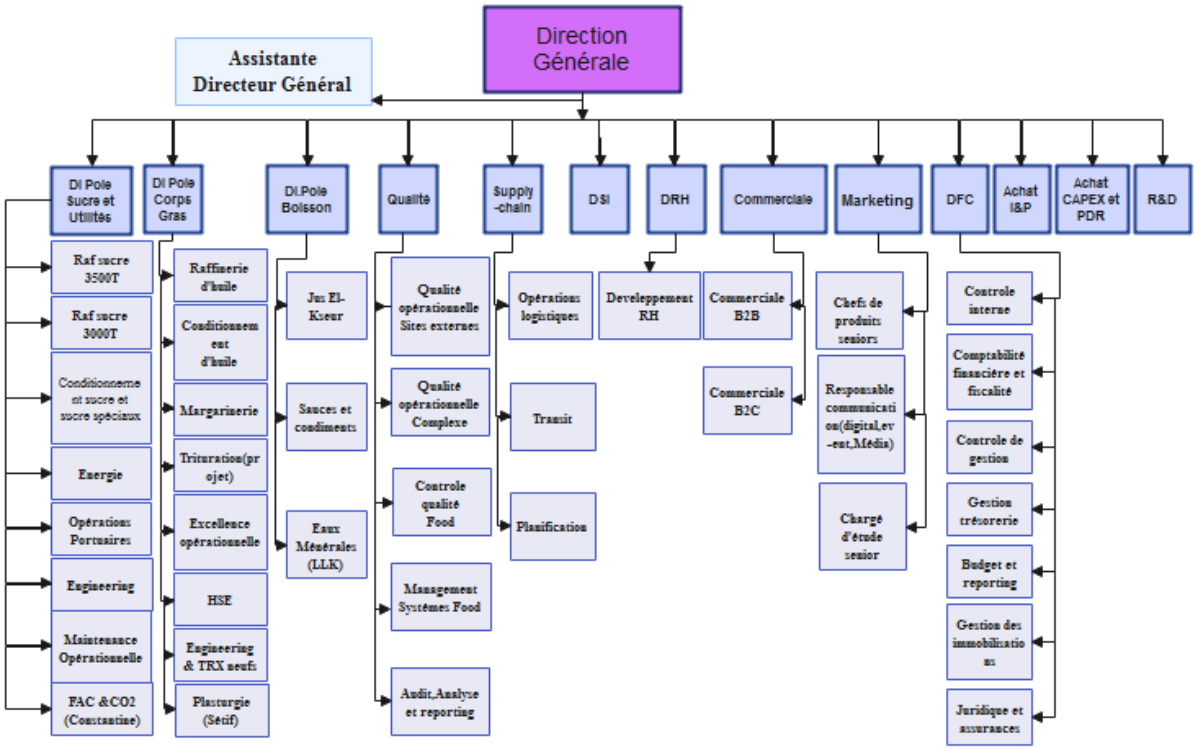

FIGURE 2.5 – Diagramme général du complexe Cevital.

2.9 Présentation de service informatique

Nous avons effectué notre stage au niveau du département Réseau et Télécom de la direction des systèmes d'information (DSI), cette dernière assure la mise en oeuvre des moyens et des technologies de l'information nécessaire pour améliorer l'activité, la stratégie et la performance de l'entreprise, elle doit ainsi veiller à la cohérence des moyens informatiques et de la communication mises à la disposition des utilisateurs, à leur maîtrise technique et à leur disponibilité et opérationnalité permanentes et ceux en toute sécurité. La figure est ci-dessous

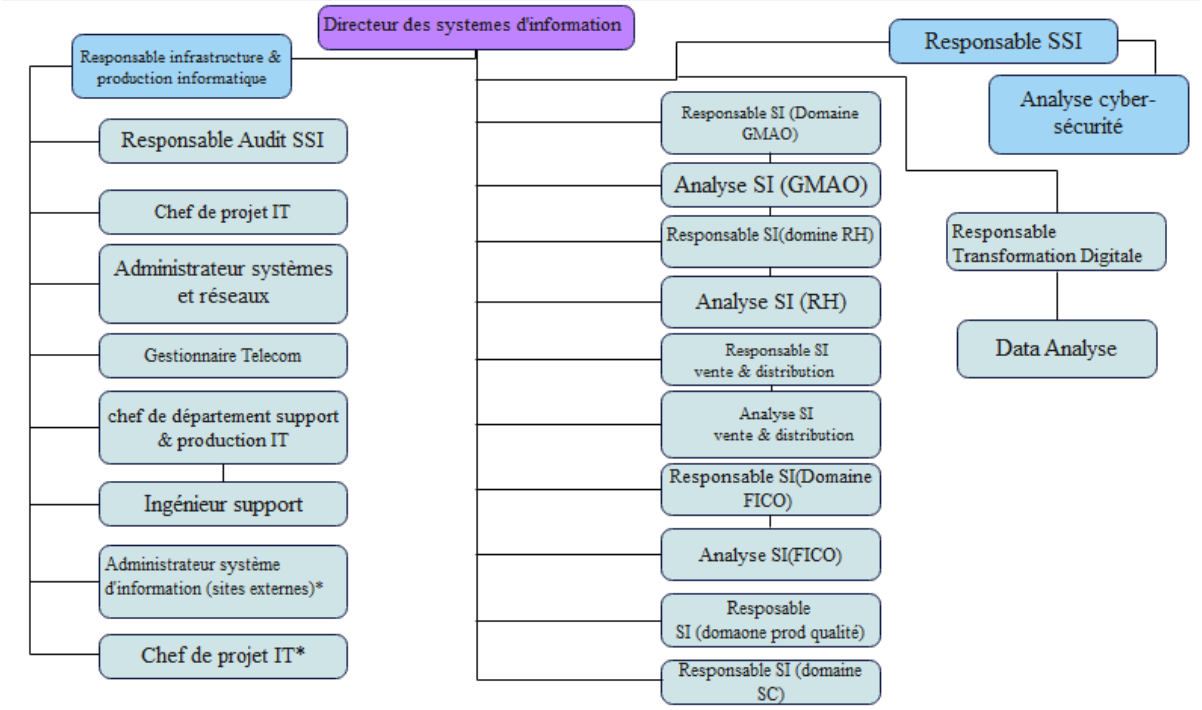

FIGURE 2.6 – Diagramme de service informatique.

Le service informatique est supervisé par les experts suivants :

2.9.1 Directeur du système d'information

Il est chargé de résoudre les problèmes et de prendre des décisions dans les plus brefs délais et au moindre coût, et opter des solutions informatiques qui améliorent la productivité de l'entreprise.

2.9.2 Administrateur système

Planifier, installer et assurer le bon fonctionnement de l'infrastructure informatique et réseau de leurs entreprise. Ils sont également responsables de la gestion et de la maintenance des systèmes qui fonctionnent sur le réseau.

2.9.3 Administrateur réseau

Il gère le réseau et assure la bonne circulation d'informations au sein de l'entreprise, en garantissant la qualité, la continuité et les performances des appareils et des réseaux tout en répondant aux besoins des utilisateurs.

2.9.4 Responsable support

Il contrôle à distance des postes de travail, aide les utilisateurs dans la manipulation des appareils et assure une assistance téléphonique en interne.

2.10 Les équipements utilisés dans l'entreprise

Un réseau est constitué de plusieurs équipements, dont la plupart sont des Cisco (Switch Catalyst, routeurs) interconnectés via des fibres optiques ou des paires de cuivre torsadées.

2.10.1 Distributeur (Backbone) de type Cisco Catalyst

Il supporte le trafic de données le plus important du réseau Cevital avec une bande passante très large, sur lequel les commutateurs d'accès, le pare-feu, serveurs et routeurs de l'entreprise y sont connectés. Il s'occupe du routage inter-Vlan (Virtuel Lan). Il permet l'accès à internet via le pare-feu et c'est généralement un serveur DHCP. Il est appelé aussi un switch fédérateur.

FIGURE 2.7 – Switch distributeur (Backbone) de type Cisco Catalyst 4507R. [27]

2.10.2 Switch d'accès et en cascade de type Cisco Catalyst 2960 et 2950

Ils sont connectés au backbone et installés dans les différents bâtiments de l'entreprise.

FIGURE 2.8 – Switch Cisco Catalyst 2960 et 2950 et son symbole sur packet tracer. [12,27]

2.10.3 Routeur de type Cisco 2900

Il permet de gérer le routage entre les différents sites de l'entreprise.

FIGURE 2.9 – Routeur de type Cisco 2900 et son symbole sur packet tracer.[12]

2.10.4 Point d'accès WIFI

L'entreprise dispose de plusieurs points d'accès WIFI, créant ainsi une couverture réseau sans fil au niveau de certaines parties du complexe.

FIGURE 2.10 – point d'accès WIFI.[12]

2.10.5 Le Pare feu

Deux pare-feux sont reliés en redondance et permettant de sécuriser le réseau, d'isoler certaines parties de celui-ci, encadre et sécurise l'accès internet

FIGURE 2.11 – Le pare-feu et son symbole sur packet tracer. [12]

2.10.6 Data center

Le data center est une piéce sécurisée, l'accés est restreint, seuls les responsables et les techniciens de la DSI (Direction Système d'Information) y ont accèdent. En outre, une climatisation des équipements est aussi assurée grâce au contrôle de la température par un système d'air conditionné avec une alimentation électrique doublée pour veiller à son fonctionnement sans coupure. En fait, le data-center de Cevital est le noyau central du réseau de l'entreprise où on y trouve les serveurs de l'entreprise, Backbones, les pare-feu, les routeurs et le standard téléphonique.

FIGURE 2.12 – Data Center. [27]

2.11 Codification des équipements de Cevital

- CEVWKS 1XXX : Ordinateur de bureau.
- CEVLAP 1XXX : Ordinateur portable.
- CEVSRV 1XXX : Serveur.
- CEVSWC 1XX : Switch.
- CEVAP 1XXX : Point d'accès wifi.
- CEVFW 1XXX : Pare-feu.
- CEVRTR 1XXX : Routeur.

2.12 Environnement des logiciels de base

Les systèmes d'exploitation et les logiciels de base installés à différents niveaux de postes de travail sont :

- Système d'exploitation windows 10, Windows Vista, etc).
- WinRAR.
- Firefox, Opera, IE.
- Norton Ghost 10.
- Adobe Acrobat, Foxit Reader.
- VMware, Virtuel pc.

2.13 Câblage informatique

Le système de câble informatique installé est conçu pour un fonctionnement optimal avec de futures améliorations. Tous les appareils informatiques existants dans l'entreprise sont interconnectés via des câbles à fibres optiques. Les prises murales sont identifiées par une étiquette avec un numéro unique au sein du résaeu et sont facilement repérables sur les panneaux de brassage pour le raccordement aux interrupteurs "prise Rj45".

2.14 Services et Applications utilisés

Environ mille utilisateurs de réseau informatique de Cevital, et divers employés effectuent leur travail quotidien en utilisant diverses applications et services fournis par le réseau. Nous pouvons nommer les applications et services suivants :

- Microsoft Exchange et Azure.
- Service Mail.
- Application comptabilité et gestion des stocks.
- Accès internet pour le collaborateur.
- Applications de GPAO (Gestion de la production assistée par ordinateur).
- Le partage de document via un serveur dédié (cloud privé).

2.15 Liaison inter-sites (architectures WAN)

Pour assurer le partage des ressources de l'entreprise et de la communication interne, Cevital dispose de liens permettant de relier le site de Bejaià aux différentes annexes de l'entreprise.

- Une liaison fibre optique point à point entre Bejaia et Alger.
- Liaison par satellite (Vsat) entre Bejaia et les sites d'El-kseur (Cojek), site de Tizi- Ouzou (Lala Khadija) et site El Kheroub (Constantine).

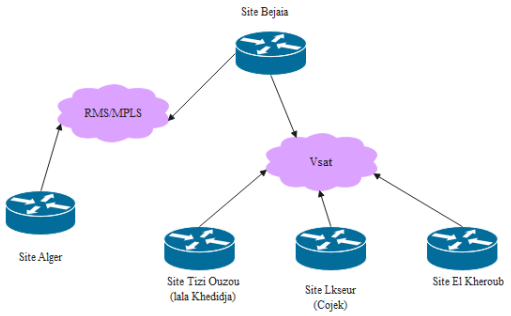

FIGURE 2.13 – L'architecture WAN du réseau Cevital (liaison inter-site). [4]

2.16 Problématique

Le service informatique d'une entreprise doit êtres apte pour gérer et assurer la disponibilité de son réseau. L'inconvénient est que l'évolution de sa taille rend difficile l'exploitation et la maintenance manuelle de ce réseau. Suite à notre visite à l'entreprise et à l'étude approfondie de son réseau informatique, nous avons pu identifier les problèmes rencontrés qui sont :

- Problème de surcharge sur un seul switch core, utilisation d'un seul domaine de diffusion.
- Manque de redondance physique pour assurer la tolérance aux pannes qui introduit un point de défaillance du réseau.
- Absence de la haute disponibilité du réseau à cause de l'architecture en cascade, la défaillance d'un switch provoque une perte d'une partie du réseau ainsi que ses ressources.
- La difficulté de gestion et de la maintenance manuelle du réseau de l'entreprise en vue sa taille.

2.17 Objectif de notre travail

- Eviter le problème de la surcharge sur un seul switch core, en utilisant la redondance et l'équilibrage des charges.
- Les pannes et les ruptures de liaisons et d'équipements ne doivent avoir aucun impact sur la disponibilité du réseau.

2.18 Solutions proposées

Afin de répondre aux exigences citées nous vous proposons ce qui suit :

- La redondance de passerelle avec le protocole HSRP.
- La redondance et l'équilibrage de charge avec le protocole GLBP.
- Intégrer la fonctionnalité d'équilibrage de charge par VLANs pour améliorer le protocole HSRP

2.19 Conclusion

Dans ce chapitre nous avons présenté l'entreprise Cevital. Ensuite, nous avons analysé son réseau informatique et trouvé quelques failles importantes qui représentent un risque sur la stabilité ainsi que le bon fonctionnement de ce dernier, celle-ci nous ont permis de lancer une problématique et d'avoir un aperçu sur la suite de notre projet.

Chapitre 3

La haute disponibilité

3.1 Introduction

Dans le deuxième chapitre, nous avons présenté les problèmes liés au réseau de l'entreprise, tels que le risque de panne d'une partie du réseau en cas de défaillance d'un équipement parent, entrainant l'arrêt de tous ces descendants, ainsi que la surcharge appliquée à un seul routeur, rendant le réseau très lent. Pour résoudre ces problèmes, il est essentiel d'assurer une continuité de service même en cas de panne d'un équipement, et d'équilibrer la charge sur l'ensemble du réseau.

Dans ce chapitre nous allons expliquer le concept de la haute disponibilité et présenter les différents protocoles qui permettent de l'assurer.

3.2 Définition de la haute disponibilité

La haute disponibilité est un ensemble de mesures mises en oeuvre pour assurer la disponibilité du service et son bon fonctionnement. Ces précautions sont prises pour éviter de graves interruptions de ce dernier qui entraînent une perte de productivité, par conséquent des pertes financières. [4,25]

3.3 La haute disponibilité dans les réseaux informatiques

La disponibilité des équipements est un élément important à prendre en compte dans tout système informatique qui concerne surtout les entreprises. Pouvoir maintenir les équipements de son réseau en fonctionnement continu pendant une longue période même en cas d'incident est appelé haute disponibilité.

En cas de panne de l'un des équipements, un autre sera élut selon certains critères et prendra le relai pour permettre aux utilisateurs de continuer à envoyer leurs requêtes sans interruption du réseau. La haute disponibilité assure la fiabilité du service dans toutes les conditions. [25]

3.4 Les protocoles de haute disponibilité

La disponibilité d'un réseau peut être assurée par plusieurs méthodes, parmis ces dernières nous citons les protocoles suivants :

3.4.1 Protocole HSRP (Hote Standby Routing Protocol)

3.4.1.1 Définition

HSRP est un protocole propriétaire de Cisco élut pour assurer la continuité d'un réseau local, il sert à configurer un groupe de routeurs, un routeur principale (actif), un routeur secondaire en attente (standby) et les autres en écoute (listen) qui partagent une même adresse IP et MAC (couche 2) pour agir comme un seul routeur virtuel. Ce protocole fournit une redondance au réseau de sorte qu'en cas de panne, le réseau doit se rétablir dès que possible à partir du premier saut selon la priorité des routeurs. [16,29,32,34]

3.4.1.2 Principe de fonctionnement

Le routeur actif (celui avec la plus haute priorité) agit comme passerelle par défaut pour le sous-réseau. En cas de défaillance, le routeur en attente (avec la seconde haute priorité) prendra le relai, à ce moment, un des routeurs qui étaient en mode écoute (listen) et qui a la plus grande priorité parmi ces derniers sera élut comme un routeur en mode standby.

En cas d'égalité dans la priorité, le routeur qui a l'adresse IP la plus élevée sera choisit comme routeur actif. [Figure 3.1]

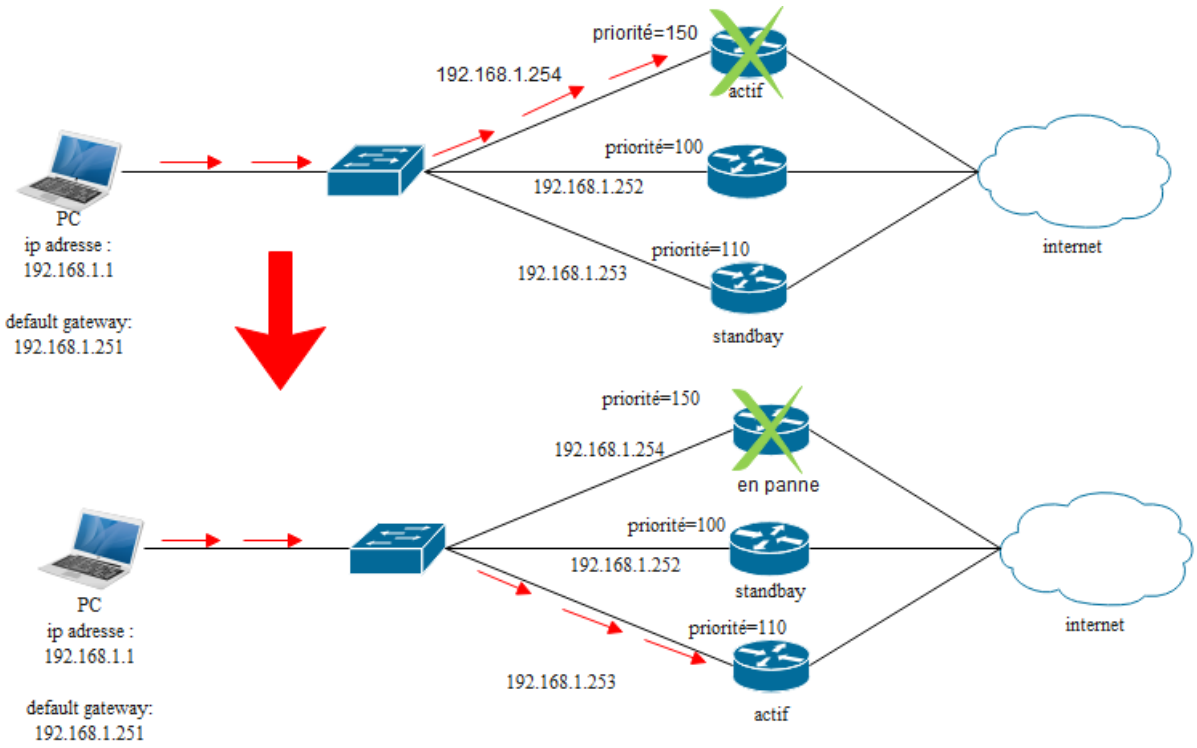

FIGURE 3.1 – Schéma montrant le principe de fonctionnement de protocole HSRP

3.4.1.3 Algorithme d'élection du routeur actif

Afin d'assurer que le routeur désigné en tant que routeur actif est le plus prioritaire, il est nécessaire de suivre plusieurs étapes : [34,39]

1. Chaque routeur dans le groupe HSRP est configuré avec une adresse IP virtuelle (VIP) , un numéro de groupe HSRP et une priorité.
2. Les routeurs émettent des paquets HELLO à intervalle réguliers (3s) pour signaler mutuellement leurs présences et leurs disponibilités.
3. Lorsqu'un routeur devient le routeur actif, il annonce sa VIP (adresse IP virtuelle) sur le réseau et répond aux paquets ARP pour cette adresse IP. Les autres routeurs du groupe HSRP sont en mode veille.
4. Si le routeur actif devient indisponible ou ne répond plus, le routeur ayant la deuxième priorité la plus élevée prend le relai et devient le nouveau routeur actif. Si plusieurs routeurs ont la même priorité, le routeur ayant l'adresse IP la plus élevée dans le groupe devient le nouveau routeur actif.
5. Si un routeur ayant une priorité plus élevée que le routeur actif est ajouté au groupe HSRP, il prendra automatiquement le relai en tant que nouveau routeur actif.
6. Si la priorité d'un routeur existant est augmentée, il peut devenir le nouveau routeur actif.
7. Si un routeur existant a une priorité inférieure à celle de l'actuel routeur actif, il restera

en mode veille et ne reprendra pas le relai, sauf si tous les autres routeurs ont une priorité encore plus basse.

3.4.1.4 Le rôle des différents équipements

Chaque équipement de groupe HSRP a son rôle. [37]

• **Routeur initiateur (initial)** : Il s'agit du premier état au démarrage de HSRP vous le verrez juste après avoir configuré le protocole HSRP ou lorsque l'interface vient d'être activé.

• **Routeur en attente (standby)** : Le routeur n'est pas le routeur actif donc continuer à envoyer des messages HELLO. Si le routeur actif tombe en panne, il prendra le relai.

• **Routeur actif** : Le routeur transmettra activement les paquets des clients et enverra des messages Hello.

• **Routeur en écoute (listen)**
Le routeur connait l'adresse IP virtuelle et écoutera les messages Hello des autres routeurs HSRP.

Les messages envoyés entre les routeurs du groupe HSRP sont :

• **Hello** : Envoyé par le routeur actif et standby toutes les 3s, si le routeur standby ne le reçoit pas (c'est à dire que le routeur actif est en panne) dans un temps de 10s il prendra le relai.

• **Resign** : Envoyé par le routeur actif pour déclarer sa démission et signaler au routeur standby pour prendre le rôle actif.

• **Coup** : Envoyé par un routeur qui veut devenir actif (si un nouveau routeur ajouté au groupe avec une priorité plus haute que celle du routeur actif).

3.4.2 Protocole VRRP(Virtual Router Redundancy Protocol)

3.4.2.1 Définition

C'est un protocole de routage standard similaire à HSRP, il fonctionne sur d'autres routeurs que Cisco, il permet de partager une adresse IP virtuelle pour assurer la redondance de la passerelle par défaut d'un réseau local.

Le groupe de routeurs partageant la même adresse IP virtuelle est appelé groupe VRRP. Le routeur ayant la priorité la plus élevée sera élut comme routeur actif appelé Master, les autres routeurs ayant la priorité inférieur au routeur Master sont des routeurs en attente appelés Backup. [15,32]

3.4.2.2 Principe de fonctionnement

Tout les routeurs de groupe VRRP doivent être configurés avec la même adresse IP virtuelle, un même identifiant de groupe (ID) et une priorité.

Le routeur ayant la meilleur priorité est désigné comme routeur Master, il se charge de répondre aux requêtes ARP, les autres routeurs ayant la priorité inférieure sont des routeurs Backup, tout les routeurs de groupe VRRP envoient périodiquement des messages VRRP pour signaler leurs présences. Les routeurs Backup surveillent le routeur Master, si un message VRRP de ce dernier n'est pas reçu par les routeurs Backup, la Master sera remplacé par un Backup ayant la priorité la plus élevée.

3.4.3 Protocole GLBP (Gateway Load Balancing Protocol)

3.4.3.1 Définition

GLBP est un protocole propriétaire Cisco, alternative à HSRP et VRRP, il assure une redondance de passerelle ainsi qu'une répartition des charges équilibrées entre un groupe de plusieurs routeurs en utilisant une seule adresse IP virtuelle et plusieurs adresses MAC virtuelles. Le groupe de routeurs sont configurés en, un routeur AVG (Actif Virtual Gateway) et le reste en routeurs AVF (Actif Virtual Forwarders), contrairement à HSRP et VRRP, tout les routeurs appartenant au groupe GLBP sont actifs et participent à l'envoie des paquets ce qui permet de répartir la charge de trafic. [24,32,34,39]

3.4.3.2 Principe de fonctionnement

Le fonctionnement de protocole GLBP consiste à configurer un ensemble de routeurs pour être un groupe GLBP, les routeurs sont identifiés par une adresse virtuelle unique partagée entre tout les routeurs du groupe, cette adresse est la passerelle par défaut pour les hôtes du réseau. Le routeur qui a la priorité la plus élevée sera choisie comme un AVG, le reste des routeurs serons des AVF.

Le routeur désigné comme un AVG est responsable de l'allocation des adresses MAC virtuelles aux membres du groupe GLBP et distribuer la charge entre les différents AVF (sachant que lui même est aussi un AVF).

Le premier utilisateur va utiliser le AVG comme passerelle, le deuxième va utiliser l'AVF qui a la deuxième priorité la plus élevée et ainsi de suite.

Si l'AVG tombe en panne un AVF ayant la priorité la plus elevée du groupe va prendre le relai. [Figure 3.2]

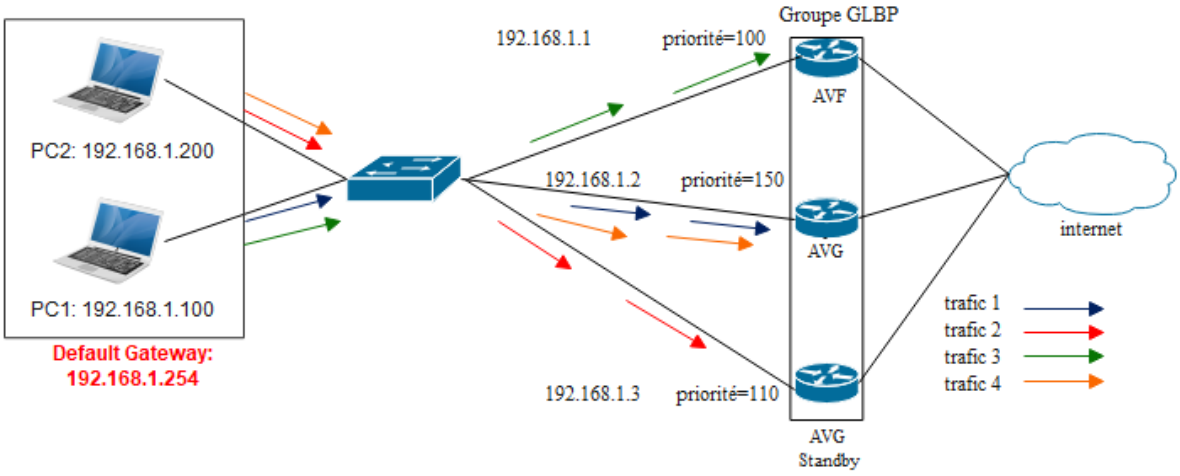

FIGURE 3.2 – Schéma montrant le principe de fonctionnement de protocole GLBP

3.4.3.3 Algorithme de redondance et répartition des charges

La répartition des charges est assurée par le protocole GLBP en suivant un ensemble d'étapes qui sont : [34,39]

1. Tout d'abord tous les routeurs doivent être connectés les uns aux autres, et doivent être configurés avec la même adresse IP virtuelle, une priorité et un numéro de groupe.
2. Le routeur ayant la priorité la plus élevée sera élut comme un AVG (Actif Virtual Gateway), le routeur ayant la deuxième meilleure priorité sera l'AVG Standby et celui qui a la troisième priorité sera l'AVF (Actif Virtual Forwarders).
3. Tout les routeurs du groupe GLBP envoient un message Hello chaque 3s pour indiquer leurs disponibilités, si un routeur n'envoie pas un Hello après 3s il sera supprimé du groupe.
4. Lorsque un utilisateur veut envoyer un trafic, il doit d'abord envoyer une requête ARP à l'adresse IP virtuelle unique pour demander l'adresse du routeur à qui va envoyer le trafic, si l'AVG est disponible, il va répondre avec son adresse MAC virtuelle, sinon il va envoyer une réponse ARP contenant l'adresse MAC du routeur AVG Standby, ainsi de suite.
5. Si par exemple un groupe GLBP est constitué de 3 routeurs R1, R2 et R3 et respectivement les priorités P1, P2 et P3 sachant que P1>P2>P3 donc les trafics seront envoyés comme suit :
   Le premier trafic sera envoyé au router R1 le deuxième au R2 et le troisième au R3.
6. Si l'AVG tombe en panne, l'AVG Standby qui est le routeur contenant la deuxième priorité la plus élevée prendra le relai, et l'AVF prendra le rôle de l'AVG Standby.
7. Si un nouveau routeur est ajouté au groupe GLBP et ce routeur contient une priorité plus élevée que celle de l'AVG, ce dernier va prendre le rôle de l'AVG même s'il n'est pas tombé en panne.

3.4.3.4 Le rôle des différents équipements

Chacun des équipements du groupe GLBP a un rôle précis :

- **AVG (Actif virtual Gateway)** : Il est aussi un AVF, il se charge de l'allocation des adresses MAC virtuelles aux routeurs du groupe et de répondre aux requêtes ARP pour distribuer la charge d'une manière égale entre les AVF.
- **AVG Standby (Actif Virtual Gateway Standby)** : C'est le deuxième routeur qui a la plus grande priorité, il prendra le rôle de l'AVG en cas de défaillance.
- **AVF (Actif Virtual Forwarders)** : Ce sont les routeurs restants du groupe GLBP.

Il existe 4 timers pour le protocole GLBP sont :

- **Hello** : Envoyé chaque 3s indique que le routeur est toujours disponible.
- **HoldTime** : Indique le temps max entre deux messages ' Hello ' avant que le routeur soit considéré comme mort.
- **Redirect Time** : Indique le temps que l'AVG répond aux requêtes ARP avec une adresse MAC virtuelle d'un AVF mort. (600s par défaut).
- **Secondary HoldTime** : Indique le temps qu'un AVF peut supporter l'adresse MAC d'un AVF mort. (14400s par défaut).

3.4.4 Tableau comparatif entre les deux protocoles HSRP et GLBP

Le tableau suivant représente une comparaison théorique entre le protocole HSRP et le protocole GLBP en termes de leur apparition, de leur principe de fonctionnement, les équipements associés, ainsi que des adresses et messages utilisés. [Figure 3.3]

HSRP	GLBP
Propiétaire cisco, 1994	Propriétaire cisco, 2005
Il fournit une redondance au réseau (la tolérance aux pannes)	Il fournit une redondance ainsi qu'une équilibrage de charge
surcharge sur un seul routeur	Charge répartit mais avec un délai long
1 adresses virtuelle et une adresse MAC	1 adresse virtuelle et plusieurs adresses MAC
Un routeurs initiateur, actif, standby et listen.	Un routeur AVG, AVG-Standby et AVF
Hello, Rsign, Coup	Hello,HoldTime, Redirect Time.

FIGURE 3.3 – La comparaison entre HSRP et GLBP

Le tableau précédent diffère entre HSRP et GLBP, les deux sont propriétaire cisco,HSRP apparu en 1994, il fournit une redondance au réseau (la tolérence de pannes des équipements), et GLBP en 2005 qui assure la redondance et l'équilibrage de charge. Une seule adresse virtuelle et une seule adresse MAC utilisées dans HSRP contrairement à GLBP ou il utilise une adresse virtuelle et plusieurs adresses MAC.

Concernant les équipements, HSRP a besoin d'un routeur initiateur, actif, standby et listen qui s'envoient des messages Hello, Resign et Coup. GLBP utilise un routeur AVG, AVG Standby et AVF qui envoient les messages Hello, HoldTime, Redirect Time pour communiquer entre eux.

Dans HSRP on a deux équipements mais un seul qui travaille d'ou le le trafic doit passer par une seule route ce qui mène au ralentissement du réseau, aussi dans GLBP, la redondance et l'équilibrage de charge sont assurés mais lorsqu'un message est volumineux, cela entraîne un temps de traitement plus long, ce qui peut provoquer un ralentissement pour les messages suivants.

3.5 Conclusion

Dans ce chapitre nous avons présenté les différents protocoles qui assurent la haute disponibilité dans un réseau local dont nous avons utilisé deux parmi dans notre étude, ainsi nous avons éclaircis leurs fonctionnements et l'avantage qu'ils portent à ce réseau.

Chapitre 4

Conception et Réalisation

4.1 Introduction

Dans le but de clarifier et compléter ce que nous avons présenté dans les chapitres précédents, nous allons dans ce chapitre simuler les deux protocoles HSRP et GLBP ainsi que quelques protocoles nécessaires pour compléter l'implémentation de ces derniers en montrant toute étape suivie tout au long de notre pratique ainsi que les logiciels utilisés. Nous allons illustrer les étapes de configurations de chaque composant de l'architecture et leurs fonctionnements par des captures d'écran. Enfin, tester l'efficacité et la validité des solutions proposées.

4.2 Choix du logiciel de simulation

Il existe plusieurs logiciels de simulation de réseau tel que NetSim, Filius, Cisco Packet Tracer, GNS3, Eve-NG etc. Pour nos implémentations nous allons utiliser deux parmi ceux cités au dessus, nous allons utiliser le logiciel Cisco Packet Tracer pour la simulation de protocole HSRP car il est facile à utiliser comme il nous offre une interface conviviale et un large éventail de fonctionnalités et de dispositifs qui nous sont nécessaires dans notre pratique. Pour l'implémentation de protocole GLBP, nous allons utiliser le logiciel GNS3, car ce dernier n'est pas encore pris en charge par le logiciel Cisco Packet Tracer.

4.2.1 Présentation de simulateurs Cisco Packet Tracer

Cisco Packet Tracer est un puissant logiciel de simulation de réseau développé par Cisco Systems. Il permet aux étudiants, aux professionnels et aux passionnés de réseautage de concevoir, configurer et dépanner virtuellement des réseaux complexes. Il fournit une interface graphique facile à utiliser et prend en charge divers périphériques réseau tels que les routeurs, les commutateurs, les serveurs et les PCS. Les capacités de simulation en temps réel permettent aux utilisateurs de visualiser l'acheminement des paquets, de surveiller le trafic réseau et de tester différents scénarios

sans avoir besoin de matériel physique. Cisco Packet Tracer est un outil précieux pour apprendre, pratiquer et valider vos compétences en réseau. [9]

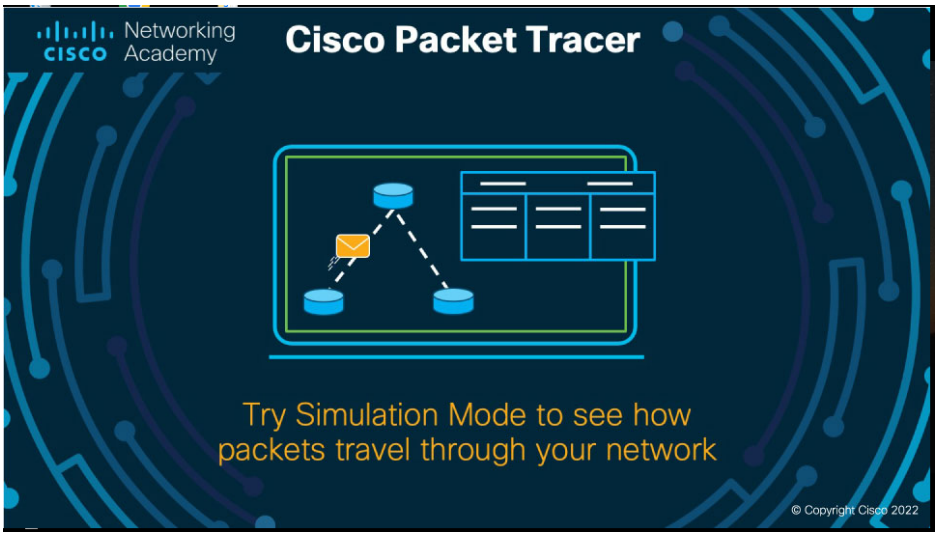

FIGURE 4.1 – Simulateur Cisco Packet Tracer

4.2.2 Présentation de simulateurs GNS3

GNS3 est un simulateur de réseau open source signifie Graphical Network Simulator version "3" largement utilisé dans l'apprentissage de l'industrie et du réseau. Cela vous permet de créer des topologies de réseau complexes à l'aide de périphériques virtuels et réels. GNS3 prend en charge divers systèmes d'exploitation réseau tels que Cisco IOS, Juniper JunOS et VyOS. Il permet aux utilisateurs de créer des configurations réseau, d'exécuter des simulations et de résoudre les problèmes de réseau dans un environnement virtuel.

En raison de sa flexibilité et de sa compatibilité avec divers périphériques réseau, GNS3 est largement utilisé par les professionnels du réseau, les ingénieurs réseau et les étudiants pour tester des configurations, simuler des scénarios réseau complexes et pratiquer la configuration et le dépannage du réseau utilisé. En résumé, GNS3 est un outil puissant et polyvalent pour l'apprentissage et la pratique des compétences en réseautage.

FIGURE 4.2 – Logo de GNS3

En premier lieu nous allons segmenter notre réseau en plusieurs VLANs (selon ce qui nous a été donné à l'entreprise CEVITAL).

4.3 Présentation de l'ancienne architecture du réseau Cevital

La figure suivante montre l'ancienne architecture de l'entreprise CEVITAL. Aprés nos études sur son fonctionnement nous avons trouvé que la surcharge sur un seul commutateur et l'emplacement en cascade de ses équipements provoque à tout moment un disfonctionnement du service. Pour l'éviter nous allons proposer une amélioration à cette dernière. [Figure 4.3]

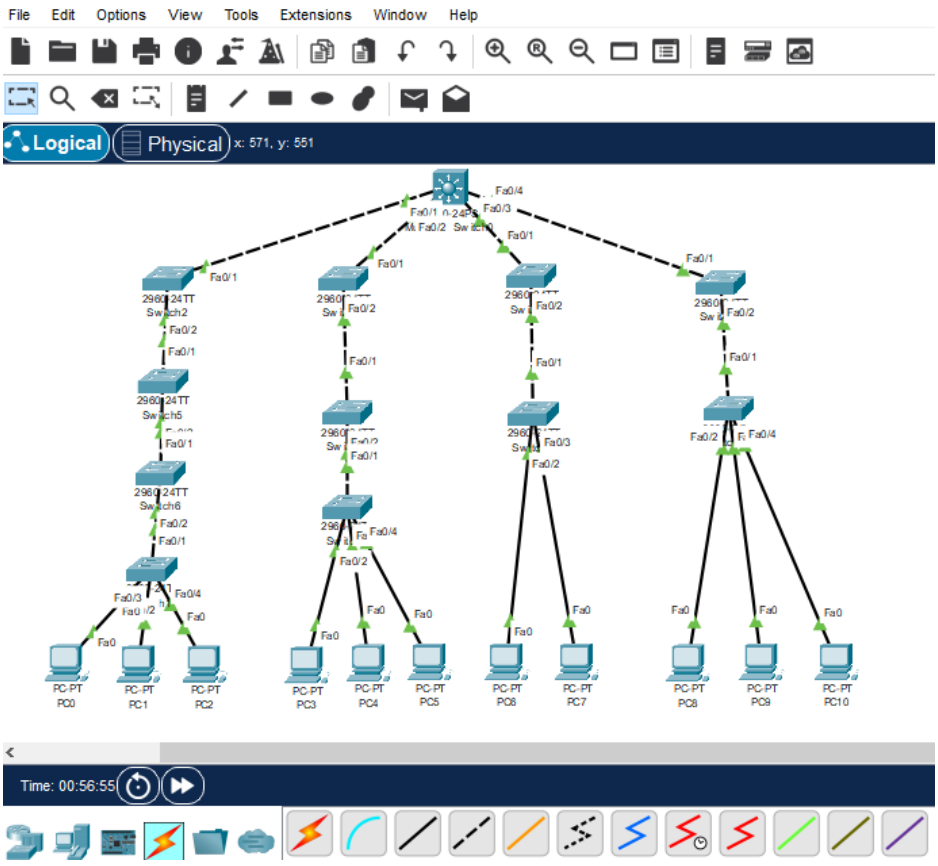

FIGURE 4.3 – Ancienne architecture de CEVITAL

4.4 Présentation de l'architecture réseau après l'amélioration

L'architecture améliorée du réseau CEVITAL présentée dans la figure comprend deux couches principales. La première couche, appelée couche "core" ou de distribution, est composée de deux switchs core. La seconde couche, appelée couche d'accès, rassemble tous les autres switchs restants de l'architecture. [Figure 4.4]

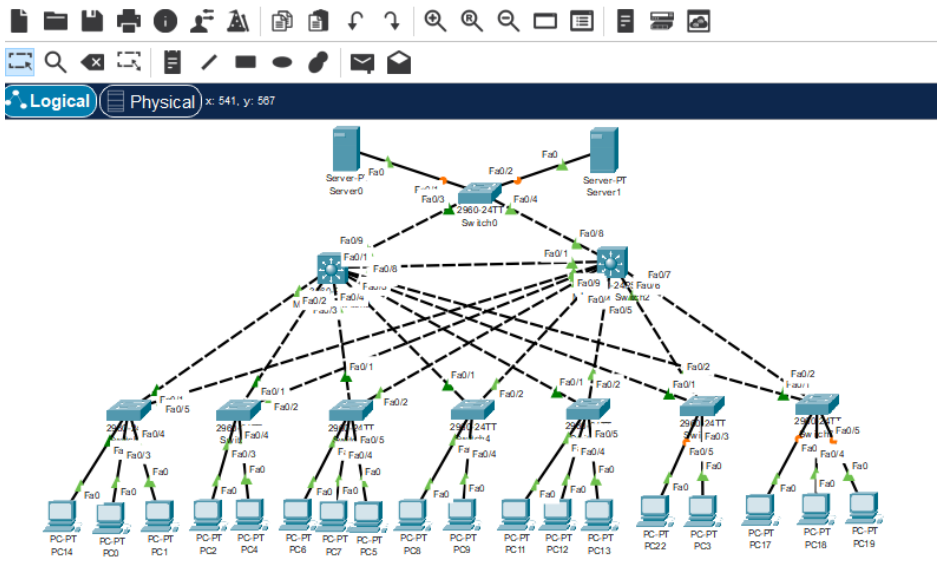

FIGURE 4.4 – Architecture améliorée

Dans la nouvelle architecture, la conception en cascade des équipements a été éliminée . En outre, un deuxième switch core a été ajouté pour assurer la redondance du réseau. Ainsi, en cas de défaillance d'un des switches, le deuxième switch prendra en charge l'ensemble du réseau pour éviter toute interruption de service.

4.5 Segmentation des VLANs

- IT : Information Technology
- DFC : Direction Finance et Comptabilité
- DRH : Direction des Ressources Humaines
- PRODUCTION
- PLANIFICATION
- COMMERCIAL
- ADG : Administrateur Directeur G'enéral
- LOGISTIQUE
- SUPPLY-CHAIN
- SERVER

4.5.1 Plan d'adressage

L'adresse attribuée à ce réseau est 10.50.0.0/24 avec un masque 255.255.255.0, le nombre de sous-réseaux qu'on peut créer est 255. Le tableau suivant présente le plan d'adressage : [Figure 4.5]

Nom VLAN	VLAN-id	Adresse du sous-réseau
IT	2	10.50.2.0/24
DFC	3	10.50.3.0/24
DRH	4	10.50.4.0/24
PRODUCTION	5	10.50.5.0/24
PLANIFICATION	6	10.50.6.0/24
COMMERCIAL	7	10.50.7.0/24
ADG	8	10.50.8.0/24
LOGISTIQUE	9	10.50.9.0/24
SUPPLY-CHAIN	10	10.50.10.0/24
SERVER	11	10.50.11.0/24

FIGURE 4.5 – Le plan d'adressage des VLANs

4.5.2 Désignation des interfaces

Le tableau suivant représente la répartition des interfaces sur les différents équipements :

Appareil Local	Appareil Distant	Interface(s) Locale(s)	Interface(s) Distante(s)
Ser1	SWA1	F0	F0/4
Ser2	SWA1	F0	F0/3
SWA1	Core1	F0/1	F0/9
SWA1	Core2	F0/2	F0/9
Core1	Core2	F0/8	F0/8
Core1	SWA2	F0/1	F0/1
Core1	SWA3	F0/2	F0/1
Core1	SWA4	F0/3	F0/1
Core1	SWA5	F0/4	F0/1
Core1	SWA6	F0/5	F0/1
Core1	SWA7	F0/6	F0/1
Core1	SWA8	F0/7	F0/1
Core2	SWA2	F0/1	F0/2
Core2	SWA3	F0/2	F0/2
Core2	SWA4	F0/3	F0/2
Core2	SWA5	F0/4	F0/2
Core2	SWA6	F0/5	F0/2
Core2	SWA7	F0/6	F0/2

FIGURE 4.6 – Tableau de la répartition des interfaces sur les différents équipements.

4.6 La configuration des équipements utilisés

Pour arriver à implémenter les protocoles HSRP et GLBP on doit passer par plusieurs étapes de configuration, commençons par la sécurisation des équipements puis la configuration des protocoles VTP, DHCP, STP et terminer avec les deux protocoles de haute disponibilité. Tout ceci sera illustré et bien expliqué dans ce qui suit :

La configuration de base

Une configuration de base sera effectuée sur chaque équipement de l'architecture, les deux switchs Core ainsi que tous les switchs d'accès.

- **La configuration de hostname**

Ceci nous permettra de renommer les équipements et leurs donner des noms significatifs. Ci-dessous, un exemple illustratif de la nomination de l'un des switchs core : [Figure 4.7]

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Core1
Core1(config)#exit
Core1#
```

FIGURE 4.7 – Commande permettant de renommer un équipement.

- **La sécurisation de mode privilégié**

Nous avons attribué un mot de passe **"cisco"** pour sécuriser l'accès au mode privilégié. [Figure 4.8]

```
Core1(config)#enable pass
Core1(config)#enable password cisco
Core1(config)#end
Core1#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
```

FIGURE 4.8 – L'attribution d'un mot de passe au mode privilégié.

Après cette configuration seul l'administrateur réseau a le droit d'y accèder

- **La sécurisation de la ligne console**

On a attribué un mot de passe pour la ligne console de chaque équipement pour sécuriser l'accés à ces derniers. [Figure 4.9]

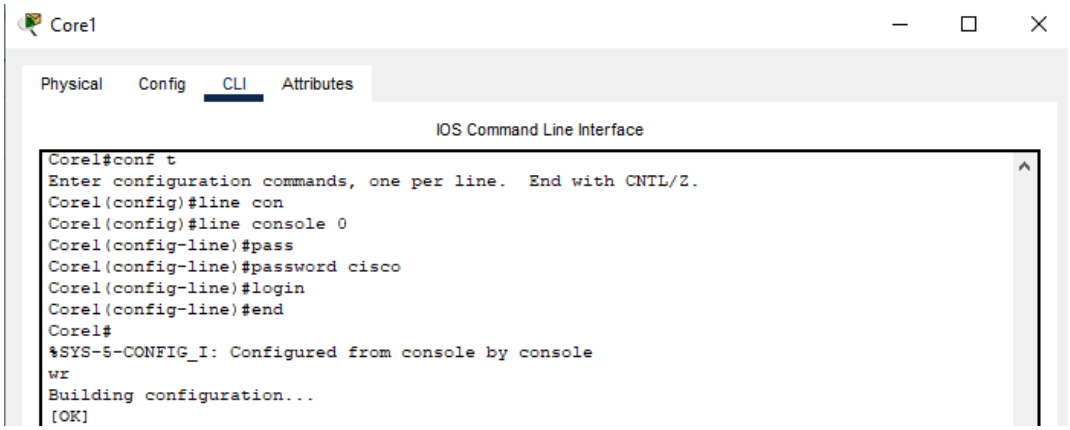

FIGURE 4.9 – La sécurisation de la ligne console

- **Sécuriser le mot de passe**

Pour rendre le mot de passe invisible nous avons activé le service **"password-encryption"**. [Figure 4.10]

```
Corel(config)#service pa
Corel(config)#service password-encryption
Corel(config)#end
Corel#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
```

FIGURE 4.10 – Commandes permettant de cacher le mot de passe.

- **La configuration de la bannière**

Une bannière de type "**banner motd**" est utilisée pour indiquer l'interdiction d'accès aux personnes non autorisées. [Figure 4.11]

```
Corel(config)#banner m
Corel(config)#banner motd "ACCES AUX PERSONNES AUTORISEES"
Corel(config)#end
Corel#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
```

FIGURE 4.11 – La configuration de la bannière sur le switch Core1

Pour vérifier la configuration de base appliquée sur un équipement on tapera la commande **"show running-config"**, la configuration apparaitra comme le montre la figure ci-dessous : [Figure 4.12]

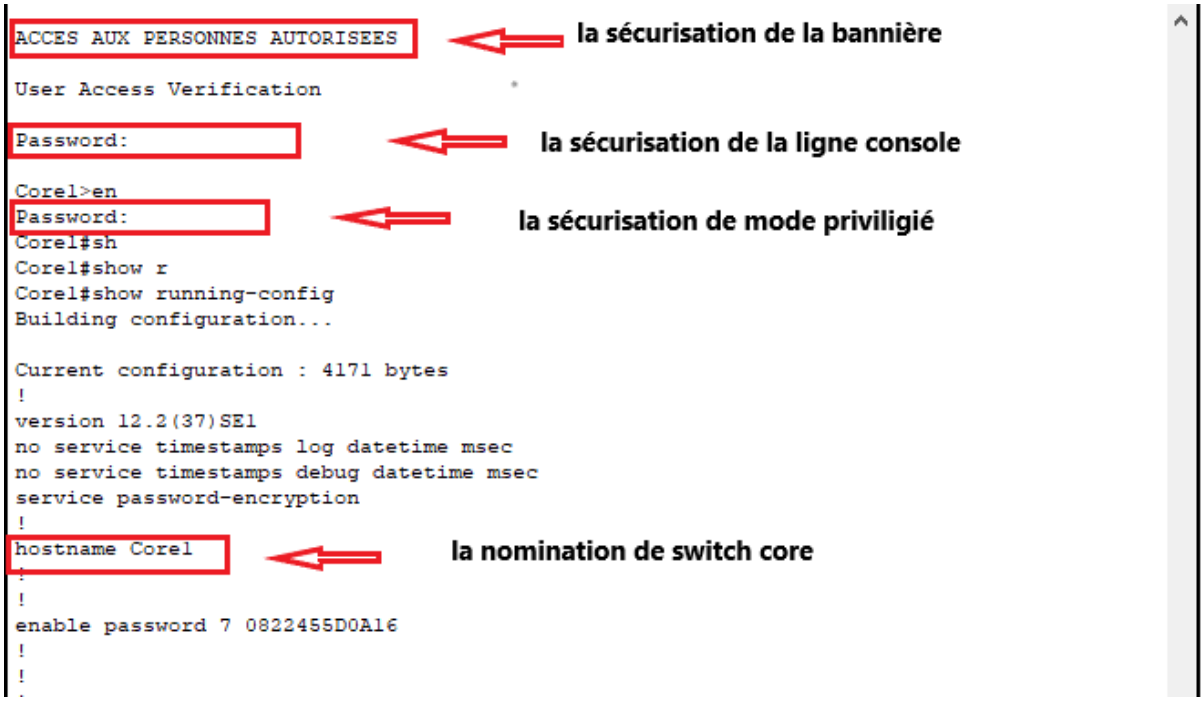

FIGURE 4.12 – Test de vérification de la configuration de base de switch Core1

4.7 La création des VLANs

Les VLANs sont crées au niveau du commutateur multilayer Core1 (Server) comme suit : [Figure 4.13]

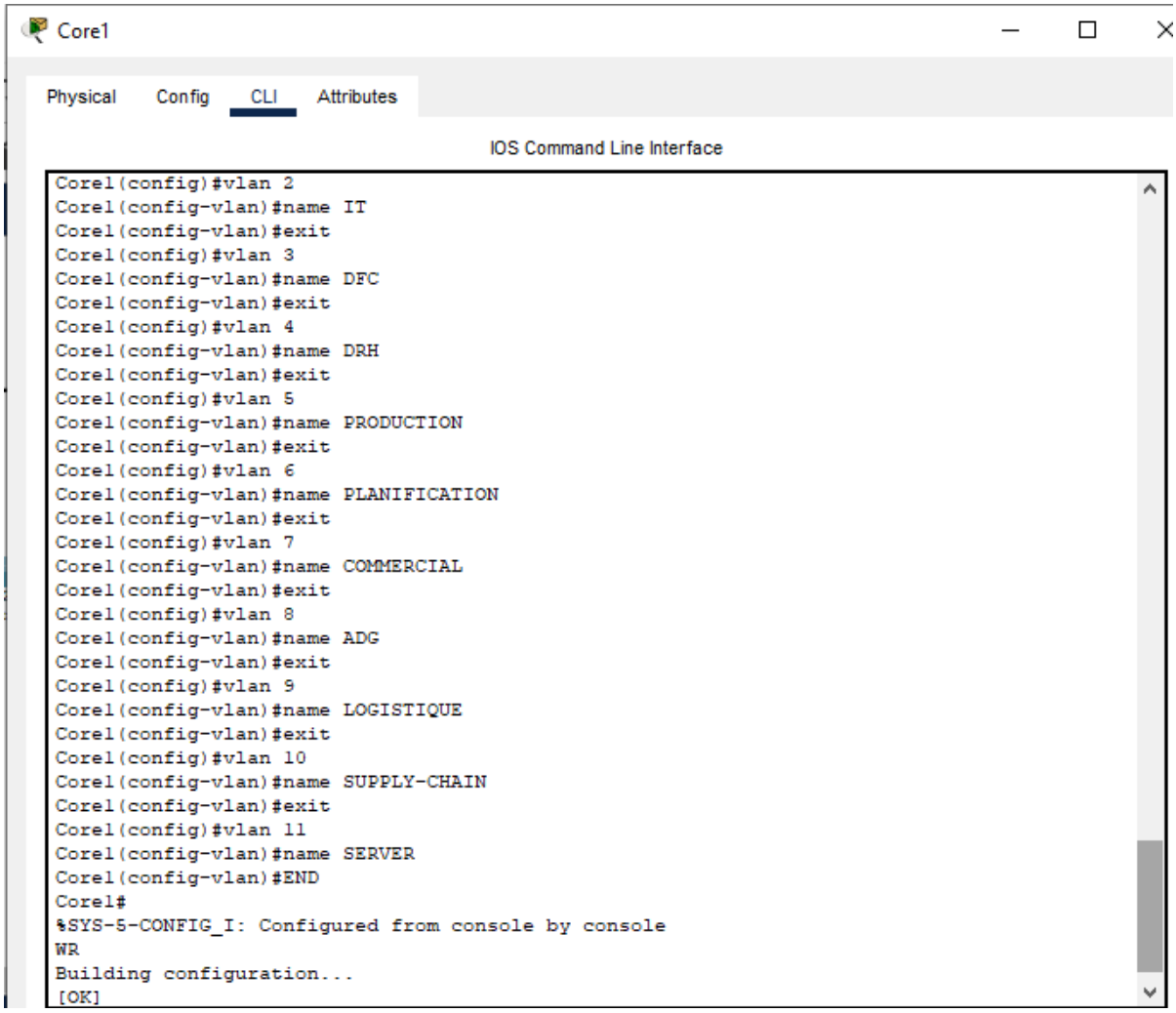

FIGURE 4.13 – La création des VLAN au niveau de commutateur Core1

4.8 Configuration du protocole VTP

Les deux modes de protocole VTP sont configurés au niveau de tous les switchs de l'architecture.

4.8.1 VTP mode serveur

Le commutateur Core1 est configuré comme un serveur VTP, c'est lui qui s'occupe de la gestion (Ajout, Modification et Suppression) de l'ensemble des VLANs au niveau de tous les switchs de l'architecture (en mode client), le nom de domaine **"cevital.com"** et le mot de passe **"cisco"**sont attribués. La figure ci-dessous représente cette configuration : [Figure 4.14]

```
Corel(config)#vtp mode se
Corel(config)#vtp mode server
Device mode already VTP SERVER.
Corel(config)#vtp ver
Corel(config)#vtp version 2
VTP mode already in V2.
Corel(config)#vtp do
Corel(config)#vtp domain cevital.com
Domain name already set to cevital.com.
Corel(config)#vtp pass
Corel(config)#vtp password cisco
Password already set to cisco
Corel(config)#end
Corel#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
Corel#
```

FIGURE 4.14 – La configuration de VTP server

4.8.2 VTP mode client

Le commutateur Core2 et tous les commutateurs d'accès sont configurés en mode VTP client. La configuration est faite comme suit : [Figure 4.15]

```
Core2(config)#vtp mode cl
Core2(config)#vtp mode client
Setting device to VTP CLIENT mode.
Core2(config)#vtp ver
Core2(config)#vtp version 2
Cannot modify version in VTP client mode
Core2(config)#vtp do
Core2(config)#vtp domain cevital.com
Domain name already set to cevital.com.
Core2(config)#vtp pass
Core2(config)#vtp password cisco
Password already set to cisco
Core2(config)#end
Core2#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
Core2#
```

FIGURE 4.15 – La configuration de VTP client

Le nom de domaine et le mot de passe doivent être les même dans tous les Switchs core et accès

4.9 La configuration de mode trunk et access

Tous les liens entre les équipements sont configurés en mode trunk et accés.

4.9.1 Mode trunk

Tous les liens entre les commutateurs sont configurés en mode trunk pour autoriser le transport de l'ensemble des VLANs, les commandes suivantes montrent cette configuration . [Figure 4.16]

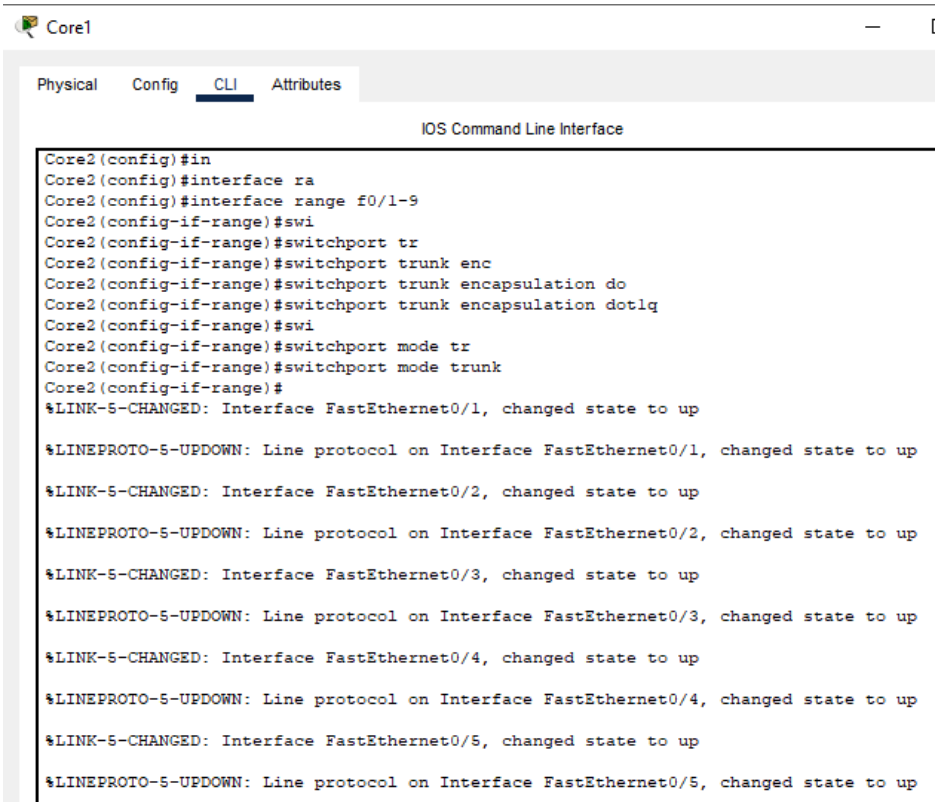

FIGURE 4.16 – La configuration de mode trunk

Les interfaces de 0/1 à 0/9 des deux switchs Core sont configurées en mode trunk.

4.9.2 Mode access

Les commandes suivantes permettent d'attribuer les ports aux VLANs, cette configuration est faite entre chaque commutateur d'accès et les terminaux. [Figure 4.17]

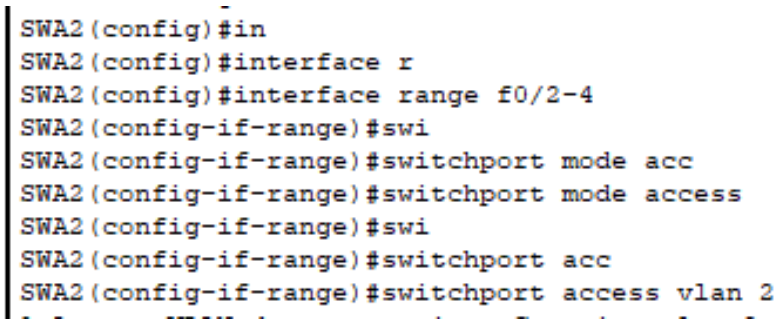

FIGURE 4.17 – La configuration de mode accès

Cette configuration permet aux PCs reliés au SWA2 de recevoir leurs adresses de la part du VLAN 2

- **Vérification de la configuration**

la commande **"show vlan brief"** permet de voir les ports attribués au VLANs. [Figure 4.18]

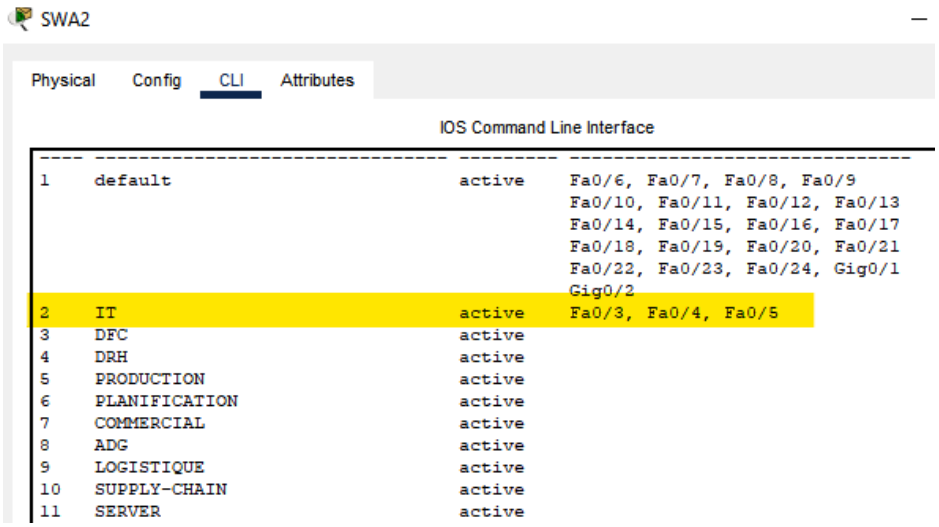

FIGURE 4.18 – Attribution de VLANs

On a attribué un VLAN à chaque switch accès SWA, cette figure montre que les trois interfaces du SWA2 sont attribués au VLAN 2.

- **L'attribution d'adresses aux VLANs**

Les commandes suivantes montrent comment attribuer des adresses au VLANs pour les deux switchs Core, Core1 et Core2 : [Figure 4.19]

```
Building configuration...
[OK]
Core1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Core1(config)#in
Core1(config)#interface vlan 2
Core1(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

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

Core1(config-if)#ip add
Core1(config-if)#ip address 10.50.2.252 255.255.255.0
Core1(config-if)#exit
Core1(config)#interface vlan 3
Core1(config-if)#
%LINK-5-CHANGED: Interface Vlan3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan3, changed state to up

Core1(config-if)#ip address 10.50.3.252 255.255.255.0
Core1(config-if)#exit
Core1(config)#interface vlan 4
Core1(config-if)#
%LINK-5-CHANGED: Interface Vlan4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan4, changed state to up
```

FIGURE 4.19 – Attribution d'adresses aux VLANs dans le switch Core1

Chaque VLAN lui a été attribué son adresse et son masque dans le switch Core1.

```
Core2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Core2(config)#in
Core2(config)#interface vlan 2
Core2(config-if)#ip add
Core2(config-if)#ip address 10.50.2.253 255.255.255.0
Core2(config-if)#exit
Core2(config)#interface vlan 3
Core2(config-if)#
%LINK-5-CHANGED: Interface Vlan3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan3, changed state to up

Core2(config-if)#ip address 10.50.3.253 255.255.255.0
Core2(config-if)#exit
Core2(config)#interface vlan 4
Core2(config-if)#
%LINK-5-CHANGED: Interface Vlan4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan4, changed state to up

Core2(config-if)#ip address 10.50.4.253 255.255.255.0
Core2(config-if)#exit
Core2(config)#interface vlan 5
Core2(config-if)#
%LINK-5-CHANGED: Interface Vlan5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan5, changed state to up

Core2(config-if)#ip address 10.50.5.253 255.255.255.0
Core2(config-if)#exit
```

FIGURE 4.20 – Attribution d'adresses aux VLANs dans le switch Core2

Chaque VLAN lui a été attribué son adresse et son masque dans le switch Core2.

4.10 La configuration DHCP

La configuration DHCP au niveau de Core1 et Core2 pour tout les VLANs est faite à l'aide des commandes suivantes : [Figure 4.21]

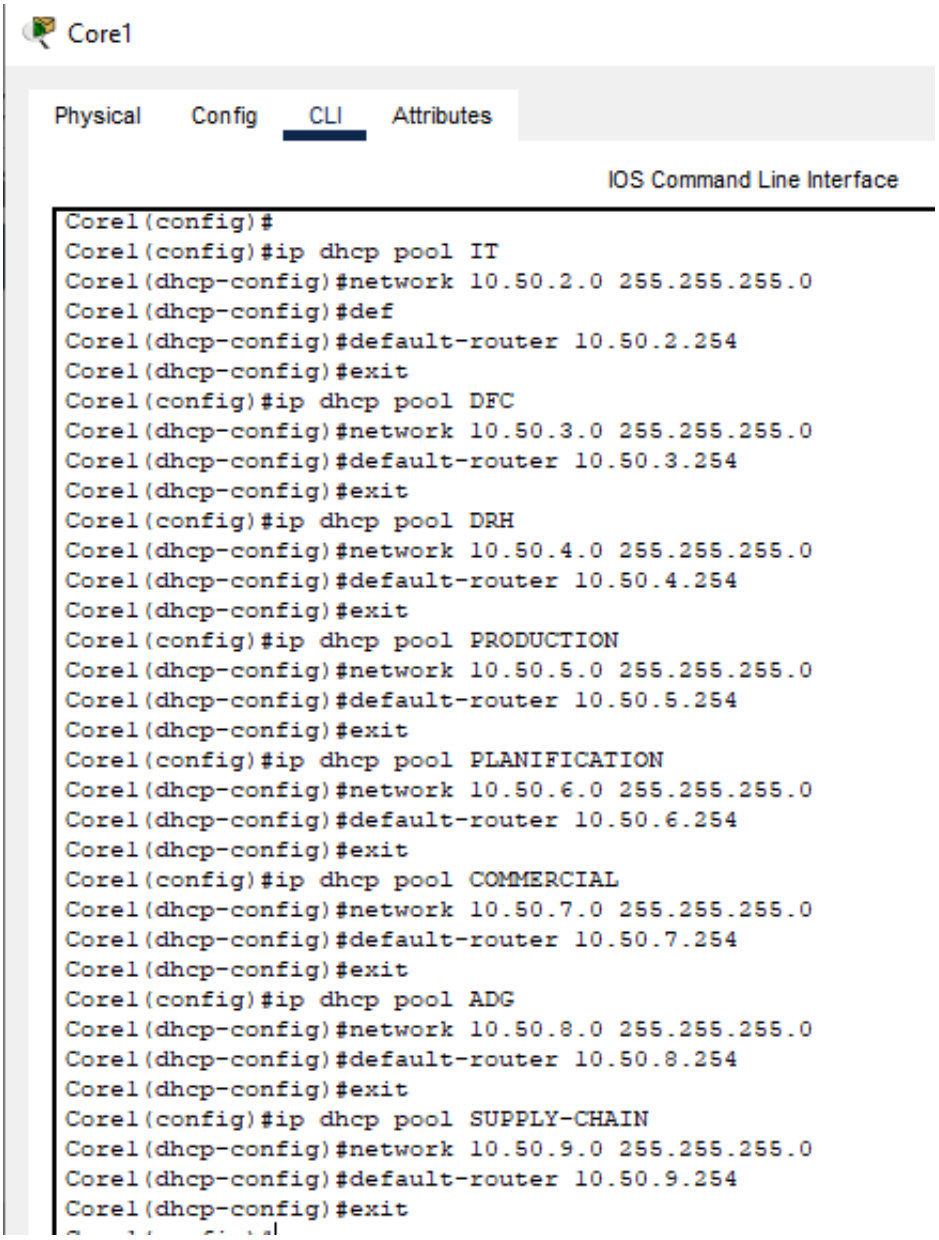

FIGURE 4.21 – La configuration DHCP au niveau de serveur Core1.

Ces configurations sont faites au niveau des deux switchs ce qui leurs permet d'attribuer automatiquement les adresses au PCs.
Pour garantir le succès de ce protocole et permettre au deux switchs d'attribuer des adresses sans provoquer de conflit, on va exclure les adresses de 127 à 251 sur le switch Core1 et de 1 à 126 sur le switch Core2.ceci est fait comme le montre la figure suivante : [Figure 4.22,Figure 4.23]

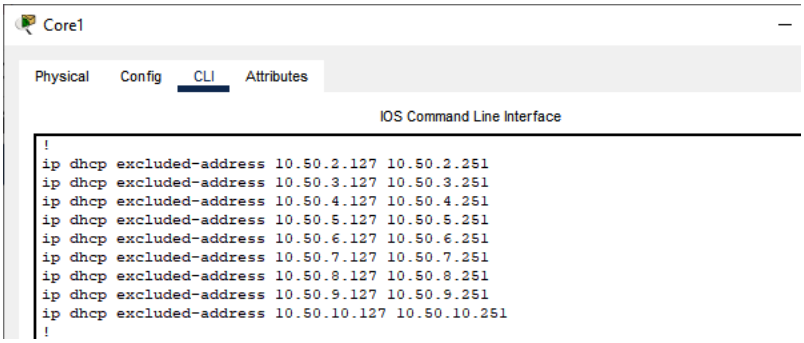

FIGURE 4.22 – L'exclusion d'adresses au niveau switch Core1

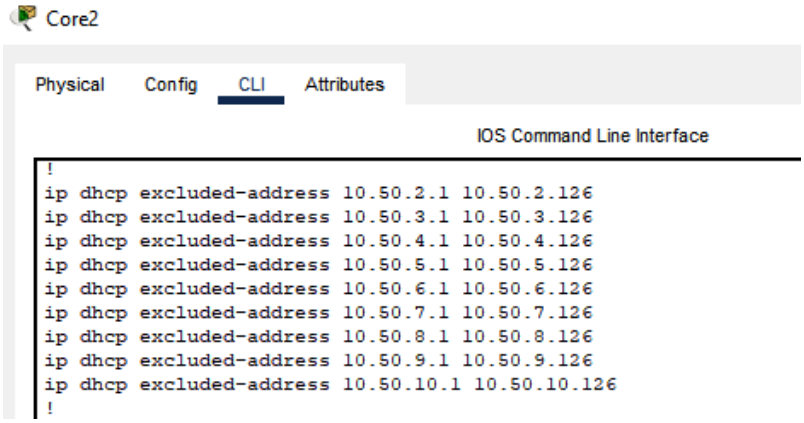

FIGURE 4.23 – L'exclusion d'adresses au niveau de switch Core2

La figure suivante montre l'attribution d'adresse pour un PC par le switch Core1 : [Figure 4.24]

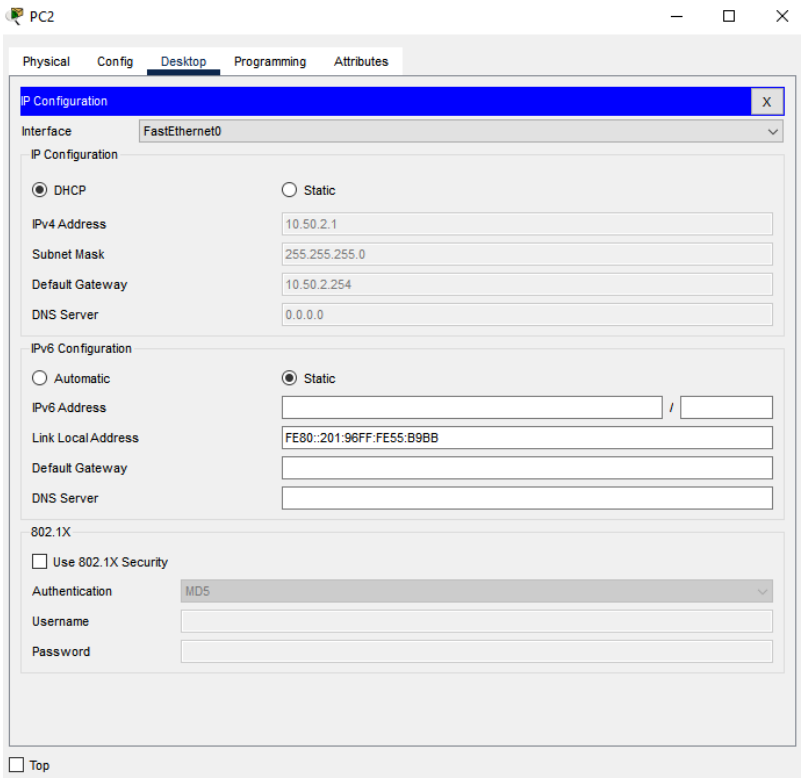

FIGURE 4.24 – L'adresse est attribuée correctement au niveau de PC2

4.11 La haute disponibilité

La haute disponibilité du réseau a pour but de garantir un service continu et sans interruption, et pour l'assurer nous allons essayer d'implémenter les protocoles suivants :

4.11.1 Le protocole HSRP (Hote Standby Routing Protocol)

Le protocole HSRP est un protocole qui assure la redondance de passerelle, pour l'implémenter on a besoins de plusieurs é quipements pour le mettre en oeuvre et cela en utilisant le logiciel Cisco Packet Tracer.

4.11.1.1 La configuration de protocole HSRP

La priorité 105 est attribuée au switch désigné comme actif, la priorité 100 est attribuée pour le switch en attente (standby). [Figure 4.25,Figure 4.26]

-Pour les VLANs (2 à 11) dans le Core1 :

```
Core1(config)#interface vlan 2
Core1(config-if)#standby 2 priority 105
Core1(config-if)#standby 2 ip 10.50.2.254
Core1(config-if)#standby 2 preempt
```

FIGURE 4.25 – La configuration de HSRP au niveau de switch Core1 (actif)

-Pour les VLANs de (2 à 11) dans le Core2 :

```
Core2(config)#interface vlan 2
Core2(config-if)#standby 2 priority 100
Core2(config-if)#standby 2 ip 10.50.2.254
Core2(config-if)#exit
```

FIGURE 4.26 – La configuration de HSRP au niveau de switch Core2 (en attente)

La figuration suivante montre la configuration de protocole STP sur les deux commutateurs Core1 et Core2 :

```
Core1(config)#sp
Core1(config)#spanning-tree vlan 2-11 prio
Core1(config)#spanning-tree vlan 2-11 priority 4096
Core1(config)#end
Core1#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
Core1#
```

FIGURE 4.27 – La configuration de protocole STP sur le commutateur Core1.

On a appliqué le protocole STP sur les VLANs de 2 à 11 en donnant la priorité 4096 au switch Core1.

```
Core2(config)#spa
Core2(config)#spanning-tree vlan 2-11 pri
Core2(config)#spanning-tree vlan 2-11 priority 8192
Core2(config)#end
Core2#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
Core2#
```

FIGURE 4.28 – La configuration de protocole STP sur le commutateur Core2.

On a appliqué le protocole STP sur les VLANs de 2 à 11 en donnant la priorité 8192 au switch Core2.

4.11.1.2 Vérification et tests de validité

On a présenter dans ce qui suit des tests de validité pour s'assurer de bon fonctionnement de protocole HSRP.

- **Vérification de protocole VTP**

On obtient cette figuration on tapant la commande **"show vtp status"** : [Figure 4.29,Figure 4.30]

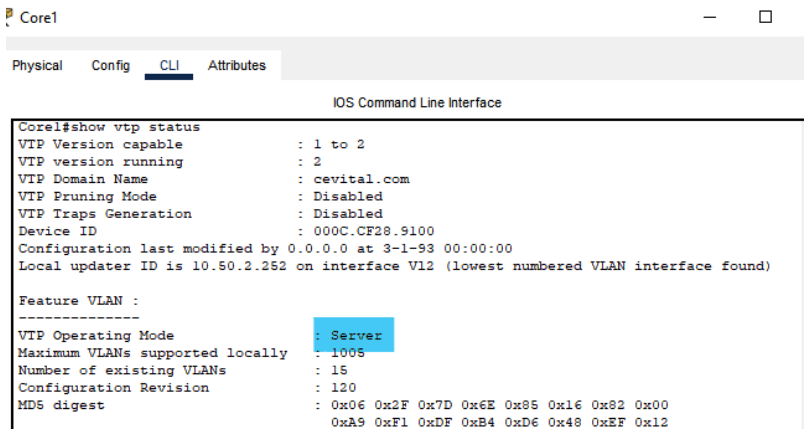

FIGURE 4.29 – Test VTP server.

L'ajout, la modification et la suppression des VLANs se fait au niveau du commutateur Core1 (configuré en mode server).

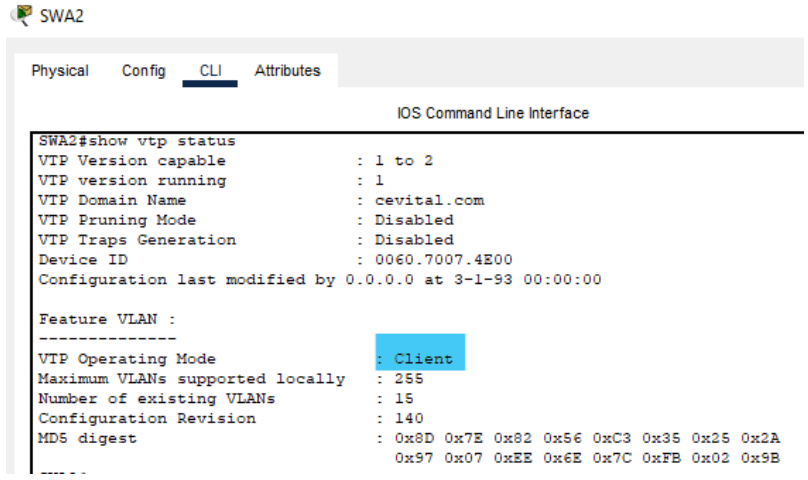

FIGURE 4.30 – Test VTP client.

- **Vérification de la configuration de protocole HSRP**

Les figures suivantes montrent les états de chaque commutateur. On a tapé la commande **"show standby brief"** au niveau de commutateur Core1 : [Figure 4.31]

La priorité attribuée au commutateur Core1 est supérieure a celle de Core2, donc dans ce cas le Core1 est actif et le Core2 est en attente (standby).

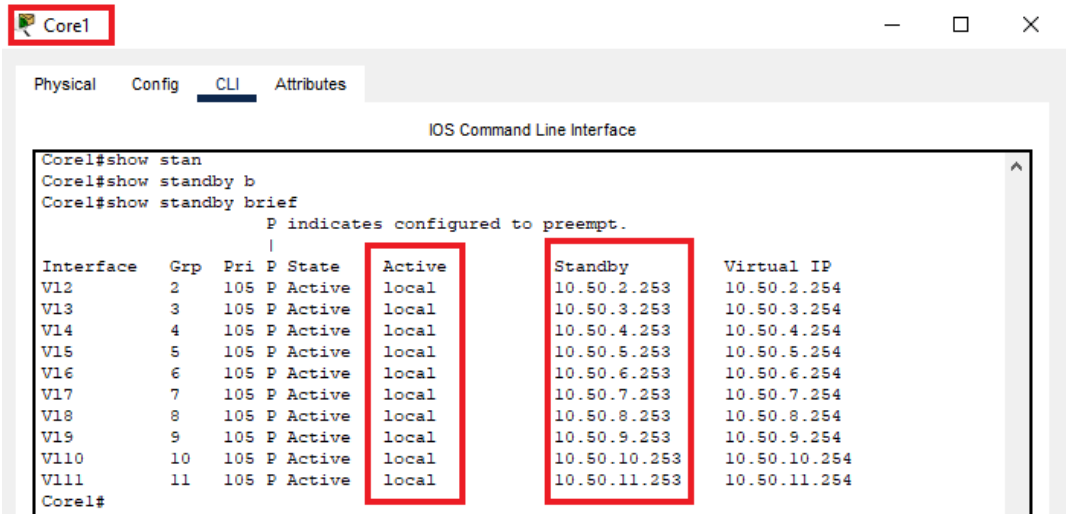

FIGURE 4.31 – Capture montrant l'état de chaque commutateur Core.

Avec cette configuration, en cas de défaillance de Core1, le Core2 deviendra le switch actif.

- **Vérification de ping entre VLANs**

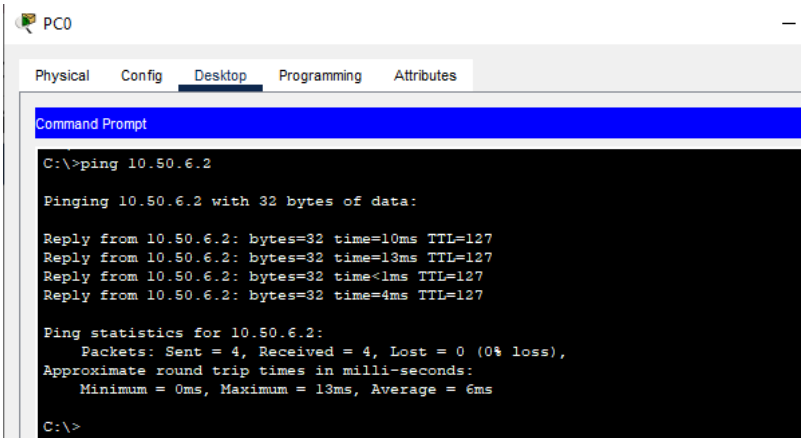

FIGURE 4.32 – Test de ping entre VLANs différents

On a testé la connectivité entre deux PCs des VLANs différents. Le test a été reussi.

- **Vérification de la disponibilité du réseau**

On a éteint le commutateur actif (Core1), le résultat figure ci-dessous : [Figure 4.33]

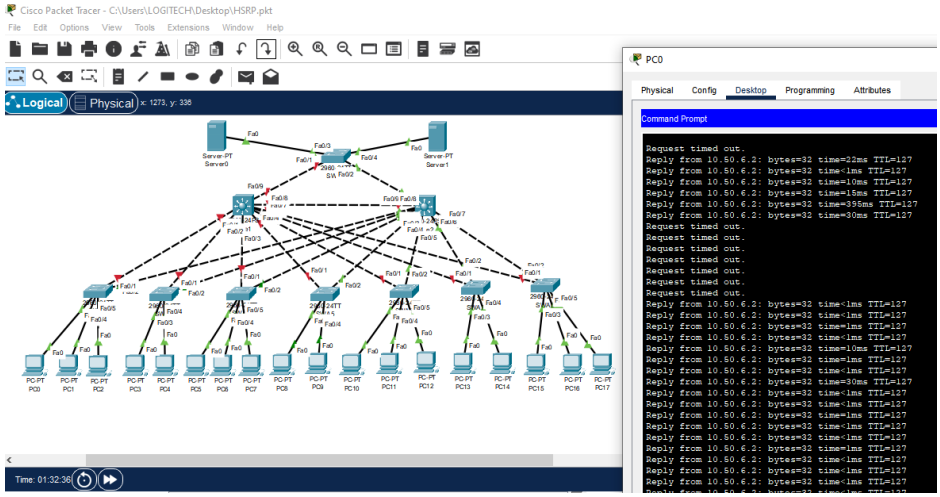

FIGURE 4.33 – Le Core2 a pris le relai

Comme le montre la figure précédente, le switch Core2 a pris le relai. Nous vérifions maintenant, l'adresse attribuée au PC0 : [Figure 4.34]

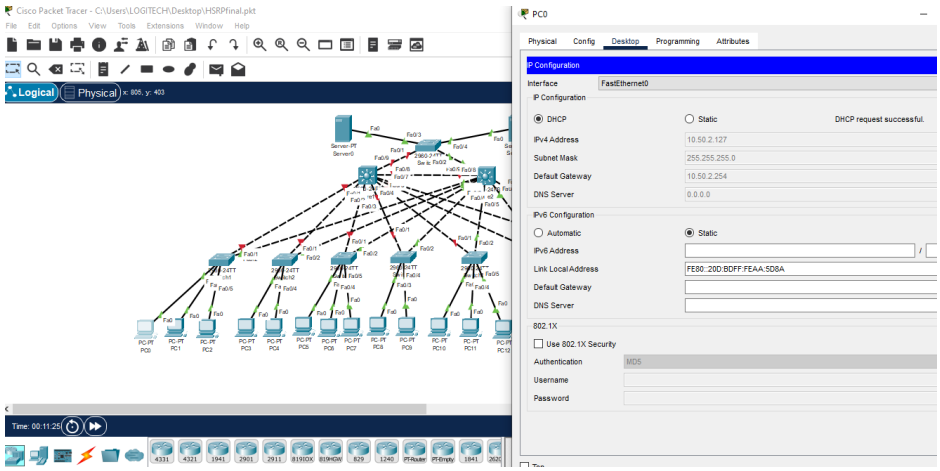

FIGURE 4.34 – L'attribution d'adresse par le switch Core2.

La capture précédente montre que le switch Core2 a attribué l'adresse au PC0

On a rallumé le switch Core1, comme le montre la figure ci-dessous : [Figure 4.35]

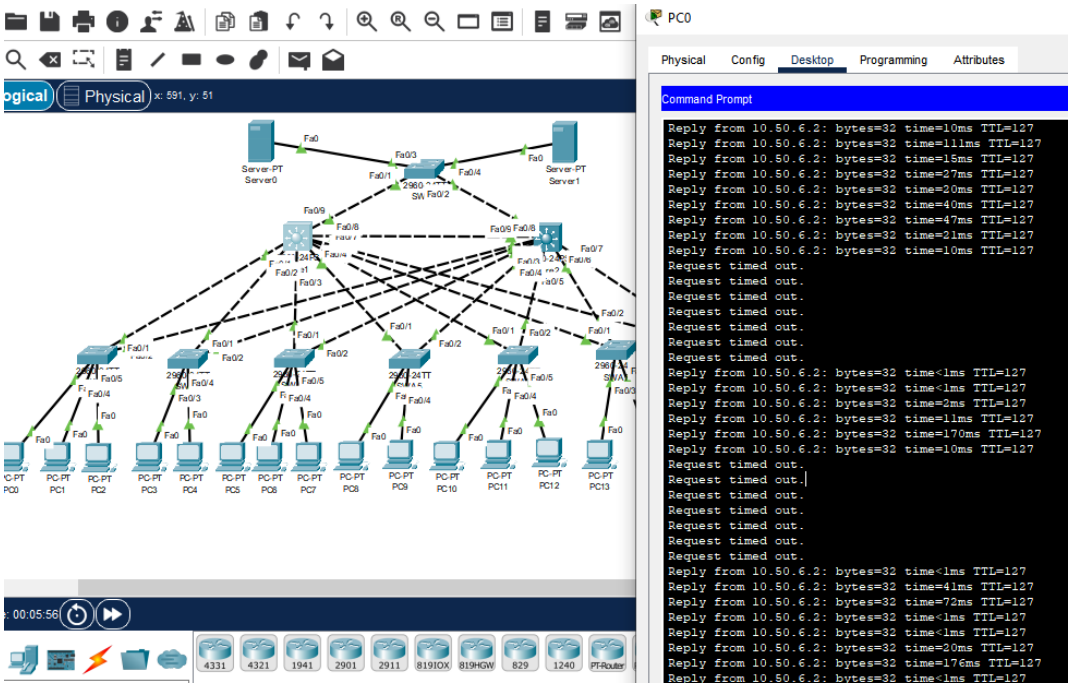

FIGURE 4.35 – Le commutateur Core1 rallumé

Le Core1 a repris son état actif à l'aide de la commande **"preempt"**

4.11.2 L'implémentation du protocole GLBP (Gateway Load Balancing Protocol)

Pour implémenter le protocole de la redondance de passerelle et l'équilibrage de charge GLBP, nous allons utiliser le logiciel GNS3.

4.11.2.1 Présentation d'une petite partie de l'architecture.

L'architecture précédente illustre une petite partie de notre architecture en prenant les équipements essentiels qui vont nous permettre la simulation du fonctionnement du protocole GLBP.

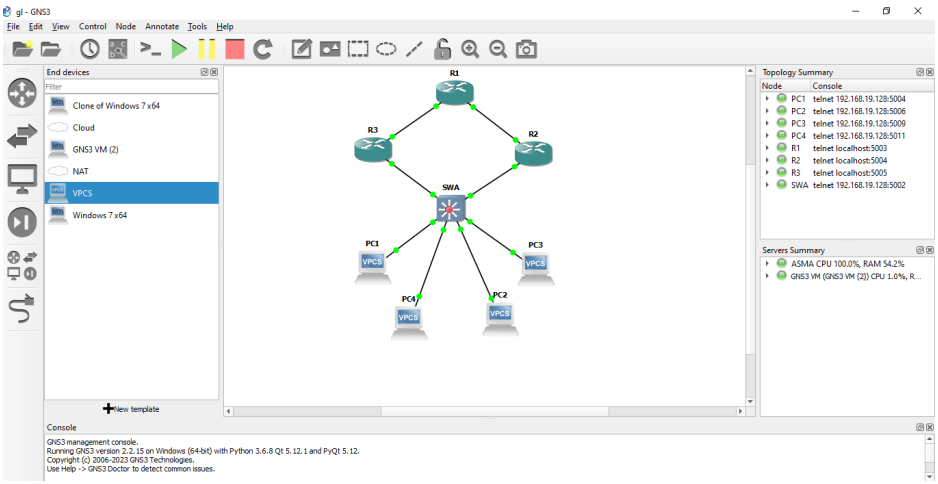

FIGURE 4.36 – Une petite partie de l'architecture.

Avant de passer à la configuration de ce protocole on va passer par plusieurs étapes de configuration. D'abord nous commençons par le protocole de routage OSPF, puis la configuration des interfaces des routeurs, l'attribution des adresses aux PCs d'une manière statique. Enfin configurer le protocole GLBP. On va montrer dans ce qui suit les étapes citées au dessus ainsi que les tests de validation que nous allons effectuer afin de s'assurer du bon fonctionnement de ce protocole.

4.11.2.2 La configuration des équipements

- **La configuration de protocole OSPF**

On a configuré le protocole OSPF au niveau des trois routeurs, en déclarant les adresses 10.60.1.0/24, 10.70.1.0/24 et toutes les adresses des VLANs crées, la configuration est faite comme suit : [Figure 4.37]

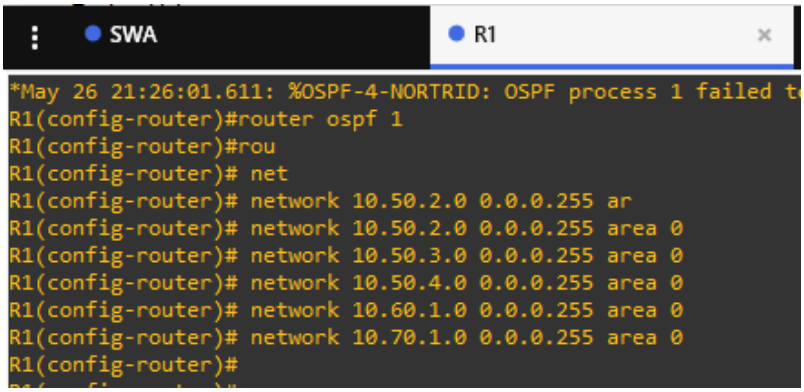

FIGURE 4.37 – La configuration de protocole OSPF.

La vérification de la configuration de protocole OSPF est faite à l'aide de la commande **"show ip route".** [Figure 4.38]

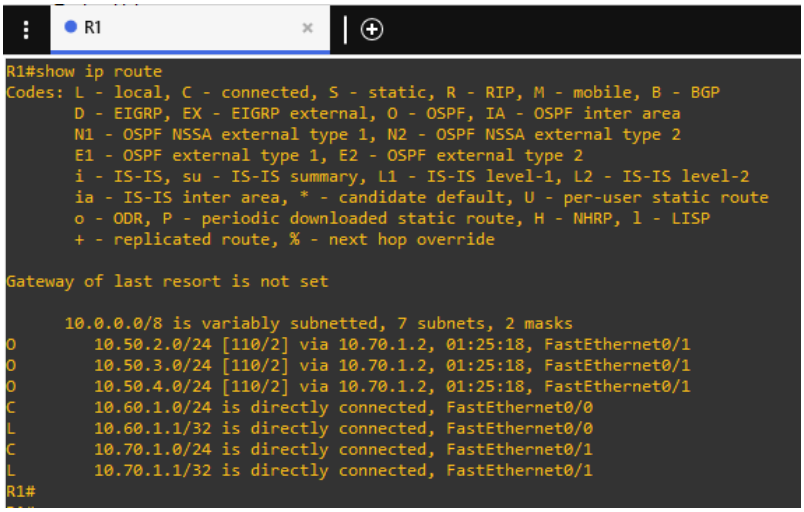

FIGURE 4.38 – La vérification de protocole OSPF.

On peut facilement observer les routes directement et indirectement connectées au routeur R1.

- **La configuration des interfaces de routeur R1**

On a configuré les deux interfaces de routeur R1 comme suit : [Figure 4.39]

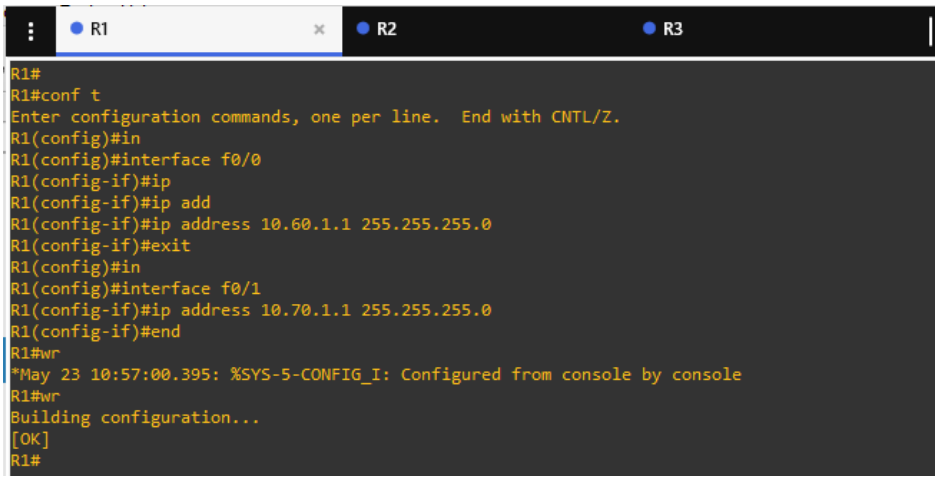

FIGURE 4.39 – La configuration des interfaces de R1.

- **La configuration des interfaces de R2 et R3**

La capture suivante montrera les étapes de configuration des interfaces de routeur R2 et R3 ainsi que la création des sous interfaces. [Figure 4.40,Figure 4.41]

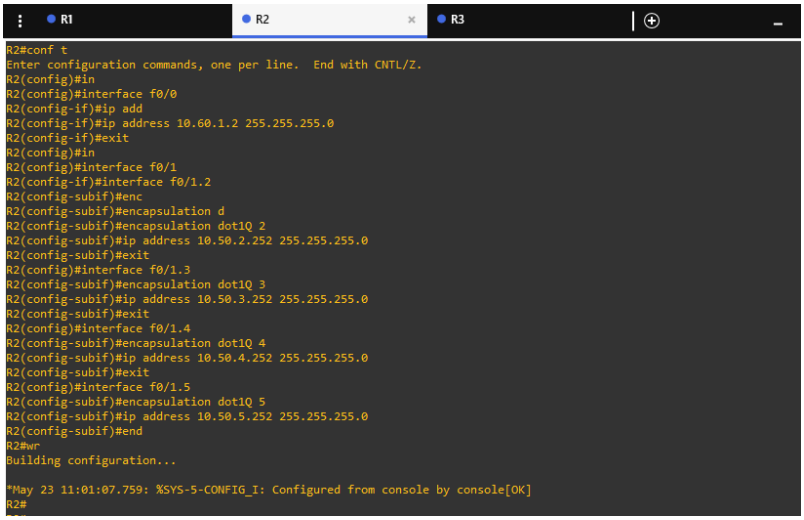

FIGURE 4.40 – La configuration des interfaces de R2.

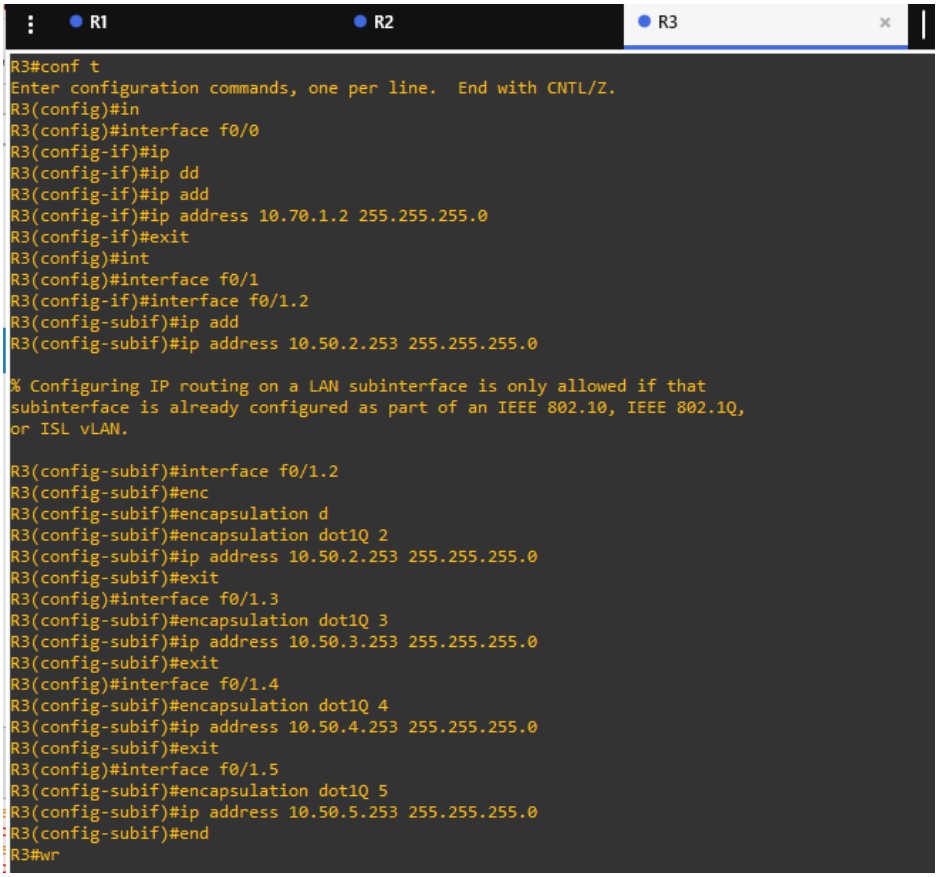

FIGURE 4.41 – La configuration des interfaces de R3.

- **La configuration des liens trunk et access**

La figure suivante montrera comment les liens sont configurés en mode trunk au niveau de switch. [Figure 4.42]

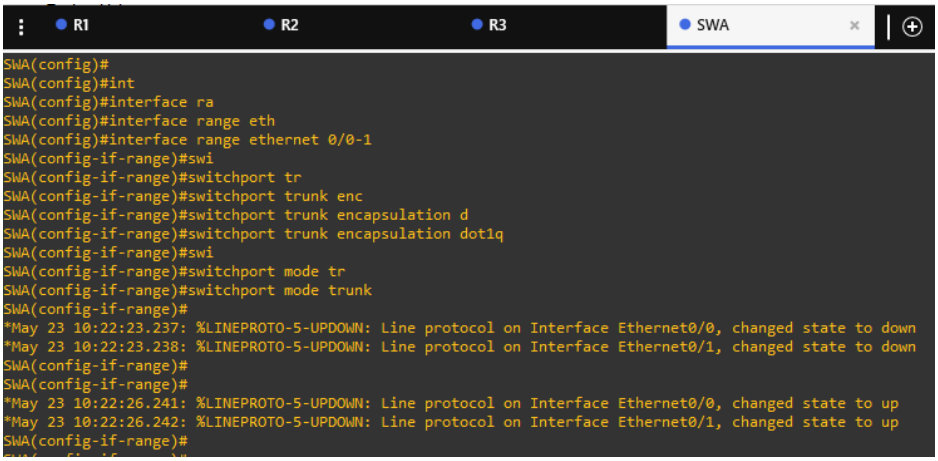

FIGURE 4.42 – la configuration de mode trunk.

La figure suivante montrera la configuration des liens en mode accès au niveau de switch. [Figure 4.43]

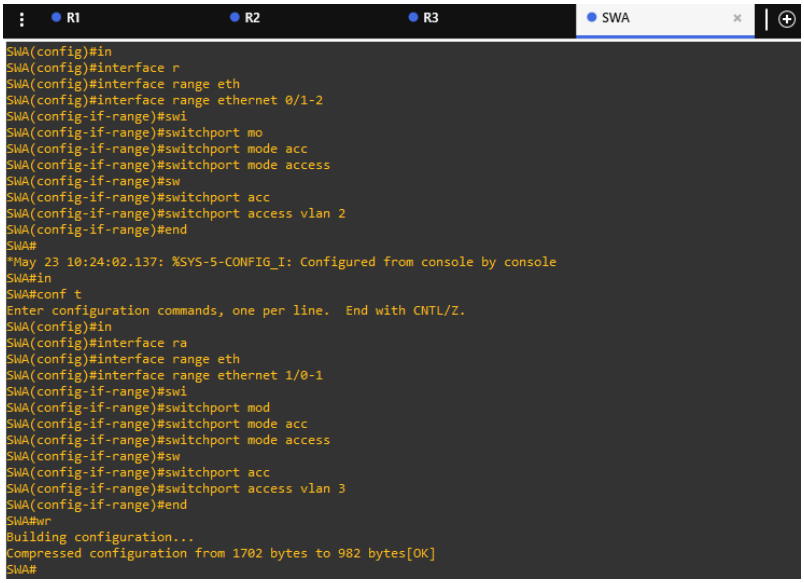

FIGURE 4.43 – La configuration de mode access.

- **La création des VLANs au niveau de switch**

La création et l'attribution de noms au VLANs est faite comme suit : [Figure 4.44]

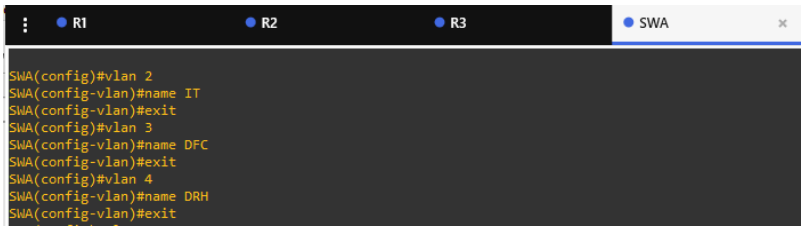

FIGURE 4.44 – La création des VLANs.

- **L'attribution d'adresses aux PCs**

Les adresses sont attribuées aux PCs d'une manière statique comme suit : [Figure 4.44]

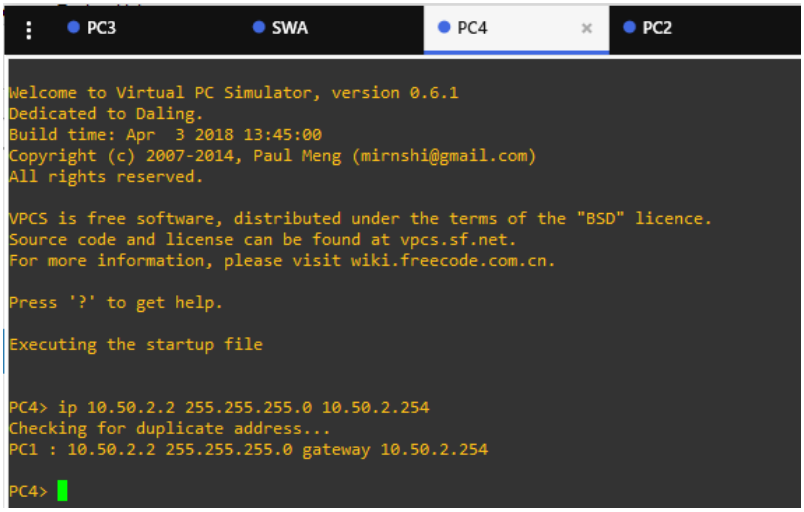

FIGURE 4.45 – L'attribution d'adresse au PC4.

4.11.2.3 La configuration de protocole GLBP

On va voir dans ce qui suit toutes les étapes de configuration de protocoles GLBP sous GNS3.

- **Au niveau de routeur R2**

La configuration de protocole GLBP pour tous les VLANs est faite comme suit : [Figure 4.46]

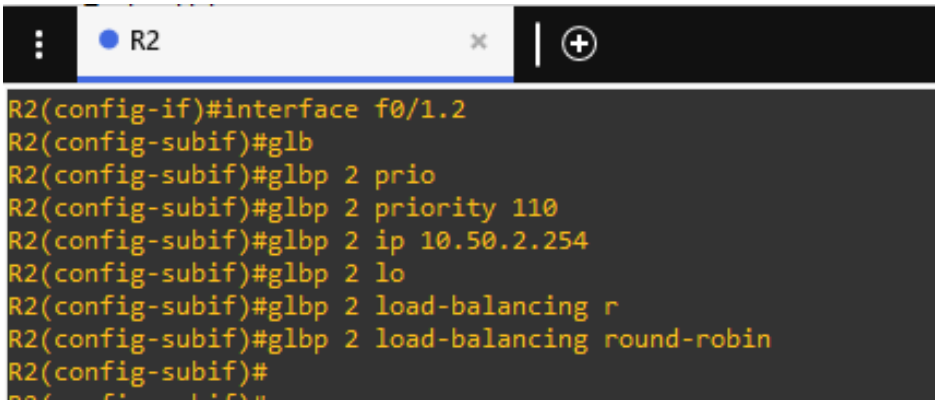

FIGURE 4.46 – La configuration de protocole GLBP au niveau de routeur R2 (AVG).

Le routeur R2 est désigné comme AVG avec la plus haute priorité 110

- **Au niveau de routeur R3**

La configuration de protocole GLBP pour tous les VLANs est faite comme suit : [Figure 4.47]

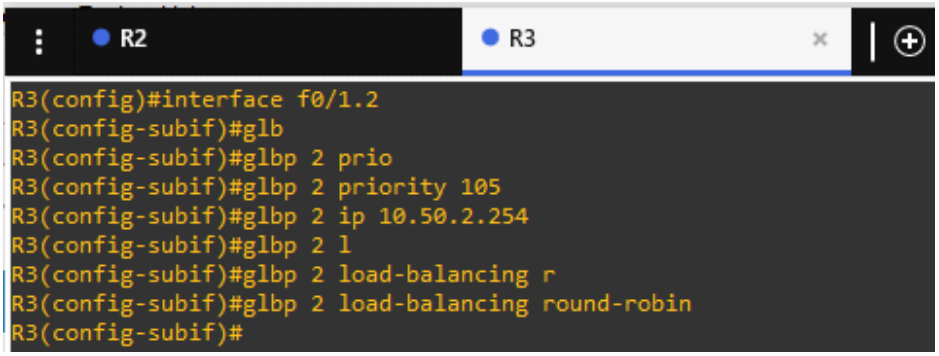

FIGURE 4.47 – La configuration de protocole GLBP au niveau de routeur R3 (AVG Standby).

Le routeur R2 est désigné comme AVG standby avec la priorité 105 inférieur que celle de l'AVG.

4.11.2.4 Tests de validations.

Apres la configuration, des tests de validation sont appliqués pour savoir si le protocole implémenté fonctionne bien. Les captures suivantes montrent ceci :

- **Vérification de la redondance de passerelle et l'équilibrage de charge**

On a coupé le lien entre le routeur désigné comme AVG et le switch d'accés, on observe que le routeur désigné comme AVG standby est devenu le routeur AVG. [Figure 4.48]

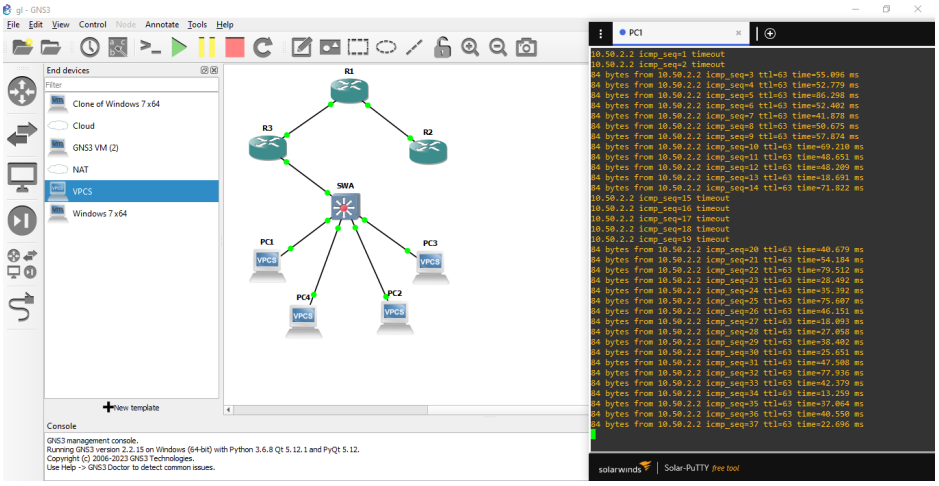

FIGURE 4.48 – Test de ping continu.

Après la reconnexion des deux équipements, à l'aide de la commande **"preempt"** l'ancien routeur AVG a repris son état comme le montre la figure suivante. [Figure 4.49]

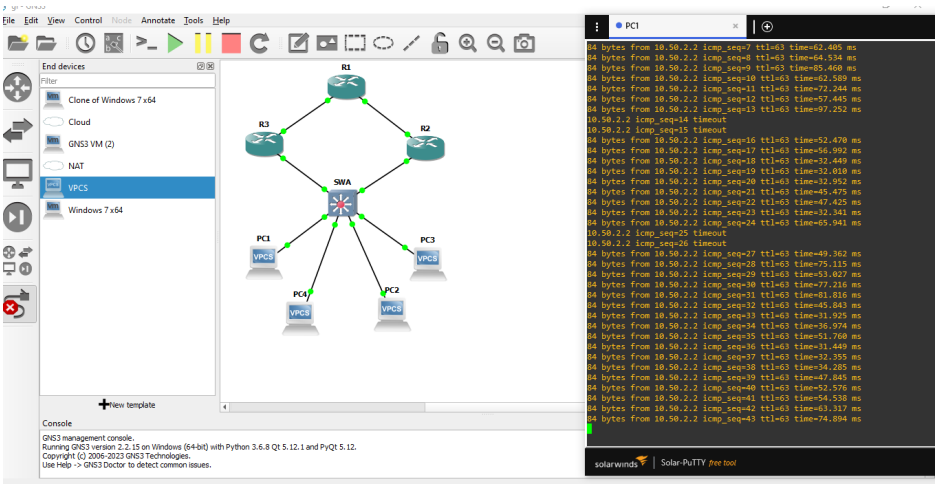

FIGURE 4.49 – Capture montrant la reprise l'AVG.

On accede à l'un des routeurs et on tape la commande **"show glbp"** pour afficher les adresses mac des routeurs, la figure suivante montre comment ceci est fait : [Figure 4.50]

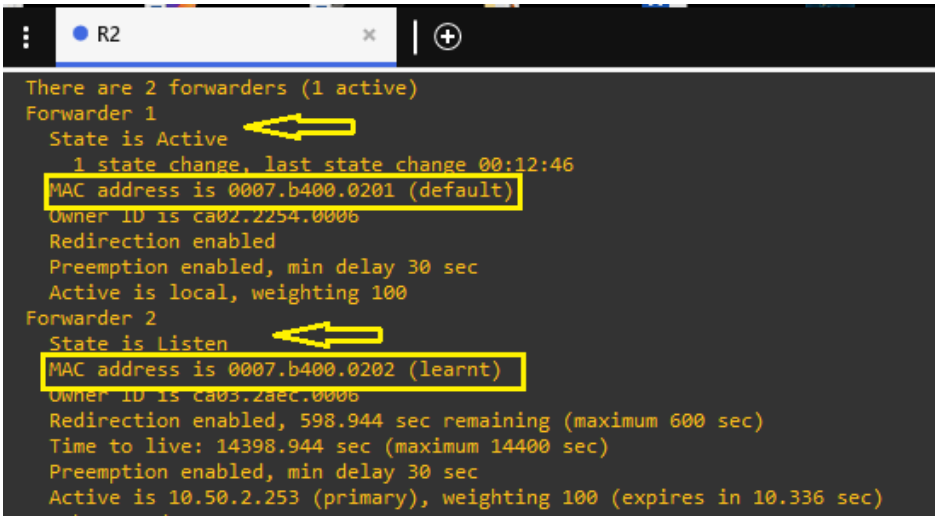

FIGURE 4.50 – Les adresses MAC des routeurs

Après le test de ping sur deux machines différentes, on tape la commande **"show arp"**, pour afficher la table ARP. [Figure 4.51,Figure 4.52]

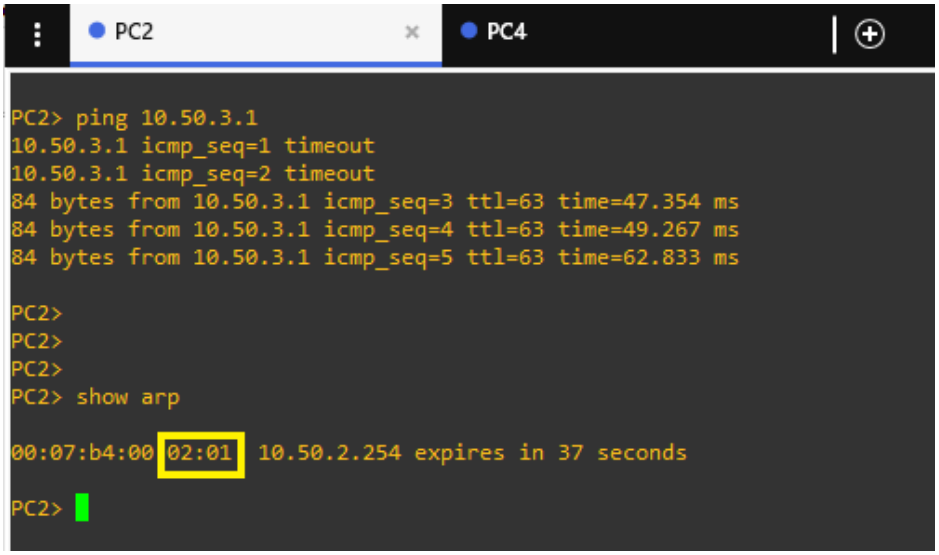

FIGURE 4.51 – L'adresse MAC affichée au niveau de PC2.

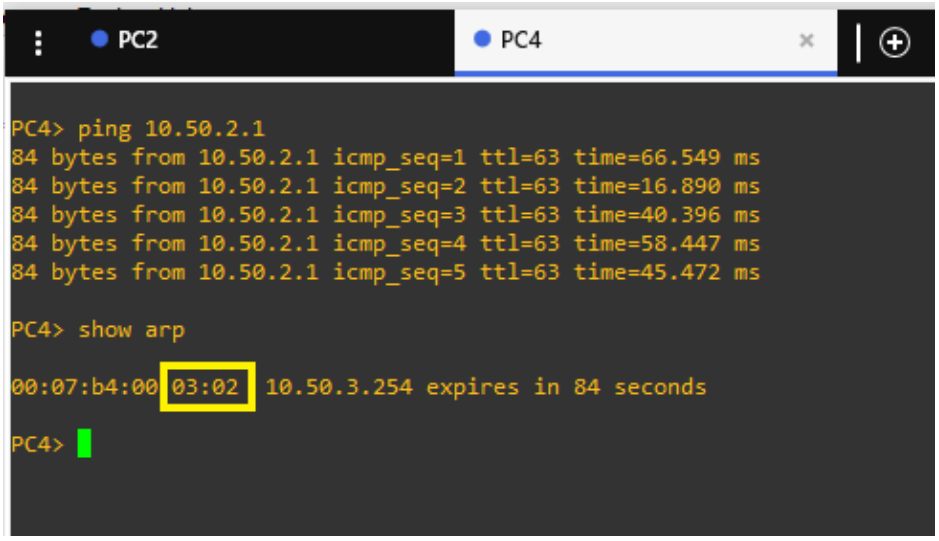

FIGURE 4.52 – L'adresse MAC affichée au niveau de PC4.

On remarque que les adresses MAC sont différentes ce qui signifie que le premier paquet est passé par le premier routeur et le deuxième paquet par le deuxième routeur. Cela veut dire que l'équilibrage des charges est assuré.

Solution choisie

Après implémentation des deux protocoles, on a trouvé que le protocole HSRP a assuré la redondance mais y'avait une surcharge sur un seul commutateur, aussi le protocole GLBP a garenti l'équilibrage de charges du réseau ainsi que la tolérance aux pannes des équipements mais le réseau été lent.

On est arrivé a trouver une solution qui répondra aux besoins de l'entreprise, en garantissant la

redondance avec le protocole HSRP en lui ajoutant l'équilibrage de charges c'est-à-dire partager les VLANs du réseau sur plusieurs commutateurs actif, On va expliquer son fonctionnement dans ce qui suit :

4.11.3 La redondance de passerelle HSRP avec équilibrage de charge par VLANs

On va essayer d'implémenter notre solution qui est de configurer les deux switchs Core de façons à laquelle ils assurent la redondance et l'équilibrage de charge au même temps. D'abord nous allons refaire toutes les étapes de configuration du protocole HSRP en changeant les priorités des VLANs et celles des équipements. On va montrer dans ce qui suit les configurations et les tests de validation que nous allons effectuer à fin de s'assurer du bon fonctionnement de cette solution.

4.11.3.1 La configuration de protocole HSRP

Au niveau de Core1 :

```
Core1(config)#interface vlan 2
Core1(config-if)#standby 2 priority 105
Core1(config-if)#standby 2 ip 10.50.2.254
Core1(config-if)#standby 2 preempt
```

FIGURE 4.53 – La configuration de HSRP dans le Core1(priorité supérieur).

```
Core1(config)#interface vlan 7
Core1(config-if)#standby 7 priority 100
Core1(config-if)#standby 7 ip 10.50.7.254
Core1(config-if)#standby 7 preempt
Core1(config-if)#exit
```

FIGURE 4.54 – La configuration de HSRP dans le Core1(priorité inférieur).

Les priorité sont attribuées comme suit :
- La priorité 105 pour les VLANs de 2 à 6.
- La priorité 100 pour les VLANs de 7 à 11.

Au niveau de Core2 :

```
Core2(config-if)#interface vlan 2
Core2(config-if)#standby 2 priority 100
Core2(config-if)#standby 2 ip 10.50.2.254
Core2(config-if)#exit
```

FIGURE 4.55 – La configuration de HSRP dans le Core2 (priorité inférieur).

```
Core2(config)#interface vlan 7
Core2(config-if)#standby 7 priority 105
Core2(config-if)#standby 7 ip 10.50.7.254
Core2(config-if)#exit
```

FIGURE 4.56 – La configuration de HSRP dans le Core2 (priorité supérieur).

Les priorité sont attribuées comme suit :
- La priorité 100 pour les VLANs de 2 à 6.
- La priorité 105 pour les VLANs de 7 à 11.

4.11.3.2 Configuration du protocole STP

La petite priorité dans le protocole STP est plus prioritaire que celle supérieure. Au niveau du Switch Core1 : [Figure 4.57,Figure 4.58]

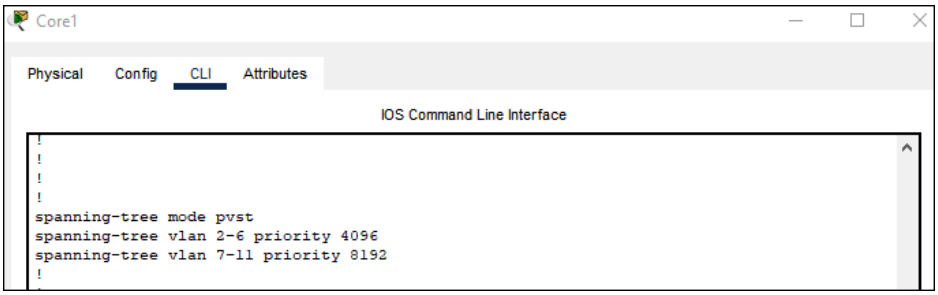

FIGURE 4.57 – Configuration du STP sur le Switch Core1

Au niveau du Switch Core2 :

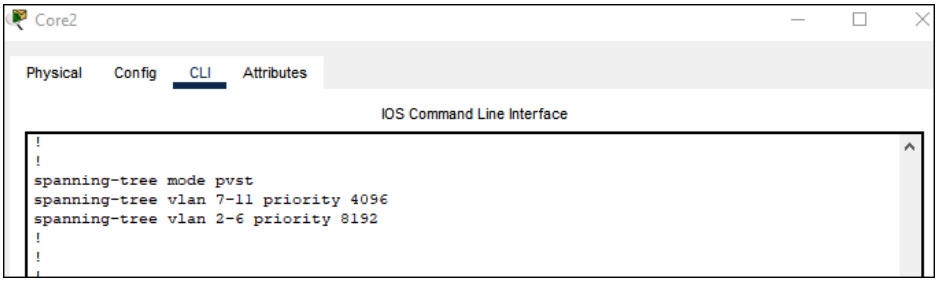

FIGURE 4.58 – Configuration du STP sur le Switch Core2

La configuration du protocole STP sert à éliminer la boucle entre les trois switch reliés. On a attribué une priorité pour les deux switchs Core. Dans notre cas le Core1 est prioritaire pour les VLANs de 2 à 6 et le Core2 est prioritaire pour les VLANs de 7 à 11.

4.11.3.3 Testes de validation

On va vérifier dans ce qui suit la configuration du protocole HSRP et tester si la redondance et l'équilibrage de charges sont atteintes.

- **Teste de connectivité entre deux PCs**

On va montrer dans ce qui suit le test de connectivité entre deux PCs : [Figure 4.59]

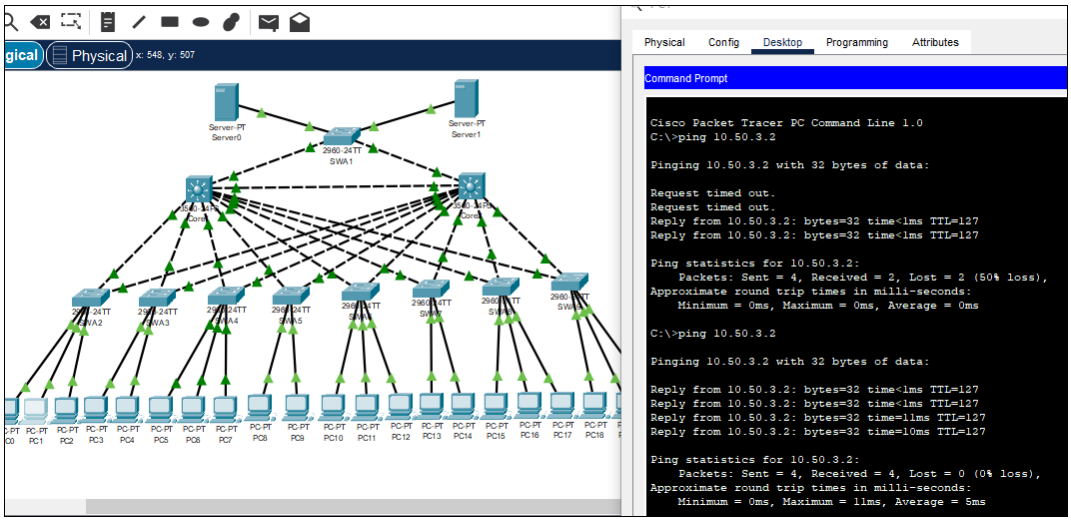

FIGURE 4.59 – Test de connectivité

Le test a été réussi comme le montre la figure ci-dessus.

- **L'attribution d'adresses aux PCs**

On va montrer dans ce qui suit comment les adresses sont distribuées. [Figure 4.60,Figure 4.61]

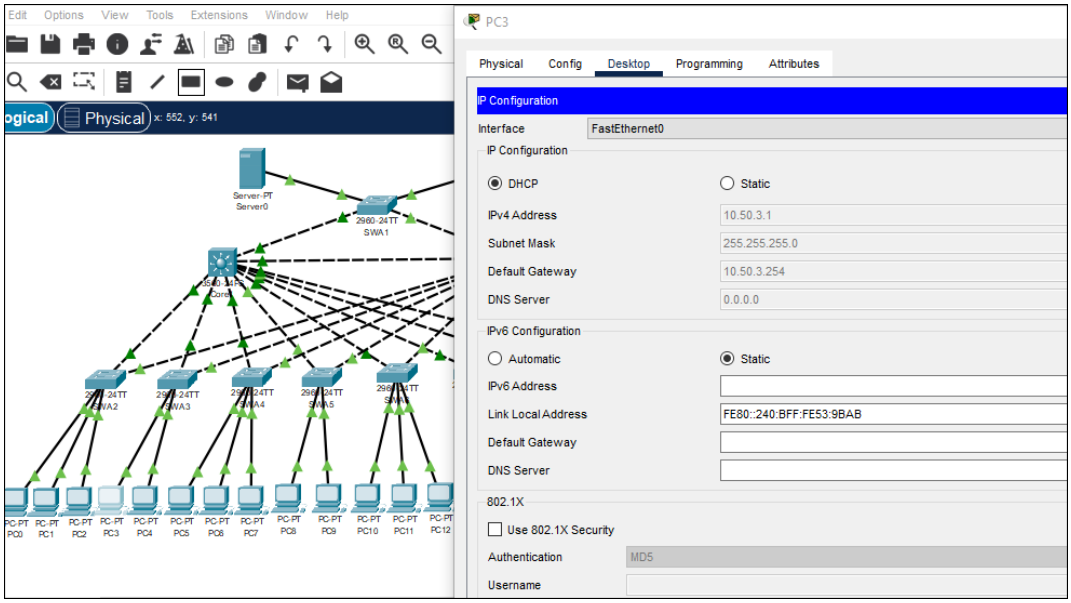

FIGURE 4.60 – Attribution des adresses par le Switch Core1

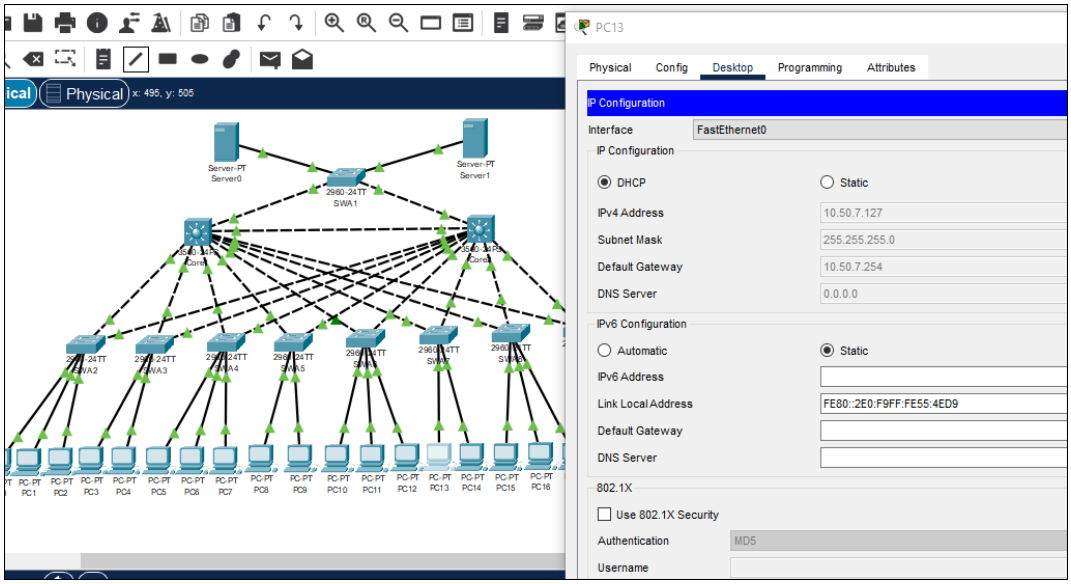

FIGURE 4.61 – Attribution des adresses par le Switch Core2

-les adresses des PCs appartenant aux VLANs de 2 à 6 sont attribuées par le commutateur Core1

- les adresses des PCs appartenant aux VLANs de 7 à 11 sont attribuées par le commutateur Core2.

- **Vérification de l'équilibrage de charge par VLANs.**

On tape la commande **"show standby brief"** pour obtenir ce qui suit : [Figure 4.62]

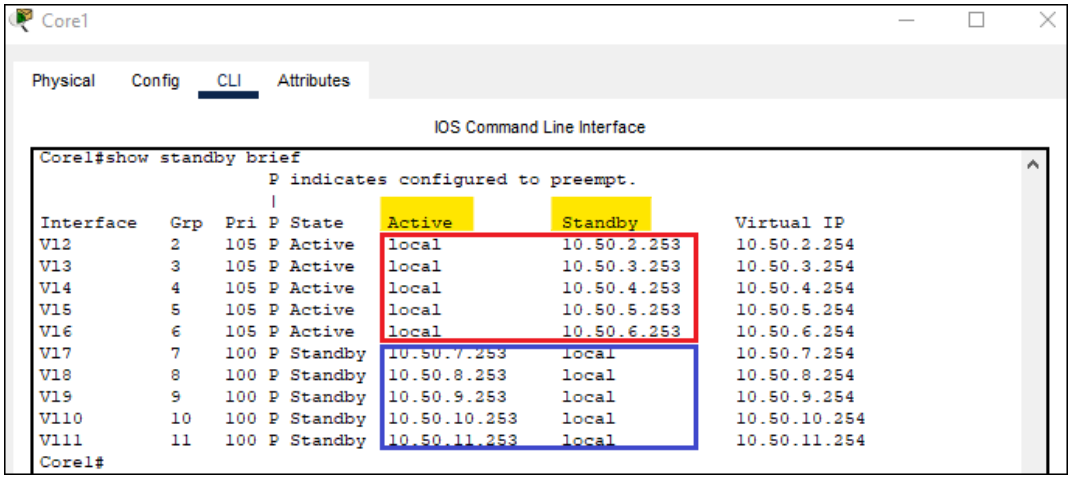

FIGURE 4.62 – La répartiton des VLANs sur les deux swutch core

On peut facilement distinguer que le switch Core1 est actif pour les VLANs de 2 à 6 et passif pour les VLANs de 7 à 11, contrairement au switch Core2 qui est actif pour les VLANs de 7 à 11 et passif pour les VLANs de 2 à 6.

- **Vérification de la redondance**

On a mit en pause le Core1, le Core2 a pris le relai comme l'illustre la figure suivante : [Figure 4.63]

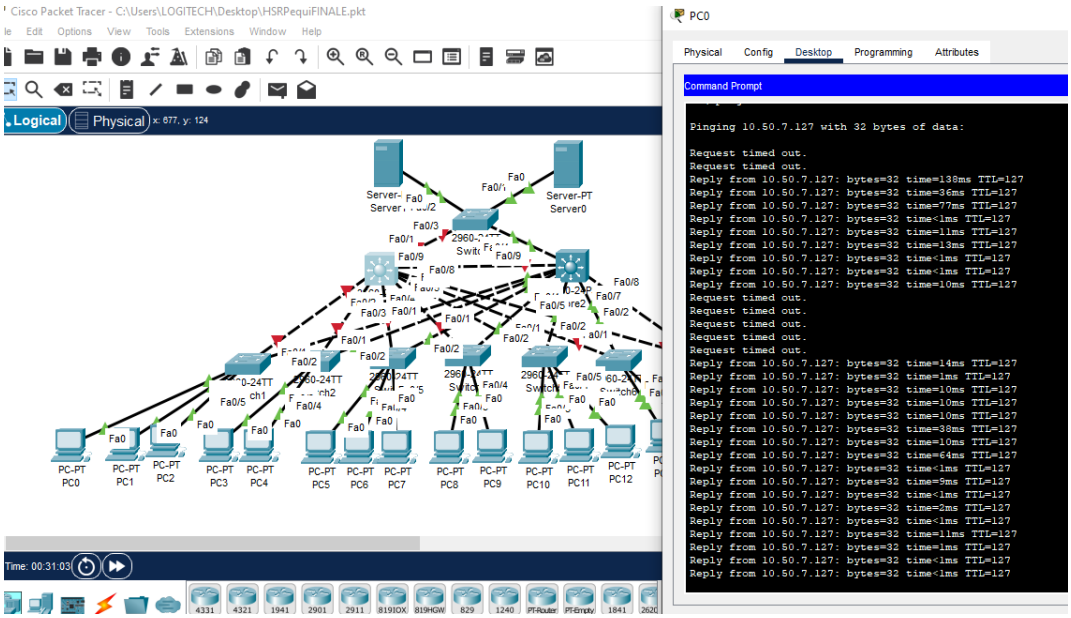

FIGURE 4.63 – Le switch Core1 est mis en pause

On doit après revérifier l'adresse du PC0, le Core2 lui a attribué une adresse comme suit : [Figure 4.64]

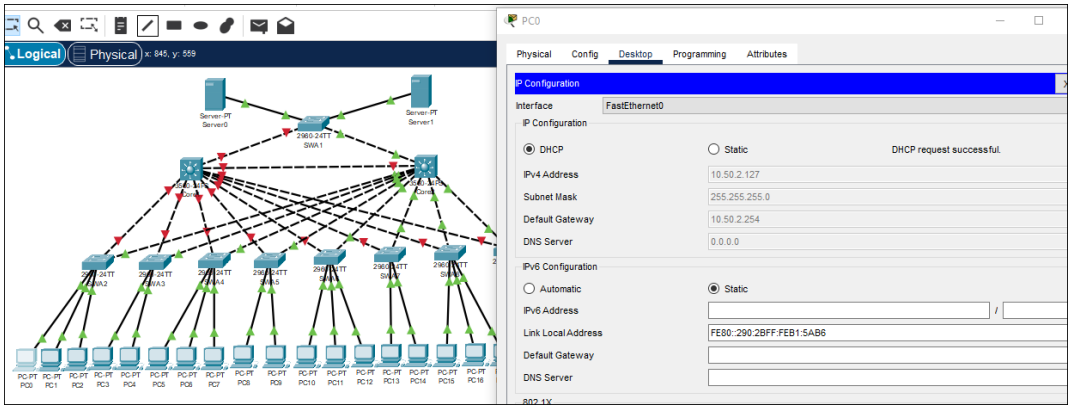

FIGURE 4.64 – Attribution d'adresse par le switch Core2

Le Core2 est devenu le responsable de la distributions d'adresses pour tous les PCs. Maintenant nous rallumons le Core1, est vérifions si ce dernier reprendra son travail en tant que le switch actif. [Figure 4.65]

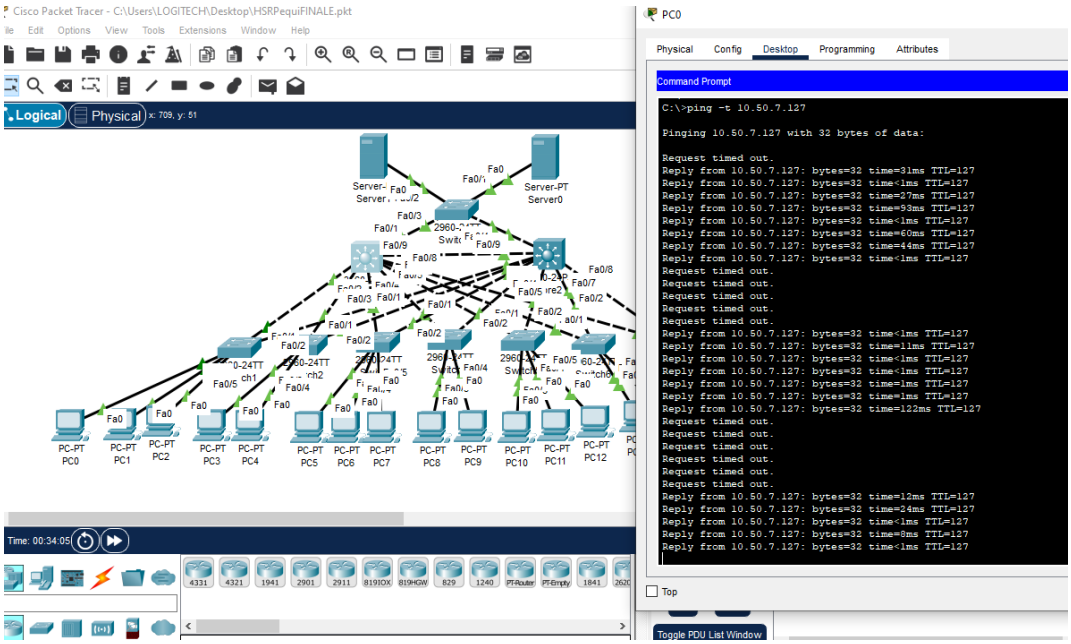

FIGURE 4.65 – Switch Core1 remis en oeuvre

Comme le montre la figure au dessus, le Core1 a repris sont état actif, cela est devenu possible à l'aide de la commande **"preempt"**. Réattribution des adresses par le switch Core1 comme suit : [Figure 4.66]

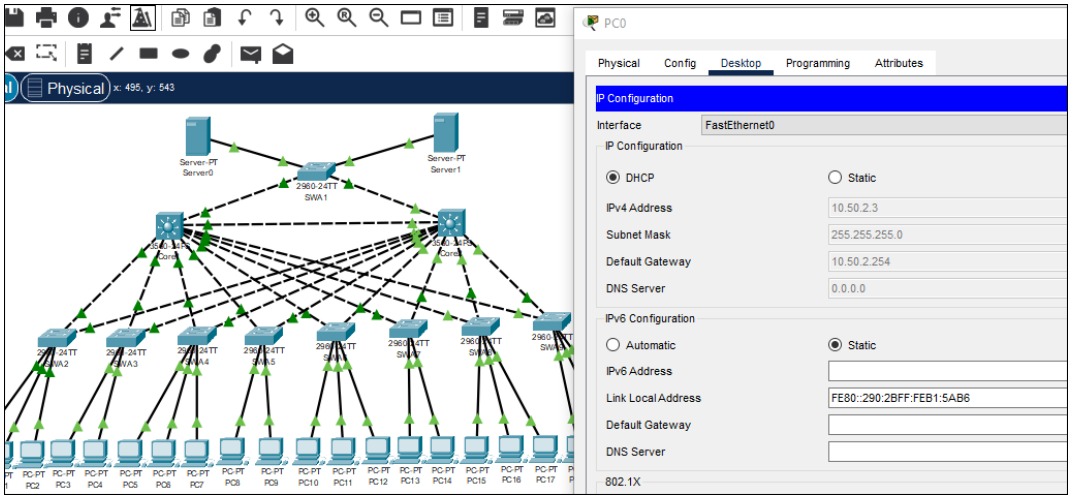

FIGURE 4.66 – Adresse de PC0

Le commutateur Core1 a distribué à nouveau l'adresse au PC0, cela signifie que ce dernier a repris son travail comme switch actif.

On est arrivé à une solution plus pertinente par rapport à notre objectif celle ci sera mieux apprécié par l'entreprise pour garantir la redondance avec équilibrage de charge. On a essayé de fusionner les deux avantages des deux protocoles, assurer la redondance (la tolérance aux pannes), et l'équilibrage de charges par VLANs. Notre solution consiste à diminuer la charge sur un seul switch Core cela veut dire que les VLANs serons partager sur plusieurs commutateurs actif, la moitié des VLANs vont prendre le Core1 comme passerelle et le reste vont prendre le Core2 comme passerelle, au même temps , si l'un des switchs Core tombe en panne le deuxième va prendre le relai et prendre en charge tout les VLANs.

4.12 Conclusion

Dans ce dernier chapitre nous avons implémenté les deux protocoles sur notre architecture améliorée, puis nous avons opté pour une solution qui combine la redondance de la passerelle et l'équilibrage de charge par VLANs. Après des tests de validation, les résultats montrent une efficacité satisfaisante qui répondent à notre objectif.

Conclusion générale et perspectives

En conclusion, notre travail visait principalement à atteindre l'objectif fixé par l'entreprise Cevital, qui consiste à mettre en place un réseau hautement disponible afin d'assurer la continuité et le bon fonctionnement de son service, tout en augmentant sa capacité de production.

Nous avons cherché, tout au long de ce travail, à trouver des solutions à notre problématique initiale, qui était la discontinuité du réseau rencontrée par l'entreprise. Plusieurs éléments ont contribué au mauvais fonctionnement du service, tels que la structure hiérarchique du réseau et sa surcharge en raison de sa taille.

Nous avons choisi de nous concentrer sur deux protocoles de haute disponibilité : le protocole HSRP, qui assure la redondance et a été mis en oeuvre sur le logiciel Cisco Packet Tracer, et le protocole GLBP, qui assure la redondance ainsi que la répartition de charge du réseau sur plusieurs éléments et a été implémenté sur le logiciel GNS3.

Au final, nous avons opté pour une solution plus intéressante et appréciée par l'entreprise, qui consiste à garantir la continuité du service en fusionnant les principes des deux protocoles. Cette approche permet d'assurer à la fois la redondance et l'équilibrage de charge avec un délai minimal.

Suite à des tests de vérification et de validation appliqués aux solutions mises en place, nous avons constaté que notre dernière solution était la plus optimisée. Elle a permis de remédier à plusieurs problèmes en assurant la continuité, la redondance et l'équilibrage de charge du réseau.

En résumé, notre travail a abouti à une solution efficace et adaptée aux besoins de l'entreprise Cevital. La mise en place d'un réseau hautement disponible contribué à garantir un fonctionnement fluide et continu du service, tout en offrant une capacité de production accrue.

Bibliographie

[1] *Tout sur la sécurité informatique*. LAVOISIER, France, dunod edition, 2016.

[2] Quality of service gateway load balancing protocol message digest algorithm 5 authentication untuk peningkatan kualitas jaringan. *TEKNIK INFORMATIKA STMIK ANTAR BANGSA*, 1, 2019.

[3] Adressage ipv4-ipv6. `https://www.avg.com/fr/signal/ipv4-vs-ipv6`, (Consulté le 02/03/2023).

[4] Ciscoo. `http://www.cevital.com/`, (Consulté le 06/04/2023).

[5] `https://yt3.googleusercontent.com/ytc/AL5GRJW-6llnUcsMgXDbxi9LTuKODFJ26ifzaeDDKIO9=s900-c-k-c0x00ffffff-no-rj`, (Consulté le 09/03/2023).

[6] `http://docplayer.fr/69810076lesvlaniipourquoicreerunr\'eseauvirtuelextraitservlancoursdoc.html`, (Consulté le 15/01/2023).

[7] Cevital. `https://www.cevital.com/lhistoire-du-groupe/`, (Consulté le 15/03/2023).

[8] Cevital1. `https://www.google.com/maps/place/Cevital+Agroindustrie/`, (Consulté le 19/03/2023).

[9] Cisco. `https://www.cisco.com/c/frbe/products/routers/`, (Consulté le 24/03/2023).

[10] Openclassroom. `http://openclassrooms.com/`, (Consulté le 26/02/2023).

[11] Adressage ipv4. `http://www.inetdoc.net/articles/adressage.ipv4/adressage.ipv4.class.html/`, (Consulté le 29/02/2023).

[12] Ciscoo. `https://datacenter.legrand.com/fr`, (Consulté le 29/03/2023).

[13] AGRANA. *Configuration et Simulation des VLANs Cas d'étude AGRANA*. Mémoire master, Université de Havre, june 2019/2020.

[14] A.K.SINGH and A.KOTHARI. Glbp in medium size enterprise. *Shivdan Singh Institute of Technology and Management Aligarh (India)*, 2011.

[15] A.K.SINGH and A.KOTHARI. Hsrp (hot stand by routing protocol) reliability issues over the internet service provider's networ, oriental journal of computer science and technology. *Shivdan Singh Institute of Technology and Management Aligarh (India)*, 2011.

[16] A.Perez. *Architecture des réseaux de télécommunications*. LAVOISIER, France, 2nd edition, 2002.

[17] A.Amrah Baba and M.Tabassum. A comparative study of igp and egp routing protocols, performance evaluation along load balancing and redundancy across different as, proceedings of the international multi conference of engineers and computer scientists 2016. *TEKNIK INFORMATIKA STMIK ANTAR BANGSA*, II, March 16 - 18.

[18] C.Duvallet. *Architectures et protocoles des réseaux*. Licence professionnelle informatique, Université de Havre, 2007/2008.

[19] D.DROMARD and D.SEREST. *Architecture des réseaux*. Pearson, France, 2nd edition, 2009.

[20] J. DORDOIGNE. *Réseaux informatique,Notions fondamentales,protocoles architectures réseaux sans fil virtualisation sécurité IPv6*. DORDOIGNE, Paris, 6th edition, 2015.

[21] E.Akli and A.Boudjelil. *Proposition d'une configuration sécurisée d'un réseau local avec les VLAN,cas d'étude :office de promotion et de gestion Immobilière de Bejaia(OPGI)*. Mémoire master(informatique), Université de Bejaia, july 2018.

[22] R. Roger Erick. *Déploiement de la technologie de VLAN et du protocole RSTP dans un réseau d'entreprise*. Diplôme licence (télécommunication), Université D'Antananarivo Ecole Supérieure Polytechnique, may 2012.

[23] H. Far and S. Ghilani. *Un simulateur graphique de protocole de liaison de données dédié à l'apprentissage et l'enseignement*. Mémoire master, Université de Ouargla, Juin 2013.

[24] Kampar, Perak, and Malaysia. Glbp in medium size enterprise. *International Journal of Trend in Scientific Research)*, 3 :728, 2019.

[25] L.ALOUACHE and H.KEMACHA. *La haute disponibilité des réseaux HSRP, cas d'étude CEVITAL Agro-industrie*. Mémoire master, Université de Bejaia, 2022.

[26] S. Lohier and D. Present. *Réseau et Transmissions protocoles infrastructures et services*. D.Present, USA, 7th edition, 2020.

[27] J.N. Méreur and Hardy Guy Malleurs. *Réseaux Internet Téléphonie Multimédia*. Jean-Noele, France, 3rd edition, 2002.

[28] M.Ferrie. A comparative study of hsrp and glbp first hop redundancy protocols. *Submitted in partial fulfilment of the requirements of Edinburgh Napier University for the Degree of Computer Systems and Networks, School of Computing*, 2016.

[29] M.Ilmiah. Performansi jaringan tcp/ip menggunakan metode vrrp, hsrp, dan glbp. *Teknologi Elektro*, 8 :77–81, 2019.

[30] M.Mansour. *Performance Evaluation of First Hop Redundancy Protocols, Libya,The 11Th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2020)*. PhD thesis in Computer Science, University of Tripoli, Madeira, Portugal, November 2020.

[31] N.Aiboud and S.Ahmed Zaid. *Proposition d'une solution de filtrage de sites web indésirables en vue de l'optimisation d'un réseau informatique*. Mémoire master(réseaux et télécommunications), Université de Tizi-Ouzou, july 2018.

[32] Noida and U.Pradesh. Review of first hop redundancy protocol and their functionalities,. *International Journal of Engineering Trends and Technology (IJETT)*, 4, 2013.

[33] WENDELL ODOM. Ccna 200-301 official cert guide, volume 2. *EMERITUS*, 2 :CC NA 200–301, 2019.

[34] J. PILLOU. *Tous sur Les réseaux et Internet*. PILLOU, Paris, dunod edition, 2006.

[35] S.Boubekri and R.Mebarki. *La disponibilité des réseaux compus,Cas d'étude SONATRACH*. Mémoire master(administration et sécurité des réseaux), Université de Bejaia, may 2016.

[36] T.Andrew. *Réseaux Edition*. Dunod, France, 3rd edition, 2012.

[37] Vlan. `http://www.researchgate.net/`, (Consulté le 16/02/2023).

[38] Vlan. `http://projet.eu.org/pedago/sin/ISN/8-VLAN.pdf`, (Consulté le 19/01/2023).

[39] UR Z.RAHMAN and R.KHAN. Performance evaluation of first hop redundancyprotocole (hsrp,vrrp,glbp). March 2017.

RÉSUMÉ

Ce mémoire aborde plusieurs aspects du réseau informatique et de la haute disponibilité, en se concentrant sur les protocoles HSRP et GLBP. Dans la section introductive, les concepts de base du réseau informatique sont présentés, mettant en évidence son importance et ses composants. Ensuite, l'entreprise Cevital est présentée, contextualisant ainsi les besoins spécifiques de son réseau informatique. La définition de la haute disponibilité est ensuite abordée, accompagnée d'une explication détaillée des protocoles HSRP et GLBP en tant que solutions pour assurer la redondance et l'équilibrage de charge. Dans les sections suivantes, l'implémentation pratique de ces protocoles est détaillée, tant sur le logiciel Cisco Packet Tracer que sur GNS3, permettant d'évaluer leur fonctionnement. Enfin, une solution innovante est proposée, qui fusionne les principes des protocoles HSRP et GLBP afin de garantir à la fois la redondance et l'équilibrage de charge. Cette approche vise à résoudre les problèmes spécifiques rencontrés par l'entreprise Cevital, assurant ainsi la continuité et l'efficacité de son réseau. Dans l'ensemble, ce mémoire offre une exploration complète des principes fondamentaux du réseau informatique, une analyse approfondie des protocoles HSRP et GLBP, et une solution pratique pour répondre aux besoins de haute disponibilité de l'entreprise.

Mots clés : disponibilité ; rśeau ; HSRP ; GLBP ; VLANs ; CEVITAL.

ABSTRACT

This thesis covers several aspects of computer networking and high availability, focusing on the HSRP and GLBP protocols. focusing on the HSRP and GLBP protocols. In the introductory section, the basic concepts of computer networking are presented, highlighting its importance and components. The Cevital company is then presented, contextualising the specific needs of its IT network. its IT network. The definition of high availability is then discussed, together with a detailed explanation of the HSRP and GLBP protocols as solutions for ensuring redundancy and load balancing. In the following sections, the practical implementation of these protocols is detailed, both on Cisco Packet Tracer software and GNS3, allowing their operation to be evaluated. Finally, an innovative solution is proposed, an innovative solution is proposed, which merges the principles of the HSRP and GLBP protocols in order to guarantee both redundancy and load balancing. This approach aims to solve the specific problems encountered by Cevital, thus ensuring the continuity and efficiency of its network. Overall, this thesis provides a exploration of computer network fundamentals, an in-depth analysis of the HSRP and GLBP of the HSRP and GLBP protocols, and a practical solution to meet the company's high availability needs

Key words : availability ; network ; HSRP ; GLBP ; VLANs ; CEVITAL.