République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieure et de la Recherche Scientifique

Université Abderrahmane Mira

Faculté de la Technologie

Département d'Automatique, Télécommunication et d'Electronique

Projet de Fin d'Etudes

Pour l'obtention du diplôme de Master

Filière : Télécommunications.

Spécialité : réseaux et système de télécommunications.

Thème

Mise en place d'un réseau local et l'interconnexion avec les sites distants (CEVITAL)

Préparé par :

Melle ALLAOUA Manel

Melle SAOU Melissa

Dirigé par :

Mr A.DIBOUNE

Mr D.BEKNADJ

Mr M.SLIMANI

Examiné par :

Mr ALLICHE Président

Mme GHARBI Examinatrice

Année universitaire : 2021/202022

Dédicaces

Avec un énorme plaisir un cœur ouvert et une immense joie,

Que je dédie ce modeste travail

À mes très chers et respectueux parents, pour leurs patiences et leurs

Encouragement et leurs sacrifices tout au long de mon parcours

À mes deux petits frères Fawzi et Islam

A ma petite sœur Yasmine

À ma précieuse famille, À mon binôme Melissa ainsi que sa famille

À mes amis et camarades

A tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail.

MANEL

Dédicaces

Je dédie ce mémoire

À mes très chers parents, je ne saurai vous remercier de tout le soutien, l'affection, la bienveillance que vous m'avez offert durant mon parcours. Je n'en serai certainement pas là sans vous, vous êtes ma source d'inspiration pour tout ce que j'entreprends.

À mes précieuses sœurs Tin-hinan et Sabine ainsi qu'à mon précieux frère Massinissa pour leurs soutiens et encouragements indéfectibles.

A mes merveilleuses amies que j'ai toujours trouvées à mes côtés pour m'écouter, m'encourager et m'épauler.

À ma binôme Manel, pour m'avoir supporté moi et mes crises d'angoisses.

À tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail.

Melissa

Remerciement

Nous tenons à présenter nos sincères gratitudes à nos très chers parents et nos familles pour leurs soutient et leurs encouragement car sans eus on n'aurait pas pu arriver jusqu'à là.

Nous tenons à remrcier profondément nos encadrants de l'université Monsieur DIBOUNE Abdelhani et Monsieur BEKNADJ Dalil pour leur confiance, leurs encouragements et leurs conseils afin de réaliser notre travail.

Nos sincères remerciement aux personnels de l'entreprise CEVITAL Bejaia, spécialement Monsieur SLIMANI Mennad notre encadrant de stage pour sa patience, son sérieux et sa grande disponibilité tout au long de notre stage au sein de l'entreprise.

A nos professeurs de l'université de Bejaia pour les solides notions théoriques qu'ils nous ont enseignée et sur lesquelles nous nous sommes appuyées pour élaborer notre travail.

Pour finir nos remercîments à tous ceux qui nous ont aidées de près ou de loin à élaborer notre mémoire de fin d'étude.

Table des matières

Sommaire

Sommaire

Sommaire

Sommaire

Sommaire

Liste des figures

Liste des figures

Liste des figures

Liste des listings

Liste des listings

Liste des listings

Liste des tableaux

Liste des tableaux

Liste des abréviations

Liste des abréviations

AVF : Active virtual Forwarder.

AVG: Active virtual Gateway.

DHCP : Dynamique Host Configuration Protocol.

DMZ: Demilitaried Zone.

DSI : Direction du Système Informatique.

EIGRP: Enhanced Interior Gateway Routing Protocol.

FDDI : Fiber Distributed Data Interface.

HSRP: Hot Standby Router Protocol.

IEEE: Institute of Electric and Electronique Engineer.

IP: Internet Protocol.

LAN: Local Area Network.

MAN: Metropolitan Area Network.

OSI: Open System Interconnexion.

OSPF: Open Shortest Path First.

PVST : Per-VLAN spanning tree.

RIP: Routing Information Protocol.

Rj45: registered jack 45.

STP: Spanning Tree Protocol.

TCP : Transmission Control Protocol.

VLAN: Virtual Local Area Network.

VRRP: Virtual Router Redundancy Protocol.

VTP: Virtual trunking Protocol.

WAN: Wide Area Network.

WIFI : Wireless fidelity.

WLAN: Wireless local area network.

Introduction générale

Introduction générale

Après le début d'apparition des ordinateurs, la constatation du besoin des consommateurs à échanger des données se fit rapidement ressentir. Pour remédier à cela l'idée de relier entre eux différents ordinateurs se plaça comme la solution adaptée. On assista alors à la naissance du réseau informatique sous sa première image.

La mise en place d'un réseau informatique dans une entreprise est une notion primordiale, elle répond aux besoins fondamentaux de l'entreprise et de ses employés à savoir de partage de ressources et de données, tout en assurant une bonne gestion du réseau, une souplesse d'utilisation et un certain degré de sécurité.

L'entreprise CEVITAL de Bejaia est une organisation à grande échelle, qui joue un rôle primordial dans l'économie du pays. Vu l'importance des informations qui sont souvent véhiculées dans les réseaux. CEVITAL s'est lancé dans la modernisation en renouvelant son réseau de télécommunication. Malgré ses avantages, ce processus de modernisation fait face à de nombreuses difficultés liées à une mauvaise distribution d'architecture et de partage de ressources. Cela est dû aux divers problèmes liés aux collisions et congestions dans le trafic de données. Notre stage au sein l'entreprise nous a permis de découvrir le réseau et de mieux comprendre son fonctionnement. L'objectif de notre projet est de proposer une nouvelle architecture sécurisée en cas de panne du réseau, et mettre en place des solutions fiables en utilisant des liens virtuels, des connexions aux sites distants pour assurer un meilleur fonctionnement et de partage de ressources.

Afin de bien mettre en lumière la réalisation de notre projet, nous avons agencé notre mémoire en 3 chapitres, à savoir :

- Dans le premier nous allons mettre en revue quelques notions de base des réseaux informatiques, pour des notions de base visant une meilleure compréhension du reste du mémoire.
- Dans le deuxième chapitre, le but est de présenter l'entreprise Cevital Bejaia, son historique et les nombreux départements qui font partie de son infrastructure puis nous allons parler de la problématique du réseau Cevital, problématique qui sera le centre de notre projet. La deuxième partie de ce chapitre sera consacré à la définition de nombreux protocoles exploitables afin d'assurer la haute disponibilité.
- Le troisième chapitre devisé en 2 parties, nous allons reconfigurer le réseau déjà existant de Cevital pour mettre en lumière ses avantages et ses inconvenants

puis dans la deuxième partie, nous avons proposé une nouvelle configuration afin d'améliorer et de corriger les faiblesses du réseau existant avec des nouveaux protocoles tels que le STP, HSRP et l'OSPF.

Pour finir notre mémoire se termine avec une conclusion générale, qui englobe les connaissances obtenues lors de la réalisation de notre projet de fin d'étude.

CHAPITRE 1

Généralités sur les réseaux informatiques.

1.1.Introduction

Dans ce premier chapitre, nous allons mettre en revue quelques notions de base des réseaux informatiques, que nous jugeons nécessaires de rappeler pour une meilleure compréhension de notre projet. Pour ce faire nous allons commencer par une définition des réseaux informatiques et de leurs objectifs, ensuite nous passerons à la classification et aux caractéristiques des réseaux, et nous terminerons en parlant des modèles de références.

1.2.Un réseau informatique

Le terme réseau informatique désigne un ensemble d'équipements et de logiciels qui échangent des informations grâce à des interconnexions qui résultent des liaisons physiques entre eux, échangeant alors ces informations sous forme de données numériques.

Il existe deux types de réseaux :

- Le réseau filaire : ce réseau se distingue par l'utilisation d'une connexion avec fil, autrement dit il utilise des câbles pour relier des ordinateurs et des périphériques.
- Le réseau sans fil : ce réseau se distingue par la non utilisation des câbles, il est utilisé par les particuliers, par les entreprises et dans les réseaux de télécommunication dans le but de limiter l'utilisation des câbles entre diverses localisations [1].

1.3.Objectifs d'un réseau informatique

Le réseau informatique est indispensable au partage des ressources et des données, à la gestion ainsi qu'à la sécurité des informations qui circulent, il peut servir plusieurs buts distincts :

- Le partage de ressources : il permet des rendre facilement accessible des informations, des données informatiques ou des périphériques via un réseau local indépendamment de leur localisation.
- Fiabilité : permet le bon fonctionnement même en cas de problèmes matériels.
- Communication entre personnes (courriers électroniques, discussion en direct, etc.).
- La communication entre processus (entre des ordinateurs industriels par exemple).
- La garantie de l'unicité et de l'universalité de l'accès à l'information (bases de données en réseau) [1].

1.4.Classification des réseaux informatiques

On distingue différents types de réseaux selon leur taille, le nombre de machines, leur vitesse de transfert des données ainsi que leur étendue. On fait généralement trois catégories de réseaux :

- Les réseaux locaux (local area network).
- Les réseaux métropolitains (metropolitan area network).
- Les réseaux étendus (Wide area network).

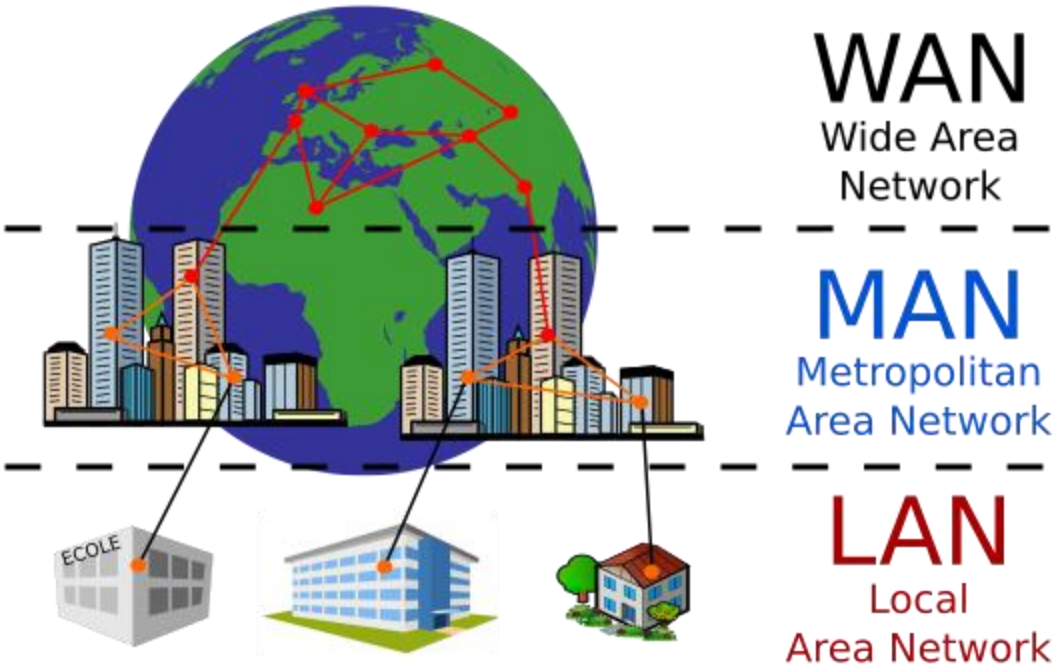

Figure 1.1 : *classification des réseaux [F1].*

A. Les réseaux locaux (LAN)

LAN signifie Local Area Network (en français Réseau Local). Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique. Ce sont des réseaux qui permettent l'échange de données informatiques et le partage de ressources (données, disques durs, périphériques divers, etc.).

La vitesse de transfert de données d'un réseau local peut s'étaler entre 10 Mbps (pour un réseau Ethernet par exemple) et 1 Gbps (en FDDI ou Gigabit Ethernet par exemple) [2].

Figure 1.2 : Réseau local (LAN) [F1].

B. Les réseaux métropolitains (MAN)

Les MAN (Métropolitain Area Network) représentent une interconnexion de plusieurs réseaux locaux répartis sur différents sites dans une zone urbaine dont l'étendue géographique n'excède pas 200 km. Autrement dit, ils couvrent une métropole (ville) à des débits supérieurs à 1000 Mb/s [2].

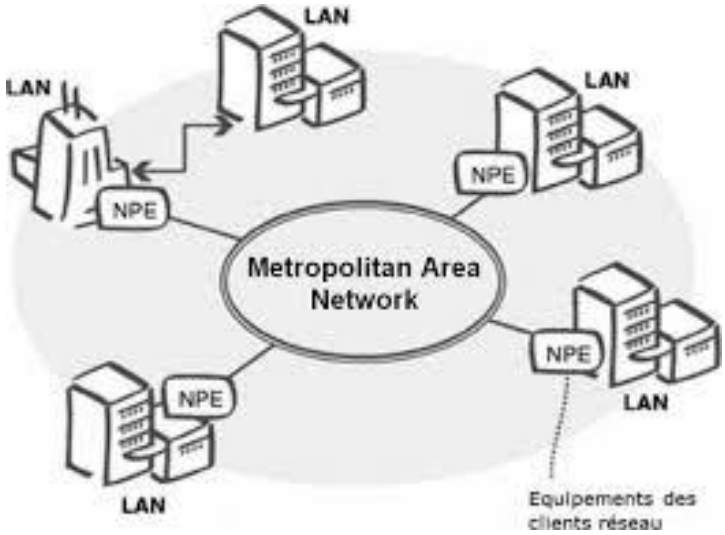

Figure 1.3 : Réseau métropolitain (MAN) [F1].

C. Les réseaux étendus (WAN)

Les WAN (Wide Area Network ou réseau étendu) représentent des réseaux qui assurent la transmission des données entre les villes et les pays à l'échelle de la planète. Les débits

disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles. Le plus connu des WAN est Internet [3].

Figure 1.4 : Réseau étendu (WAN) [F1].

1.5.Les topologies des réseaux informatiques

Il existe deux types de topologies informatiques. La première est la topologie physique, elle décrit la manière dont les ordinateurs sont reliés et interconnectés entre eux. La seconde s'agit de la topologie logique, qui décrit la manière dont les équipements communiquent [3].

1.5.1. Les topologies physiques

A. Topologie en bus

La topologie en bus repose sur un câblage, sur lequel viennent se connecter des nœuds (postes de travail, équipements d'interconnexion, périphériques). Elle est la plus simple des topologies. Lorsqu' une machine émet des données, la trame circule sur toute la longueur du bus jusqu'à ce qu'à son arrivée au destinataire. Une seule station émet en même temps. Pour empêcher l'apparition des signaux parasites et de l'écho du signal transmis, chaque extrémité est terminée par bouchon, qui est une résistance de 50 à 120 Ohom. [4].

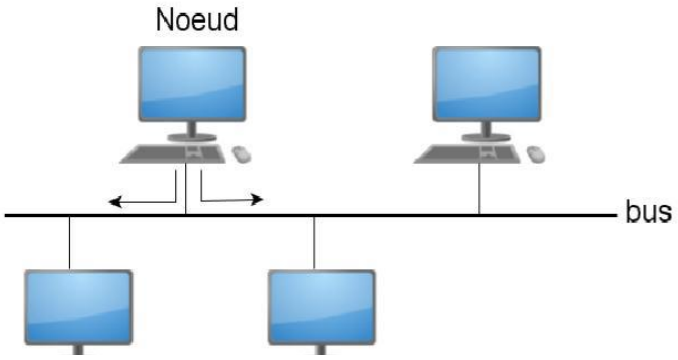

Figure 1.5 : Topologie en Bus [F1].

a) Les avantages :

- Facile à mettre en place ;
- Lorsqu'un câble est interrompu, le reste du réseau n'est pas perturbé ;
- L'ajout d'un terminal n'interrompt pas le fonctionnement ;
- Economique en câble et en prix.

b) Les inconvénients :

- Faible sécurité ;
- Réduction des préférences en cas de charges importantes ;
- L'imprévisibilité du temps d'attente ;
- Un seul ordinateur peut envoyer un signal à la fois ;
- Une panne de support induit à une défaillance de réseau.

B. Topologie en étoile

La topologie en étoile est la topologie la plus utilisée dans les réseaux locaux. Elle repose sur des matériels actifs. Un matériel actif remet en forme les signaux et les régénère. Les câbles sont raccordés à un point central (switch).

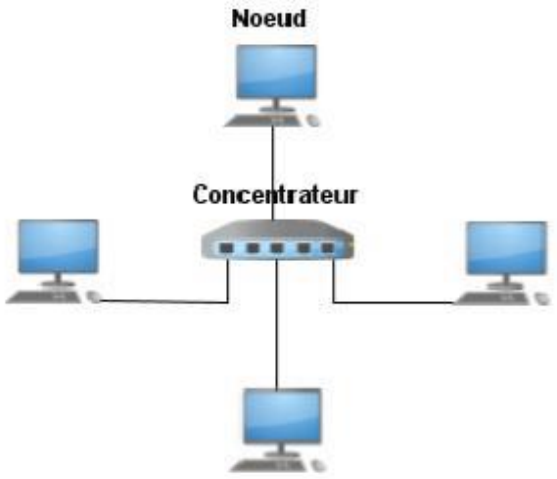

Figure 1.6 : Topologie en étoile [F3].

a) Les avantages :

- Possibilité d'ajout de postes facilement ;
- Lorsqu'une connexion est débranchée, le reste du réseau n'est pas perturbé ;
- Les pannes sont facilement localisables ;
- Le terminal est responsable des performances et non le nœud central.

b) Les inconvénients :

- La topologie repose totalement sur le nœud central ;
- Pour les réseaux étendus le prix est très élevé.
- Nécessite plus de câbles qu'un bus linéaire.

C.Topologie en anneau

La topologie en anneau connue comme une des topologies les plus anciennes, particulièrement utilisé par les réseaux Token ring qui utilise la technique d'accès par jeton. Cette topologie repose sur une boucle fermée, en anneau (ring), constituée de liaisons point à point entre périphériques. Les trames transitent par chaque nœud qui se comporte comme un répéteur (élément actif), la station qui a le jeton émet des données qui feront le tour de l'anneau, la station qui les a envoyées les élimine et passe le jeton à son voisin et ainsi de suite.

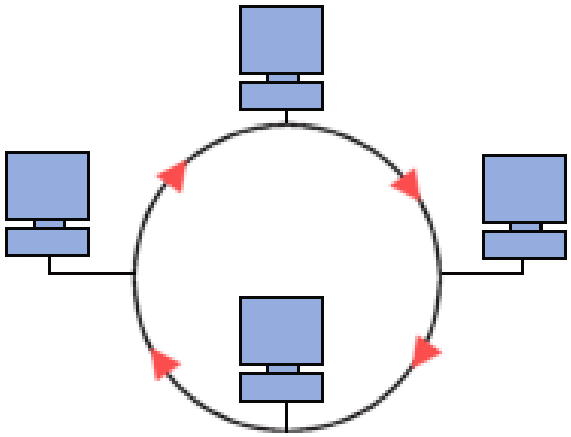

Figure 1.7 : Topologie en anneau [F1].

a) Les avantages :

- Facilement installable ;
- Meilleur fonctionnement que la topologie en bus ;
- La forte charge n'influe pas sur ses performances ;
- Evite la gestion des collisions.

b) Les inconvénients :

- L'ajout d'un nœud supplémentaire influe sur la performance ;
- Le trafic du réseau est paralysé lorsqu'une unité active est en panne ou retirée ;
- Les performances sont plus lentes que les de la topologie en bus ;
- cout élevé.

D.Topologie maillée

Un réseau maillé est une topologie de réseau qui définit un réseau (filaire ou non) dans lequel tous les hôtes sont connectés en pair-à-pair (peer-to-peer) sans hiérarchie centrale, formant une structure de type réseau. Par conséquent, chaque nœud doit recevoir, envoyer et relayer des données. Cela évite les points sensibles qui isoleraient des parties du réseau en cas de panne. Si un hôte tombe en panne, ses voisins emprunteront une autre route.

Un réseau maillé utilise plusieurs chemins de transmission entre différents nœuds. Cette méthode garantit la transmission des données en cas de défaillance du nœud.

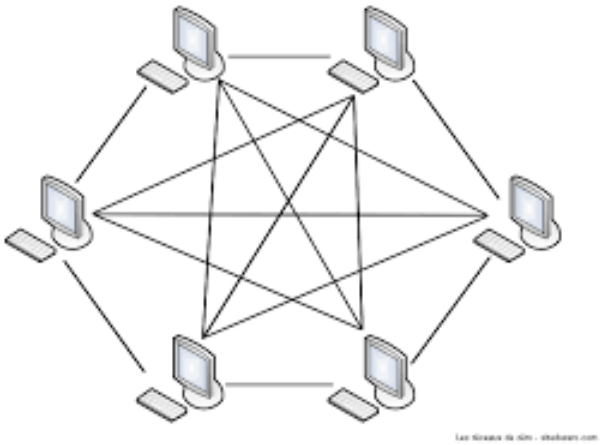

Figure 1.8 : Topologie maillée [F2].

a) Les avantages :

- La topologie est l'une des topologies les plus robustes ;
- Une erreur peut être facilement détectable ;
- Chaque connexion a la capacité porter sa propre charge de données ;
- Elle garantit la sécurité et la confidentialité.

b) Les inconvénients :

- Le câblage doit être en grande quantité ;
- Lors d'une topologie maillée entièrement connectés le coût du câblage est extrêmement élevé ;
- L'agencement et la configuration deviennent plus difficiles si la connectivité devient conséquente.

E. Topologie hybride

Une topologie hybride est une fusion de plusieurs (deux ou plusieurs) topologies de réseau différentes. Par exemple, si un réseau qui utilise une topologie en anneau est joint à un autre

réseau qui utilise une topologie en étoile. Une nouvelle topologie formée d'une combinaison de deux topologies de réseau est appelée une topologie hybride. La fusion de deux réseaux n'est pas une topologie hybride si les réseaux à fusionner ont le même type de topologie. Par exemple, un réseau qui utilise une topologie en bus est combiné avec un autre réseau qui utilise une topologie en bus, de sorte que la fusion des deux réseaux reste la topologie en bus au lieu de la topologie hybride. La topologie hybride portera les caractéristiques de la topologie d'origine qui l'a construite.

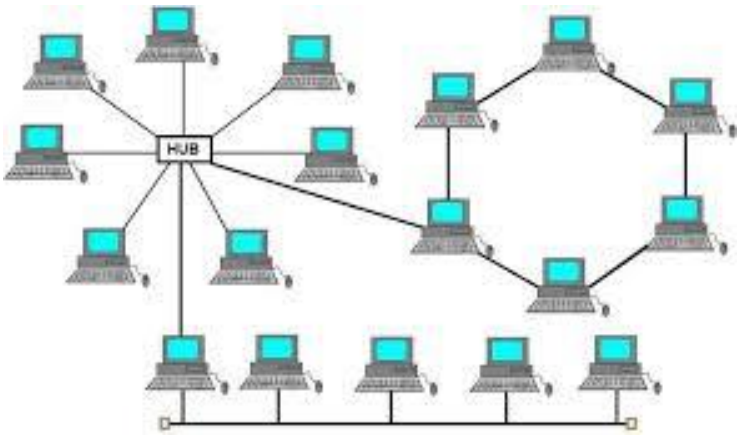

Figure 1.9 : Topologie hybride [F2].

a) Les avantages :

- Elle peut combiner deux ou plusieurs topologies de réseau différentes ;
- La vitesse du réseau est cohérente car elle combine les forces et les faiblesses de chaque topologie de réseau ;
- Si l'une des connexions réseau est déconnectée, les autres connexions réseau ne seront pas déconnectées à leur tour.

b) Les inconvénients :

- Les coûts de maintenance du réseau sont chers ;
- L'installation et la configuration du réseau sont compliquées.

1.5.2. Les topologies logiques

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

A. Ethernet

Ethernet est un protocole de réseau informatique, Ethernet est basé sur le principe selon lequel les membres du réseau (pairs) envoient des messages sur un système radio, captif à l'intérieur d'un fil ou d'un canal commun, parfois appelés éther. Chaque pair est identifié par une clé unique au monde appelée adresse MAC afin que chaque station du réseau Ethernet ait une adresse unique. La propagation des trames est bidirectionnelle, les débits prévus par la norme sont 1Mbps et maintenant 100 Mbps. [W1]

Avant de pouvoir emmètre, une station doit d'abord vérifier qu'aucune autre station n'est en train d'emmètre au même moment, car si la trame est en pleine circulation, alors l'émetteur continu la phase de détection jusqu'à ce que le média soit libre. Si deux stations décident démettre en même temps elles créeront ce qu'on appelle une collision, pour rétablir cette collision, la norme a mis en place une technique de détection de collision (Collision Detect). Son fonctionnement consiste dans un premier temps à détecter la collision et les machines qui y sont responsables. Puis les stations arrêtent démettre pendant un certain temps avant de se remettre en mode d'émission. [W2]

B. Token ring

Un réseau Token Ring est un réseau local (LAN, réseau local) où tous les ordinateurs sont connectés dans une topologie en anneau ou en étoile et transmettent un ou plusieurs jetons logiques (Token) d'hôte à hôte. Chaque station est physiquement connectée aux stations précédentes et prochaines. Le jeton passe d'une station active à une autre suivant l'unique sens de transmission prédéfini. Chaque station reçoit la trame de la station précédente et l'envoie vers la prochaine station [w2].

C. FDDI

FDDI (Fiber Distributed Data Interface) fonctionne selon une topologie physique en anneau. Les machines peuvent être interconnectées soit en étoile à la sortie d'un concentrateur, soit directement sur l'anneau. Elle permet d'interconnecter plusieurs LAN à une vitesse de 100 Mbit/s sur de la fibre optique, ce qui lui permet d'atteindre une distance maximale de 200 km.

Les données transitent généralement par l'anneau principal. En cas de panne, le trafic est automatiquement basculé sur l'anneau secondaire (appelé secours). Certains fabricants de matériel proposent des variantes qui utilisent les deux anneaux. Ce processus double la bande

passante. En cas d'échec de connexion entre deux stations adjacentes (comme une rupture de câble), les stations en aval et en amont rebouclent l'anneau primaire vers l'anneau secondaire afin de configurer automatiquement le nouvel anneau. Si plusieurs interruptions se produisent en même temps, l'anneau sera divisé en deux sous-réseaux. [W3]

1.6. Les architectures des réseaux informatiques

Il existe différentes architectures de réseau, qui ont pour rôle l'agencement de matériels de transmission, de logiciels, d'infrastructures permettant la transmission des informations.

A. Architecture poste à poste

Les réseaux « postes à postes » sont également appelés des réseaux « Peer to Peer » ont comme atout de pouvoir fonctionner sans administrateur central. Dans un réseau peer to peer chaque poste est à la fois client et serveur autrement dit, son principe consiste à relier les postes entre eux dans une topologie physique.

Chaque utilisateur décide lui-même des partages sur son disque dur et des permissions qu'il octroie aux autres utilisateurs. Mais une ressource partagée l'est pour tous les autres utilisateurs, c'est le concept de « partage arbitraire ». Une ressource partagée sur un ordinateur apparaît sur les autres ordinateurs qui s'y sont connectés, ce qui est extrêmement bénéficiaire pour le travail en groupe [5].

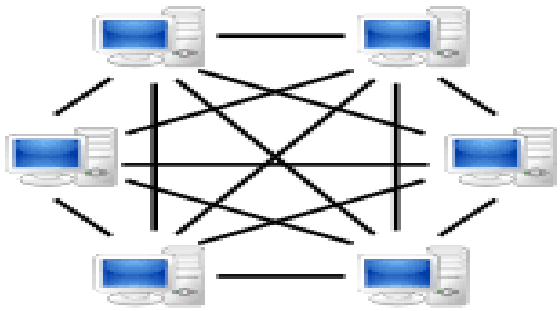

Figure 1.10 : Architecture poste à poste [F2].

a) Les avantages :

- Méthode pratique et non couteuse ;
- La ressource partagée est un atout pour les groupes de travail ;

- Chaque utilisateur peut décider lui-même de partager ses ressources avec les autres postes.

b) Les inconvénients :

- La sécurité est extrêmement limitée ;
- Le fonctionnement du réseau est sous la responsabilité de chaque utilisateur ;
- L'accessibilité des ressources est dépendants des postes ;
- le système devient ingérable à l'augmentation du nombre de postes.

B. Architecture client/serveur

Cette architecture consiste en un processus de coopération entre un serveur et un client. Un réseau client/serveur contient généralement plus de 10 postes de travail. La plupart des stations sont des "postes clients", autrement dit les ordinateurs utilisés par les utilisateurs, les autres stations sont dédiées à une ou plusieurs tâches particulières et sont dites serveurs. Des machines clientes contactent un serveur, qui leur fournit des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion, etc. [6].

Etant donné que le serveur est centralisé, il peut gérer des ressources communes à tous les utilisateurs.

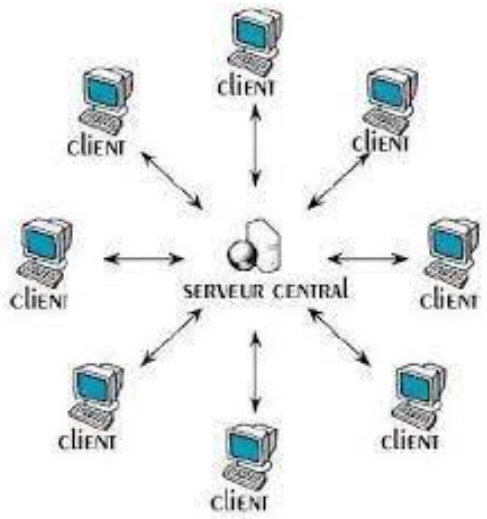

Figure 1.11 : Architecture client/serveur [F2].

a) Les avantages :

- Un contrôle de sécurité simplifié ;

- Les technologies supportant l'architecture client/serveur sont plus matures que les autres ;
- Facilité d'enlever clients ou même des serveurs.

b) Les inconvénients :

- Ne supporte pas le trop de charge ;
- L'architecture est dépendante du serveur, sans lui rien ne fonctionne ;
- Le coût de la mise en place et de la maintenance est élevé ;
- Les clients sont en incapacité de communiquer entre eux.

1.7. Caractéristiques des réseaux

Les principales caractéristiques d'un réseau sont sa topologie (physique et logique) et le support utilisé pour la transmission, le matériel d'interconnexion ainsi que les méthodes de transmission [7].

A. Support de transmission

Dans les réseaux locaux, nous trouvons plusieurs supports de transmission, dans lesquels nous citons :

a) Le câble coaxial

Un câble coaxial est constitué d'une âme conductrice cylindrique coaxiale et de tresses, séparées par un isolant qui limite les interférences causées par les bruits extérieurs. Nous pouvons ajouter un blindage dans le cas où il y'a beaucoup de bruit. Même s'il perd du terrain, notamment par rapport à la fibre optique, le médium est encore largement utilisé.

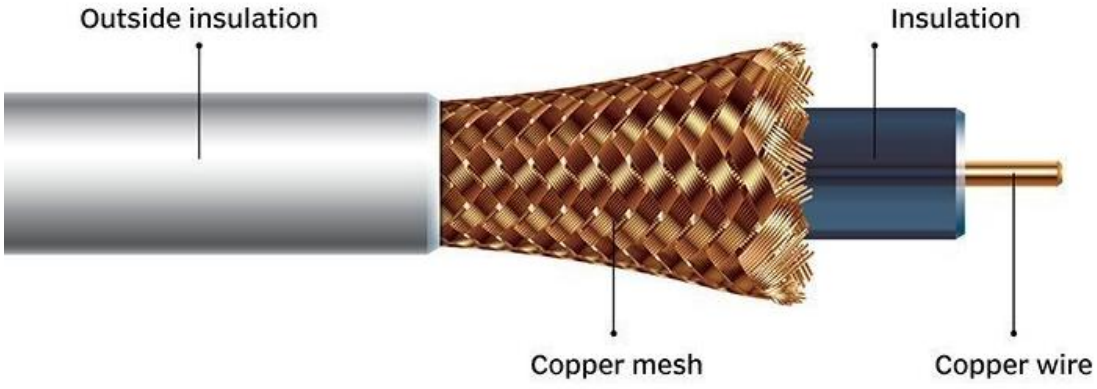

Figure 1.12 : câble coaxial [F3].

b) La paire torsadée

Une paire torsadée est un support de transmission qui se compose de deux fils conducteurs enroulés en hélice l'un autour de l'autre, ce type de ligne convient à la transmission analogique et numérique. Cependant, du fait que les câbles ne dépassent pas 0,2 à 1 mm de diamètre, l'affaiblissement des signaux véhiculés est très important, ce qui limite leur usage à des communications sur de courtes distances jusqu'à 100 m comme le câble coaxial. Mais elle est meilleure car il y'a moins de perturbation. Les paires torsadées peuvent être blindées, une gaine métallique enveloppant complètement les paires métalliques, ou non blindées. Elles peuvent être également «écrantées». Dans ce cas, un ruban métallique entoure les fils.

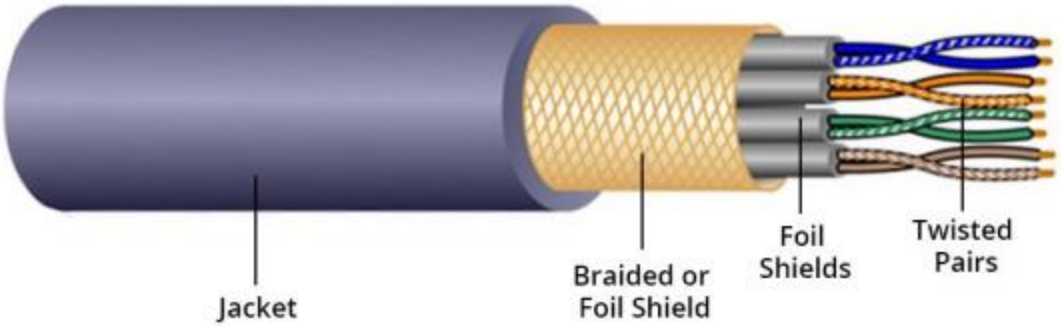

Figure 1.13 : Câble à paire torsadée [F3].

c) La fibre optique

La fibre optique est un moyen de transmission de donné le plus rapide et plus efficace, dont l'âme est très fine qui est en verre ou en plastique, elle a la propriété de conduire des lumières. La modulation du faisceau lumineux émis par le laser permet de transmettre, via la fibre optique un signal haute fréquence.

Pour une connexion optique nous devons avoir un émetteur et un récepteur. Pour la réaliser, différents types de composants sont envisageables. Les informations numériques sont modulées par un émetteur de lumière. Ce dernier peut être une diode électroluminescente (DEL) ou un laser.

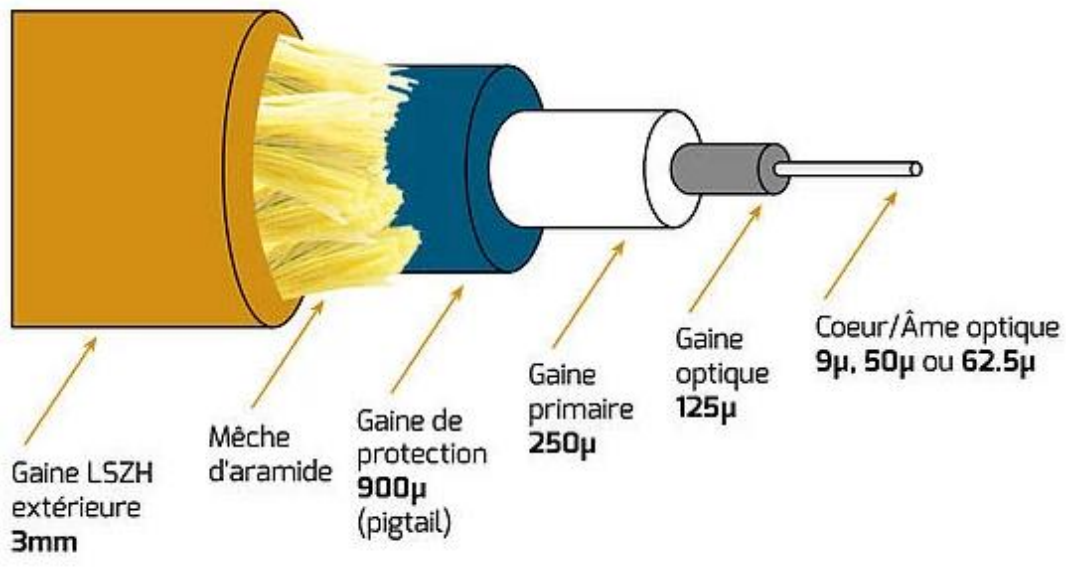

Figure1.14 : Fibre optique [F3].

d) Les liaisons infrarouges et les ondes hertziennes

Les réseaux locaux sans fil ou WLAN (la norme 802.11) est un réseau qui couvre un réseau local d'entreprise, soit une portée d'environs une centaine de mètre dont le débit de la zone couverte varie entre 1 et 2 Mbits. Il permet de relier entre les terminaux présents dans la zone couverte. Le standard prévoit deux supports de transmission.

- Les liaisons infrarouges sont utilisés pour l'interconnexion dans les courtes distances et oblige à mettre une borne dans chaque bureau car le rayonnement est bloqué par les murs.
- Les ondes hertzienne ont une plus grande souplesse, peuvent traverser les murs. Le standard IEEE 802.11 fonctionne dans les bandes des 2,4 GHz. [12]

B. Mode de transmissions

Nous distinguons trois modes d'exploitation d'une liaison qui sont :

a) La liaison simplex

Cette liaison est un mode de communication unidirectionnel, dans lequel chaque appareil est soit toujours émetteur ou toujours récepteur.

Ce mode de liaison est utilisé quand il n'est pas nécessaire pour l'émetteur de recevoir une réponse de la part du récepteur. Un circuit électronique comme un capteur qui envoie régulièrement et de manière autonome des données pourra utiliser une liaison simplex.

C'est un mode de communication utilisé pour la diffusion, c'est à dire lorsqu'un même émetteur transmet simultanément à de nombreux récepteurs. Ainsi, la liaison entre un émetteur de télévision et les postes récepteurs.

Si nous prenons l'exemple d'un capteur et d'un système d'enregistrement, la communication simplex permettrait au capteur de transmettre ses données de manière autonome, sans être en mesure de recevoir des commandes ou des accusés de réception de la part de l'enregistreur.

b) La liaison half-duplex

Dans le cas de la communication semi-duplex, deux systèmes interconnectés sont capables d'envoyer et de recevoir à tour de rôle.

Cette communication est avantageuse. En effet, elle réduit de moitié le nombre de canaux utilisés. Par contre, elle impose que les deux systèmes communicants déterminent qui a le droit de parler en premier. Dans le cas contraire, on risque d'avoir une collision (quand les deux systèmes tentent de parler simultanément) ou un blocage (quand les deux systèmes se mettent à l'écoute simultanément). De plus, un délai supplémentaire peut être induit lors du basculement du sens de communication d'une direction à l'autre.

Si l'on prend l'exemple d'un capteur et d'un système d'enregistrement, la communication semi-duplex permettrait par exemple au capteur de se mettre en attente d'une requête de l'enregistreur, puis, à la demande de celui-ci de transférer les données mesurées.

c) La liaison full-duplex

Dans la communication full-duplex, les deux systèmes interconnectés sont capables d'émettre et de recevoir simultanément.

Du à l'existence d'un canal de transmission dédié à chaque sens de communication, ce mode de communication exige aussi que chacun des deux systèmes soit capable de traiter à la fois des données entrantes et sortantes.

Si l'on prend l'exemple d'un capteur et d'un système d'enregistrement, la communication full-duplex permettrait au capteur de transmettre ses données simultanément, tout en autorisant le système d'enregistrement à lui envoyer des commandes à tout moment. [W1]

C. Matériel d'interconnexion

Un réseau local sert à interconnecter des équipements de loin comme de près pour cela nous utilisons de différents protocoles de communication et différents types de matériels qui sont : [8]

a) Répéteur :

Dispositif amplifiant et répète les signaux qui lui parviennent pour étendre la distance de câblage dans un réseau local [8].

Figure 1.16 : Répéteur [F4].

b) Le pont :

Un pont (bridge) est un dispositif permettant de relier des réseaux de même nature [8].

Figure 1.17 : pont [F4].

c) Le routeur :

Les routeurs sont des équipements d'interconnexion qui agissent au niveau 3 (couche réseau) et permettant d'assurer le routage des paquets entre deux réseaux ou plus.

Il permet l'acheminement optimal des paquets de données entre différents réseaux. En général les routeurs intègrent un switch de petite capacité.

Un routeur contient généralement deux adresses IP une pour le réseau local et une autre pour sa connexion au deuxième réseau.

Il existe des modems qui contiennent un routeur et un switch intégré tel que F.A.I [9].

Figure 1.18 : Routeur [F4].

d) Passerelle :

La passerelle est un système matériel et logiciel qui sert à relier deux réseaux utilisant deux protocoles et/ou architectures différents, la passerelle crée un pont entre les deux réseaux. Les informations ne sont pas directement transmises, elles sont plutôt traduites pour assurer la transmission tout en respectant les deux protocoles.

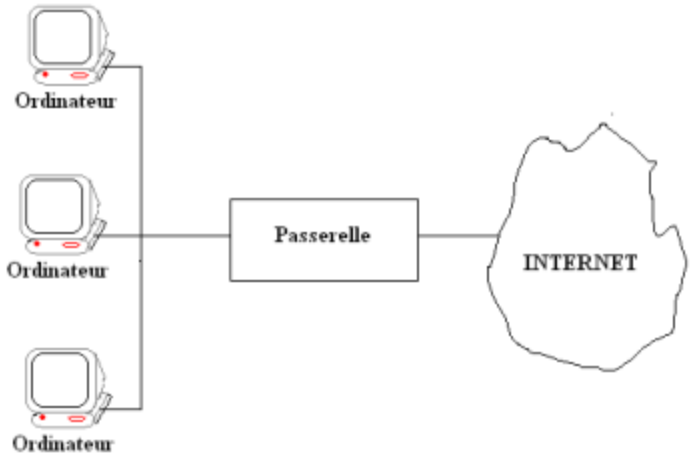

Figure 1.19 : Passerelle [F4].

e) Concentrateur (Hub)

Le concentrateur est un matériel permettant la concentration sur trafic réseau provenant de plusieurs hôtes et de régénérer le signal. Ce dernier opère au niveau 1 du modèle OSI.

Il possède autant de ports qu'il peut connecter de machines entre elles. Son rôle est de récupérer les données binaires parvenant sur un port et de les diffuser sur l'ensemble des ports. [8]

Figure 1.20 : concentrateur [F2].

f) Commutateur (switch) :

Le commutateur utilise un mécanisme de filtrage et de commutation consistant à diriger les flux de données uniquement vers les machines concernées. Ce dernier est actif et agissant au niveau 2 du modèle OSI.

Un commutateur inspecte les adresses de source et de destination des messages et ne transmettra le message que sur le port adéquat, les autres ports restants dès lors libres pour d'autres transmissions pouvant se produire simultanément. Contrairement au hub, on peut donc dire qu'il est « intelligent », car il est capable de savoir qui est le destinataire d'un message [9].

Figure 1.21 : Commutateur [F4].

g) Adaptateur :

Les adaptateurs (adapter) sont utilisés pour insérés dans un poste de travail ou un serveur afin de les connecter à un système de câblage [9].

Figure 1.22 : Adaptateur [F4].

h) Carte réseau :

Une carte réseau est une carte d'extension qui sert d'interface physique entre les périphériques. Elle a pour fonction de préparer, d'envoyer et de contrôler le flux de données sur le réseau, également à traduire les données venant du câble en octets afin que l'unité centrale de l'ordinateur les comprenne. Elle est insérée dans un slot libre de la machine [8].

Figure 1.23 : Carte réseau [F2].

1.8. Les modèles de références

Ces modèles permettent de classer divers protocoles réseaux, à savoir des standards qui décrivent telle ou telle fonctionnalité que le réseau doit respecter.

A. Le modèle OSI

Le modèle OSI (Open System Interconnection) est un cadre conceptuel qui définit la façon dont les systèmes de réseau communiquent et envoient des données des expéditeurs aux destinataires. Ce modèle est utilisé pour décrire chaque composant de la communication de données afin d'établir des règles et des normes pour les applications et l'infrastructure réseau.

Le modèle OSI est un modèle qui comporte 7 couches, qui sont réparties en couches hautes, couches intermédiaires et couches basses.

- Couche physique : c'est des signaux : modulation, puissance, support de transmission (câble, fibre optique).
- Couche liaison de donnée : établissement, maintient et libération des connexions entre les étalements du réseau, détection et correction des erreurs.
- Couche réseau : responsable de l'adressage et le routage.
- Couche transport : transfert entre utilisateurs (transparence).
- Couche session : optimisation et réglage des sessions (reprise de transfert).
- Couche présentation : compression et représentation (poids fort à gauche ou adroite).
- Couche application : offrir aux logiciels des standards d'accès aux réseaux (fichier virtuel) [3].

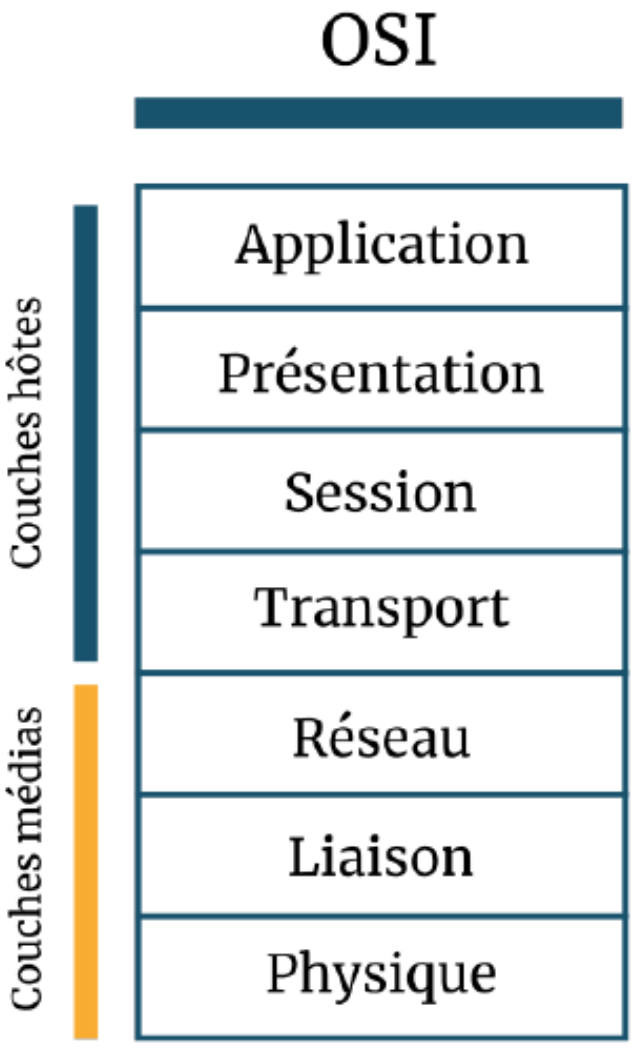

Figure 1.23 : Modèle OSI [F2].

B. Le modèle TCP/IP

Le modèle TCP/IP est une architecture qui est lié à deux protocoles : le protocole TCP et le protocole IP.

Les protocoles TCP/IP fonctionnent sur des couches qui peuvent être classées verticalement, et la couche supérieure exploite les services fournis par les couches inférieures. Chaque niveau contient des protocoles qui réglementent des règles spécifiques pour la transmission de données et desservent des niveaux supérieurs. C'est une architecture qui est basée sur quatre couches dans lesquelles chaque couche résout un certain nombre de problèmes afin que la communication entre équipements se fasse. [10]

Figure qui illustre la différence entre le modèle TCP/IP et le modèle OSI :

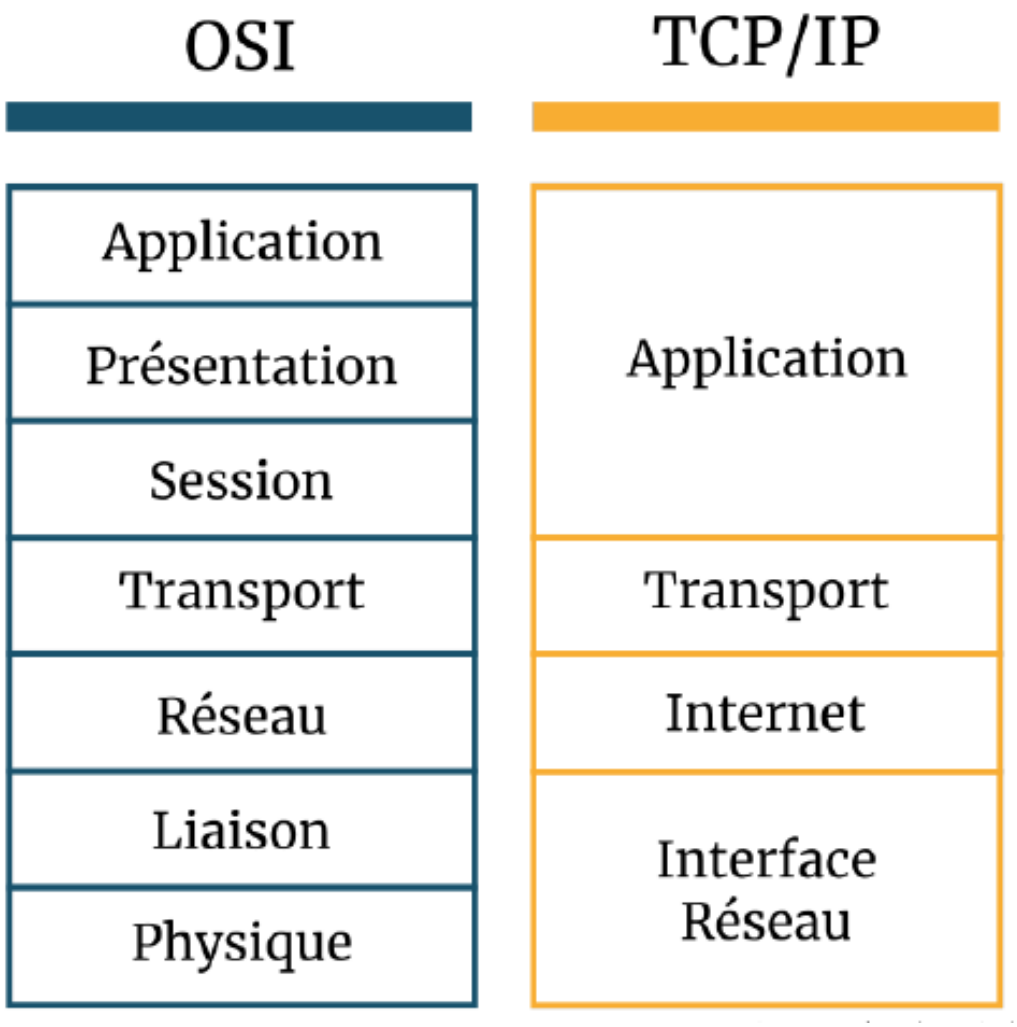

Figure 1.24 : Modèle OSI – TCP/IP [F2].

1.9. Conclusion

Dans ce chapitre nous avons passé en revue des généralités sur les réseaux informatiques, à savoir leurs objectifs et leur classification. Nous avons aussi découvert la topologie, l'architecture ainsi que les caractéristiques de ces réseaux et nous avons fini par montrer la déférence entre le modèle de référence OSI et le modèle TCP/IP.

CHAPITRE 2

Etude du réseau existant

Partie I : Etude de l'existant

2.1.Introduction

Le réseau d'entreprise a pour rôle de connecter tous les ordinateurs entre eux, via les périphériques de couche 1, 2,3 qui pourront donner l'accès aux utilisateurs à ses donnes et au partage de fichiers.

Dans cette première partie du chapitre, le but est de présenter l'entreprise Cevital Bejaia, son historique et les nombreux départements qui font partie de son infrastructure puis nous allons parler de la problématique du réseau Cevital, problématique qui sera le centre de notre projet.

2.2. Présentation de l'entreprise

En 1998, ISSAD Rebrarb créa l'entreprise CEVITAL Agro-industrie qui est devenue le leader du secteur agroalimentaire en Algérie. Implantée au sein du port de Bejaia (Algérie). CEVITAL Agro-industrie se compose de plusieurs unités de production telles que : raffinerie d'huile, raffinerie de sucre, margarinerie, unité de conditionnement d'eau minérale, unité de fabrication et de conditionnement de boisson rafraichissante, conserverie, silos portuaires ainsi qu'un terminal de déchargement portuaire.

CEVITAL Agro-industrie offre des produits de qualité supérieure à des prix compétitifs, grâce à son savoir-faire, ses unités de production ultramodernes, son contrôle strict de qualité et son réseau de distribution. Elle couvre les besoins nationaux et a permis de faire passer l'Algérie du stade d'importateur à celui d'exportateur pour les huiles, les margarines et le sucre. [11]

2.3. Historique de Cevital agro-industrie

1998 : Création de Cevital SPA industrie agro-alimentaire,

2006 : Acquisition de COJEK.

2007 : Création de MFG (VERRE PLAT),

2008 : Création de NUMILOG, 2013 : Acquisition d'OXXO.

Avant d'atteindre la notoriété quelle connait actuellement l'entreprise Cevital a traversé d'importantes étapes historiques avec un parcours et des valeurs qui ont fait sa réussite et sa renommée. Industrie agroalimentaire et grande distribution, électronique et électro-ménager, sidérurgie, industrie du verre plat, construction industrielle, automobile, services médias… Le

Groupe Cevital s'est construit, au fil du temps et surtout des investissements, autour de l'idée forte de constituer un ensemble économique.

Cevital œuvre continuellement dans la création d'emplois et de richesse. Elle est l'origine de la création de 3494 emplois en l'espace de 9 ans (1999-2008), sans compter les emplois indirects générés grâce aux plusieurs centaines de sous-traitants auxquels elle fait appel. [11]

2.4. Emplacement géographique de l'entreprise

Le complexe de production de Cevital se situe dans le nouveau quai de port BP 334 liberté Bejaia, à 3km du sud-ouest st de la ville. Cette situation géographique lui profite bien étant donné qu'elle lui offre l'avantage de la proximité économique.

En effet, elle se situe très proche du port et de l'aéroport de Bejaia ce qui lui permet de posséder un quai privé. Le complexe s'étend sur une superficie de 45 000 m² ce qui est considéré comme le plus grand complexe privé en Algérie. Il a une capacité de stockage de 182 000 tonnes/an (Silos portuaires), 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 2.1 : Image satellitaire de CEVITAL Bejaia.

2.5.Infrastructure de l'entreprise

Après la création de l'entreprise en 1998, Cevital Agro-industrie a fait des avancées importantes et possède aujourd'hui plusieurs unités de production ultramodernes :

- 2 raffineries de sucre.
- 1 unité de sucre liquide.
- 1 raffinerie d'huile.
- 1 margarinerie
- 1 unité de conditionnement d'eau minérale (se situe à Tizi Ouzou).
- 1 unité de fabrication et de conditionnement de boissons rafraîchissantes (site EL-Kser).
- 1 conserverie.

Cevital est aujourd'hui le premier terminal de déchargement portuaire en Méditerranée. Ceci est dû à la possession de plusieurs silos portuaires ainsi que celle d'un terminal de déchargement d'une capacité de 2000 tonnes/heure. [11]

2.6.Organigramme de Cevital

L'organigramme général de l'organisation administrative de l'entreprise de Cevital se présente sous la fourme du schéma ci-dessous :

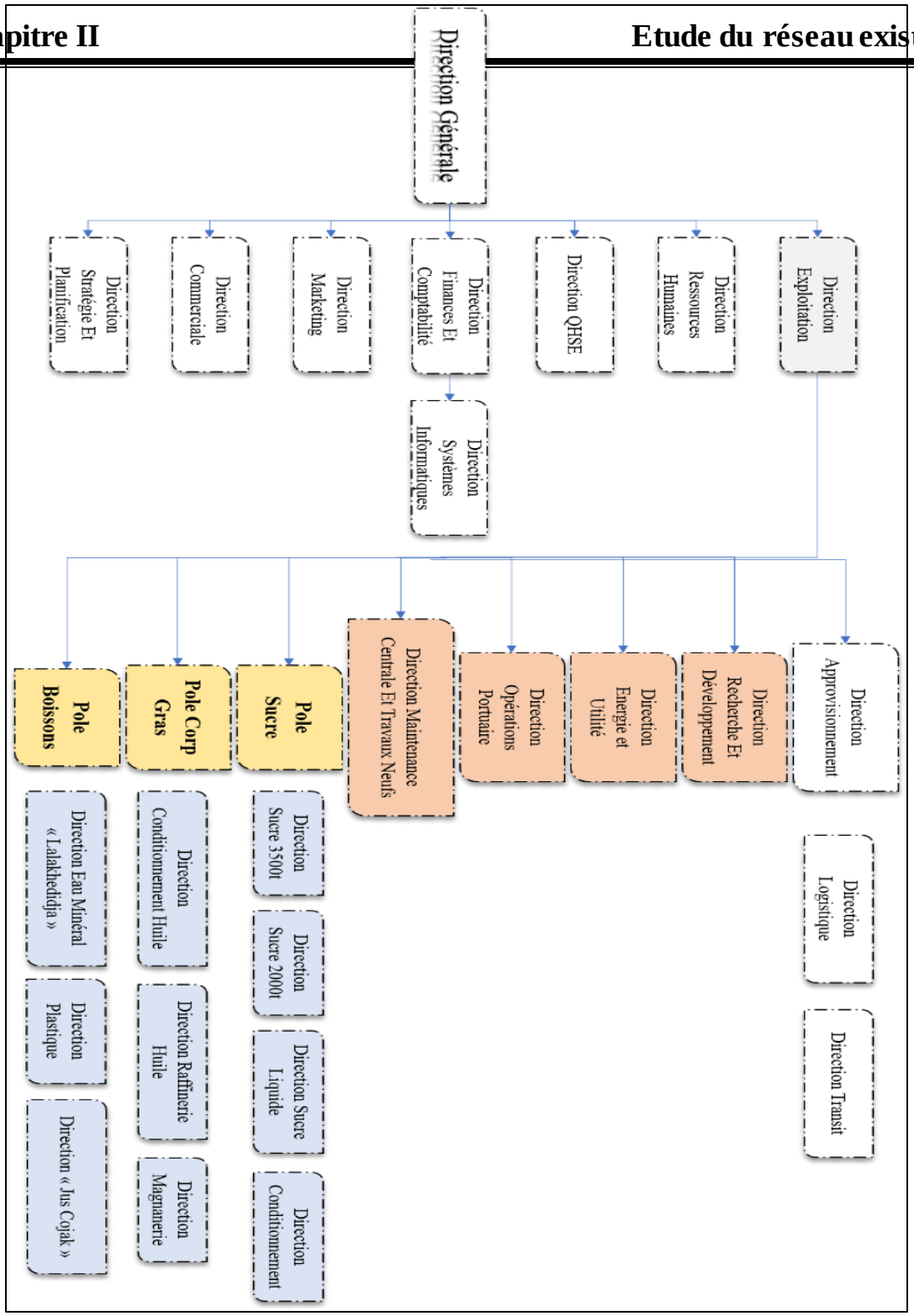

Figure 2.2 : Organigramme de l'organisation administrative de Cevital. [11]

2.7.Architecture du réseau Cevital

Afin de pouvoir relier les différentes annexes, unités de production et direction du complexe, Cevital a mis en place un grand réseau interne. Ce réseau peut se décomposer en plusieurs parties : Le backbone du réseau, un pare-feu et un DMZ (démilitarized zone) une couverture WIFI, un routeur et un Datacenter (ou sont placés les serveurs de l'entreprise). Il est composé

de plusieurs équipements dont la plupart sont de marque Cisco (Switch, Catalyst, Routeur) interconnectés entre eu grâce à la fibre optique, ou cuivre.

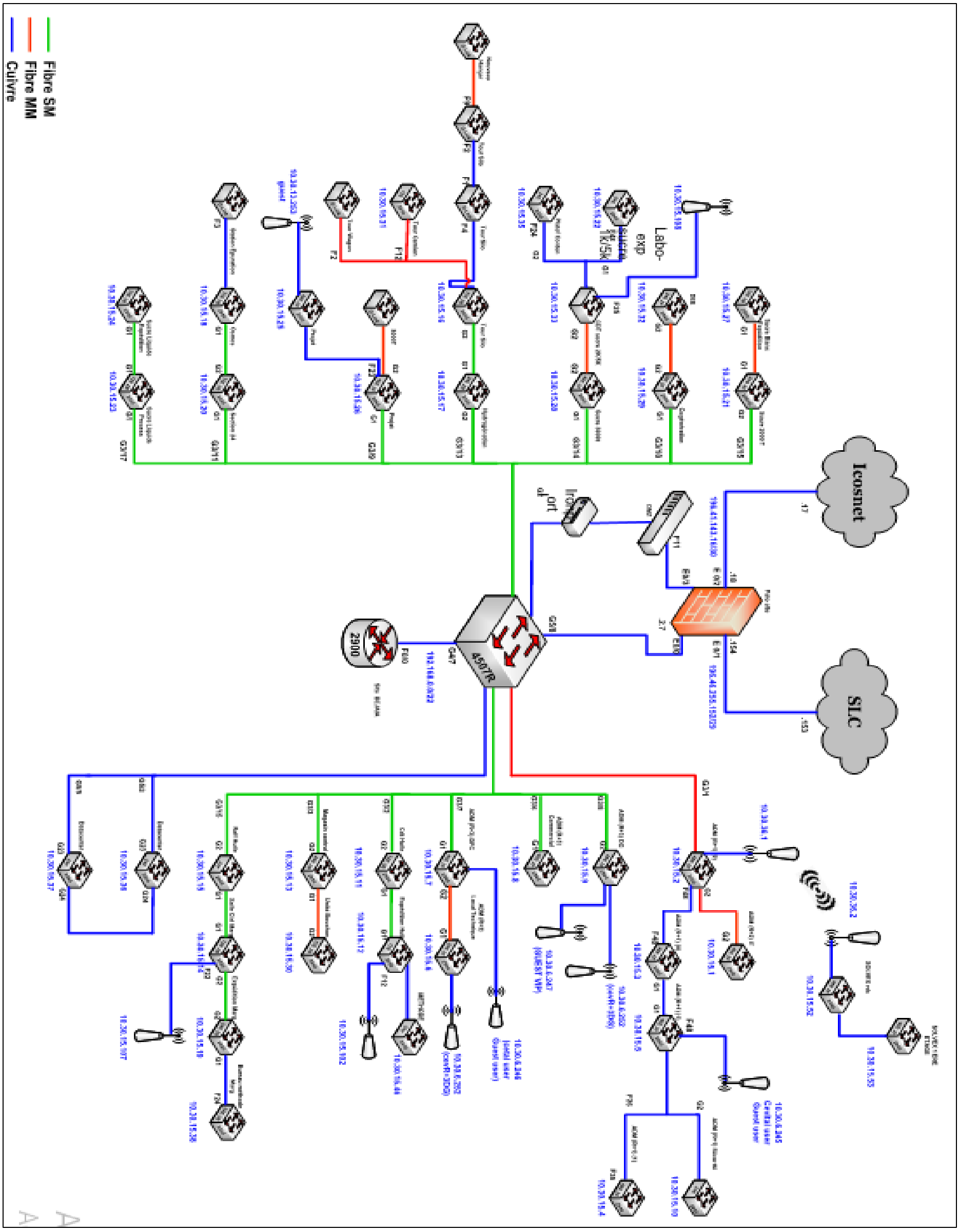

Figure 2.3 : Architecture du réseau informatique du site Cevital Bejaia.

2.8.Equipements utilisés dans l'architecture :

Les équipements utilisés à l'entreprise sont :

A. Distributeur (backbone) Cisco CATALYST 4507R :

Le distributeur est l'élément central du réseau, il est constitué de 7 slots, 244 ports et une alimentation allons jusqu'à 1500W. Il prend en charge le trafic de données le plus important du réseau complexe à très haut débit auquel sont connectés les commutateurs d'accès, les pare-feu, les serveurs et les routeurs de l'entreprise. Il est responsable du routage inter-VLAN. Il accorde l'accès à Internet via un pare-feu, généralement un serveur DHCP.

Figure 2.4 : Distributeur (backbone) [F4].

B. Switch d'accès : Cisco Catalyst 2960 et 2950 :

Les switches sont installés dans les différents bâtiments de l'entreprise et nous pouvons connectés directement 24 ports avec un câble Rj-45 au distributeur ça bande passante est de transfert est de 16 Gbits/s, une mémoire de flash 32 Mo, mémoire de DRAM 64 Mo il peut prendre jusqu'à 64 VLAN.

Figure 2.5 : switch d'accès [F4].

C. Switch en cascade : Cisco Catalyst 2950 et 2960 :

Les différents commutateurs de cette couche sont montés en cascade c'est l'interconnexion de plusieurs switches d'accès qui permet de créer des switches en cascade et offrent aux utilisateurs un accès au réseau Au sein de leurs commutateurs, les VLAN peuvent définir plusieurs sous-réseaux selon le service de l'entreprise.

Figure 2.6 : switch en cascade [F4].

D. Routeur : Cisco 2900 :

Un routeur est un élément qui permet de faire circuler les données, de protéger les informations contre les menaces de sécurité, et a le pouvoir de donner la priorité à une machine par rapport aux autres.

La gamme cisco 2900 peut offrir 2 ou 3 ports GE avec un port SFP leur RAM est de 2,5 Go et 8 Go de mémoire flash, il peut offrir jusqu'à 75 Mbps. Un routeur supporte plusieurs protocoles tel que IPv4, IPv6, OSPF, IGRP, BGP.

Figure 2.7 : Routeur Cisco 2900 [F4].

E. Point d'accès WIFI :

L'entreprise dispose de plusieurs points d'accès WIFI pour créer une couverture réseau sans fil dans certaines parties du complexe.

Un réseau sans fil peut attendre une distance de 3000 m avec un débit de transfert qui peut aller jusqu'à 867 Mbits/s avec une bande de fréquence qui varie de 2,5 GHz a 5 GHz.

Figure 2.8 : point d'accès WIFI Cisco [F4].

F. Pare feu :

Le pare-feu protège la totalité du trafic réseau et a la capacité d'identifier et de bloquer le trafic indésirable. Deux pare-feu reliés en redondance permettent de sécuriser le réseau, d'isoler certaines parties de celui-ci, encadre et sécurise l'accès internet.

Un pare-feu est composé d'un débit équivalent à 2Gbits/s avec un débit prévenance des menaces de 1Gbites/s et un débit de VPN qui est 500 Mbits/s, il est relié avec un câble virtuel et les protocoles supportés sont OSPFv2/v3, BGP, RIP, IGMP, BFD.

Figure 2.9 : Pare feu Palo Alto 3020[F4].

G. Data center

Le data center est une salle sécurisée dont l'accès est restreint aux seuls responsables et techniciens de la DSI (Direction des Systèmes d'Information), la température est régulée par le système de climatisation, la puissance est doublée, le bon fonctionnement des équipements est garanti.

Le data center de Cevital es considérer le noyau central du réseau de l'entreprise on y retrouve :

- Les serveurs de l'entreprise.
- Le switch cœur.
- Les pare feu.
- Les routeurs.
- Le standard téléphonique

Figure2.10 : DATA center [11].

2.9.VLAN de l'entreprise

Un réseau local virtuel (VLAN) est un réseau local distribué sur des équipements au niveau 2 du modèle OSI. C'est une technologie qui permet de perfectionner le réseau fractionnant le réseau en plusieurs VLANs.

L'entreprise Cevital a mis en place cette technologie dans sa topologie. Elle a donc segmenté le réseau en plusieurs VLANs en fonction des différents départements. L'adressage utilisé dans l'architecture est de classe A, segmenter en plusieurs sous réseaux 10.10.0.0/24.

Le tableau suivant montre la liste les VLANs de l'entreprise :

VLAN		Direction
ID	Nom	/
10	DRH	Direction des Ressources Humaine
11	Achat	/
12	IT	Technologie de l'Information
13	RFreduction	Raffinerie réduction
14	RFsucre	Raffinerie Sucre
15	DEE	
16	DFC	Direction Finance et comptabilité
17	Commercial	/
18	Imprimante	/
19	DG	Direction Général
20	Serveur	/

Tableau 2.1 : Liste des VLANs de l'entreprise.

2.10.Emploi d'un réseau informatique

L'une des principales utilisations d'un réseau informatique est la possibilité du partage de fichier pas un accès aux fichiers à distance.

Cevital a plusieurs utilisateurs et collaborateurs qui exploitent divers applications et services offerts par le réseau pour permettre le bon fonctionnement de leur travail. Nous pouvons citer les applications et services suivants :

- Applications de gestion de la production assistée par ordinateur.
- Cloud privé est dédié pour le partage de document.
- Service Mail.
- Gestion des stocks et Application compatibilité.
- Donner un accès aux collaborateurs.

2.11. Critique du réseau existant

Dans ce qui a précédé, nous avons passé en revue tous les caractéristiques du réseau informatique déjà existant de l'entreprise Cevital Bejaia. Nous avons alors remarqué plusieurs lacunes, qui mettent fortement en péril les performances du réseau existant, et qui peuvent même donner des dysfonctionnements fréquents.

Les lacunes remarqués se résument alors à :

- Absence de liaison avec les sites distants ce qui implique que chaque site a son propre data center, non seulement c'est couteux mais en plus le partage de ressources et de la communication sont inexistants.
- Il n'existe qu'un seul backbone qui se charge de centraliser le réseau. Ce qui entraine la surcharge de ce dernier.
- Il existe plusieurs points de défaillance dans l'architecture du réseau qui sont dus au manque de serveurs redondants. Ces derniers ont pour rôle de garantir la tolérance aux pannes, ainsi que les connexions de secours aux appareils.
- La liaison en cascade des switches limite la bande passante ce qui ralentit les applications ainsi que les ressources et la défaillance de l'un des switches couperait du réseau à tous les utilisateurs.

2.12. Problématique

La prise en charge des réseaux informatiques des grandes entreprises, est très importante pour assurer le bon fonctionnement et la continuité du réseau, et donc pour assurer les services de collecte, de stockage, de traitement et de communication des informations entre les salariés.

Qui sont non seulement nombreux, mais également dispersés en plusieurs endroits. En revanche, elle provoque un ralentissement ou un arrêt de l'activité, affectant ainsi le bon fonctionnement de l'équipe et sa productivité.

On conclut alors que l'infrastructure du réseau d'entreprise devient primordiale. La problématique qui se pose est de trouver la topologie à utiliser pour assurer la continuité et le bon fonctionnement du réseau Cevital. Tout en faisant face aux pannes des dispositifs et en garantissant la communication des informations entre les employés même à des sites distants.

2.13.Proposition

Dans l'optique de trouver une solution appropriée au problème qui a été posé, nous suggérons de :

- Mettre en place des connexions inter-sites avec des liaisons spécialisés entre le site central et les sites distants tout en assurant un équilibrage des charges entre les liaisons afin de permettre le partage de ressources et de la communication.
- Pour minimiser le nombre de commutateurs en cascade, on pourrait utiliser une architecture avec deux backbones interconnectés et redondants tout en mettant en œuvre des protocoles de haute disponibilité et de routage au niveau du cœur.
- L'utilisation d'un protocole de hautes disponibilités serait une solution pour le problème de défaillance des appareils.

2.14.Solution adoptée

Après avoir démontré les problèmes du réseau existant de Cevital nous avons travaillé afin de trouver une solution adéquate. Nous sommes donc arrivés à la conclusion que la meilleure solution est de premièrement commencer par utiliser une architecture à 2 switches de niveau 3 renforcée avec un protocole de routage OSPF. On ajouterait ensuite un protocole de haute disponibilité au niveau de la distribution, dans ce cas nous avons préféré choisir le HSRP. Pour minimiser le nombre de switch en cascade, nous avons opté pour la connexion du plus grand nombre de switches directement au backbones de distribution. Et enfin nous mettrons en place des connexions vers les routeurs Algérie Télécom, pour qu'ils puissent établir des liaisons de fibre optique point à point entre Bejaïa et les sites distants d'EL Kser (Cojek) et de Tizi-Ouzou (Lala Khadija).

2.15.Déduction

Cette partie nous a donné une vision globale du réseau informatique de Cevital. Et a mis en évidence certains problèmes importants qui ont conduit à la proposition d'une solution. Cette dernière se résume principalement à une proposition d'une nouvelle d'architecture du réseau, à l'implémentation de la haute disponibilité et la mise en place d'une connexion inter-sites.

Partie II : La haute disponibilité

2.16.Introduction

Après avoir déduit dans la première partie de ce chapitre que l'une des mesures les plus primordiales pour régler les défaillances du réseau existant de Cevital est l'implémentation de la haute disponibilité. Il s'agit de toutes les solutions mobilisées pour assurer la disponibilité d'un service. Ce concept garantit donc le bon fonctionnement du service en question, 24h sur 24 et ce, sans interruption.

Cette partie sera donc consacrée à la définition de nombreux protocoles exploitables pour assurer ceci.

2.17.La redondance

Le principe de la redondance du réseau consiste à la reproduction d'un composant du système informatique dans le but d'avoir recours à une solution de rechange lorsqu'un élément dupliqué est défaillant. Il permet donc d'améliorer la fiabilité, la sécurité et la disponibilité du réseau de l'entreprise. La redondance se présente alors comme une solution incontournable pour assurer la haute disponibilité [W5].

2.18.Les protocoles de redondance

Pour amener à bien un réseau d'entreprise et assurer la redondance de ce dernier. Il existe une multitude de protocoles. Chacun des protocoles possède un rôle différent.

A. HSRP (Hot Strandby Router Protocol)

Le protocole HSRP (Hot Standby Routing Protocol) est un protocole mis en place par Cisco. Il permet de garantir la haute disponibilité et d'augmenter la tolérance de panne. Le principe de ce protocole est d'instaurer une mise en commun du fonctionnement de plusieurs routeurs physiques ou de switch de niveau 3 (2 au minimum), de façon à ce que la relève puisse être assurée entre eux. En d'autres termes HSRP permet à ce qu'un routeur de secours prenne automatiquement et instantanément le relais de façon transparente dès l'apparition d'un problème.

- **Fonctionnement du HSRP**

Le fonctionnement du protocole HSRP consiste en pratique à utiliser deux routeurs (ou plus) pour former un même groupe que l'on nomme « standby group ». Les routeurs seront considérés comme un seul routeur dit "Virtuel", qui deviendra l'unique passerelle des hôtes du réseau local. Les membres du groupe de ce routeur virtuel qui se trouvent être des routeurs physiques ont la capacité de s'échanger des messages d'état et des informations. Un routeur physique peut donc être "responsable" du routage ; il s'agit ici du routeur actif qui est élu au moyen d'une priorité, pour transmettre les paquets envoyés au routeur virtuel. L'autre sera en redondance ; il sera nommé routeur passif. Il aura la tâche de transmettre les paquets à la place du routeur actif en cas de défaillance.

Au moment où le routeur actif travaille, il envoie des messages aux autres routeurs qui sont dans le groupe « standby group » pour leur préciser qu'il fonctionne toujours. Lorsqu'il tombe en panne, il est automatiquement remplacé par un routeur passif. Les paquets continueront de transiter de manière transparente car tous les routeurs partagent les mêmes adresses IP et MAC aux yeux des hôtes du réseau ; et ce malgré le changement du chemin par lequel transitent les paquets [W6].

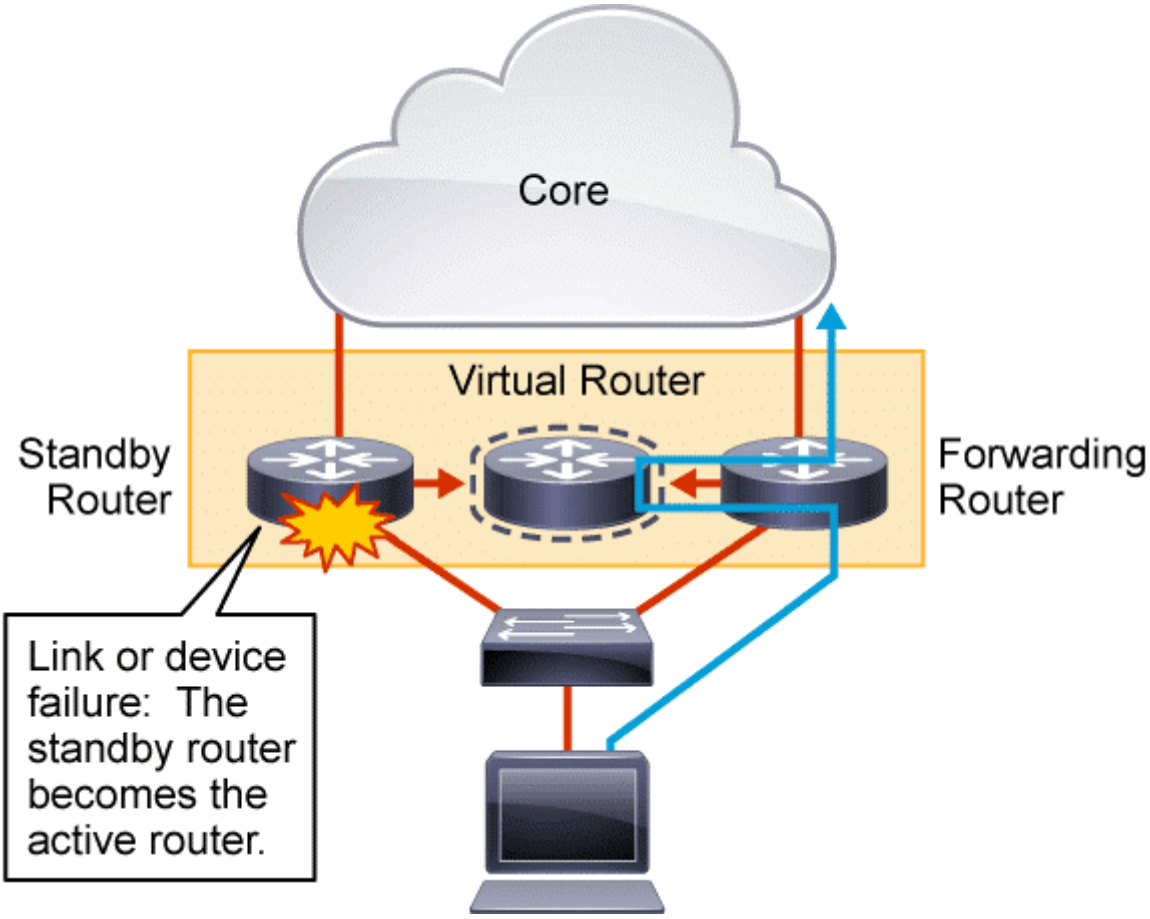

Figure 2.11 : schéma physique et virtuel d'un réseau HSRP [F5].

B. VRRP (Virtual Router Redundancy Protocol)

Parmi les protocoles qui assurent la redondance, il existe le protocole de Redondance de Routeur Virtuel (Virtuel Router Redundancy Protocol, VRRP). Il s'agit d'un protocole visant à accroitre la disponibilité de la passerelle par défaut qui sert les hôtes d'un même sous-réseau.

Le VRRP est un protocole d'élection. Il attribue de façon dynamique les charges d'un routeur virtuel à l'un des routeurs VRRP présents dans le réseau local. L'un des membres du groupe VRRP sera nommé routeur maître sur la base de la priorité, et son rôle consistera à être responsable du transfert du trafic local. Il n'y aura qu'un seul routeur maitre qui sera désigné. Les autres routeurs eux seront des routeurs de secours. Ces routeurs de secours seront prêts à prendre le relais du routeur maître en cas de défaillance de ce dernier.

L'aboutissement de l'emploi de la fonctionnalité VRRP est de pouvoir de disposer d'un chemin d'accès par défaut extrêmement disponible pour le processus de routage même sans

configurer le routage dynamique ou les protocoles de décèlement de routeur sur chaque hôte final [W6].

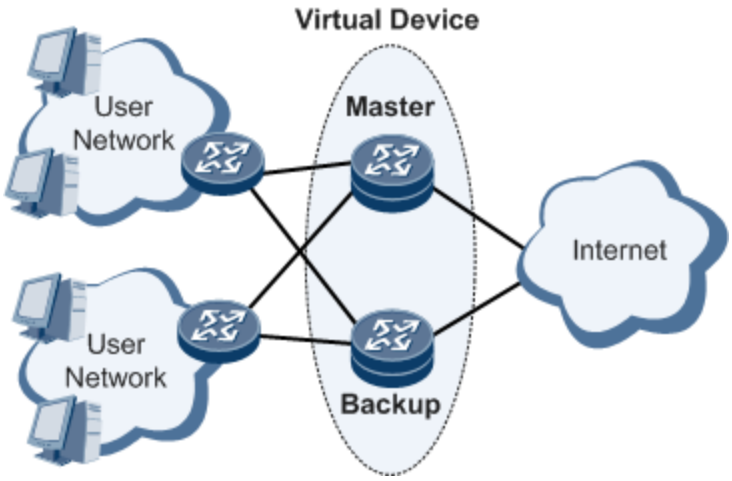

Figure 2.12 : schéma d'un réseau VRRP. [F6]

C. GLBP (Gateway Load Blancing Protocol)

Le protocole GLBP combine deux fonctions principales. Premièrement il se charge de gérer les passerelles redondantes. Et de l'autre côté, il permet d'équilibrer le trafic entre elles.

La différence entre le protocole GLBP et les protocoles HSRP et VRRP dont nous avons parlé précédemment réside dans le fait d'impliquer tous les routeurs dans le routage, alors qu'avec les autres protocoles cités ; un seul routeur était considéré comme actif, tandis que les autres étaient en standby. Le GLBP permet donc une utilisation complète de la bande passante dédiée à tous les routeurs.

Le routeur avec la plus grande priorité, ou dans le cas de priorité égale, la plus grande adresse IP configurée sera nommé « AVG » (Active Virtual Gateway). Les autres routeurs auront le statut « AVF » (Active Virtual Forwarders). Le principal rôle de l'AVG est de distribuer la charge entre les différentes passerelles de façon équilibrée. Pour se faire, il interceptera toutes les requêtes ARP et y répondra en altérant la réponse, indiquant la sienne, celle d'un AVF, celle de l'AVF suivant, etc. Les routeurs échangent entre eux, et dès que l'AVG disparaît de la rotation au niveau des réponses ARP, le meilleur AVF se chargera de le remplacer [W6],

2.19.STP (Spanning Tree Protocol)

Le protocole STP (Spainning Tree Protocol) est un protocole qui a été conçu pour les commutateurs. Son rôle réside en la création de chemin unique entre deux points, autrement dit

un chemin sans boucles dans les réseaux commutés. Ce qui nous évitera une paralysie du réseau et nous aidera à garder une topologie physique redondante. Le STP détecte ces boucles, les désactive, et fournit un mécanisme de liens de sauvegarde.

Dans un réseau commuté on procède à une élection machinale d'un switch maître (root bridge) par le STP. L'élection de ce root bridge sera faite en fonction des numéros de priorité configurés. Dans le cas de priorité égale on se tournera vers l'adresse MAC la plus basse. Après ça sera au tour de la désignation des ports racine (root port), qui se trouvent être le port avec la « distance » la plus courte vers le commutateur racine. Chaque commutateur possède un seul root port qui est choisi d'après le coût du trajet vers le root bridge. Pour finir il y'aura ce qu'on appelle la détermination des ports désignés, ça consiste à designer le port relié au segment qui mène le plus directement à la racine. Les ports restants seront bloqués.

Les BPDU (Bridge Protocol Data Unit) sont les diffuseurs de toutes informations du protocole STP, ils servent à conserver une empreinte des changements sur le réseau dans le but d'activer ou de désactiver les ports voulus et déterminer la topologie du réseau [13].

A. PVST (Per-VLAN Spanning Tree)

Le PVST (Per-VLAN Spanning Tree) est un mode fonctionnement mis en place par Cisco. Il permet au STP dans un réseau qui contient plusieurs VLAN d'agir de manière indépendante sur chacun des VLAN séparément. Il est capable d'effectuer un équilibrage de charge de couche 2 en transférant une partie du trafic VLAN sur une liaison d'assemblage et un autre trafic VLAN sur une autre liaison d'assemblage [13].

2.20. EtherChannel

L'EtherChannel est une technologie qui a pour but d'augmenter la vitesse en procurant des liaisons à haut débit, de fournir une redondance et de d'augmenter la tolérance aux pannes entre les commutateurs. A cet effet la méthode est d'assembler plusieurs liens de ports physiques pour créer un seul lien logique. Le maximum de liens de ports physiques qu'on peut assembler est de 8 liens [13].

2.21. VTP (VLAN Trunking Protocol)

Le protocole VTP (VLAN Trunking Protocol) donne le moyen de directement configurer les VLAN sur un seul commutateur dit serveur, qui diffusera cette configuration vers les autres

commutateurs du réseau qui seront en mode client. Si une modification doit être faite sur la configuration sur les réseaux locaux virtuels, elle sera faite aussi directement sur le commutateur en mode serveur. Grace à cela aucune incohérence de configuration ne peut se faire entre tous les commutateurs.

Les commutateurs peuvent être en trois modes différents. Le mode serveur, transparent et client. Leurs rôles consistent à configurer et diffuser l'information pour le mode serveur ; recevoir la configuration et la transmettre à d'autres commutateurs sans la prendre en compte pour le mode transparent ; en ce qui concerne les commutateurs en mode client ils reçoivent la configuration et l'appliquent automatiquement [15].

2.22.Les protocoles de routage

Il existe plusieurs protocoles de routage, tels que le RIP, l'EIGRP et l'OSPF. Ce sont des systèmes de communication qui pour rôle de partager des informations entre des routeurs et d'aider à construire et mettre à jour une table de routage [16].

A. RIP (Routing Information Protocol)

Le protocole RIP (Routing Information Protocol) est un protocole de routage qui se base sur le nombre de sauts pour calculer la valeur qui définit le chemin le plus adéquat à emprunter pour atteindre un réseau. L'ultime objectif de ce protocole est de permettre aux routeurs de communiquer à distances relativement courtes (<= 15 sauts).

B. EIGRP (Enhanced Interior Gateway Routing Protocol)

Le protocole EIGRP (Enhanced Interior Gateway Routing Protocol) est un protocole de routage propriétaire mis en place par Cisco. Ce qui implique que jusqu'à 2013 ou il est devenu partiellement ouvert, il ne pouvait être utilisé que par des équipements Cisco. EIGRP est un protocole de routage à vecteur de distance IP tout en utilisant des fonctions d'un protocole à état de lien. Il se base sur la métrique, tenant compte de la bande passante et du délai, et non pas des sauts. Il utilise DUAL (Diffusion Update Algorithm) pour sélectionner le meilleur chemin dans un réseau. Mais aussi un second chemin de secours. Ce qui est très efficace lors de panne.

C. OSPF (Open Shortest Path First)

Le protocole OSPF (Open Shortest Path First) est protocole de routage interne à état de lien. Contrairement au RIP il prend en compte l'état de liaison qui sépare les routeurs au lieu du

nombre de sauts qui les séparent, ce qui aide à déterminer un meilleur chemin avec une meilleure bande passante utile. L'OSPF fait en sorte que chaque routeur connaisse plus que son voisinage, mais aussi la totalité des routeurs présents dans son réseau.

2.23. Conclusion

Après avoir passé en revue les caractéristiques du réseau informatique de Cevital, découvert ses failles et proposé une solution dans la première partie de ce chapitre. Nous avons dans la deuxième partie découvert plusieurs protocoles qui pouvaient assurer la haute disponibilité et qu'on pourrait utiliser lors de notre projet afin régler les défaillances du réseau existant. Nous les avons définis et nous avons montré les avantages qu'ils pourraient apporter.

Chapitre 3

Réalisation et configuration du réseau Cevital

3.1.Introduction

Dans ce chapitre qu'on va deviser en 2 parties, nous allons dans un premier temps reconfigurer le réseau déjà existant de Cevital pour mettre en lumière les configurations et protocoles déjà utilisés tels que la segmentation de VLAN, le VTP, le DHCP, etc., et exposer leurs utilités. Puis après avoir réalisé que malgré ces utilités, il subsiste certaines faiblesses très dérangeantes dans cette configuration, nous allons passer à la deuxième partie de ce chapitre qui consistera à la proposition d'une nouvelle configuration afin d'améliorer et de corriger les faiblesses du réseau existant avec des nouveaux protocoles tels que le STP, HSRP et l'OSPF. Les deux configurations seront basées sur le simulateur CISCO Packet tracer 8.1.0.

3.2.Présentation du simulateur

Packet tracer est un simulateur de réseaux, qui permet à construire un réseau physique virtuelle, de simuler les comportements des protocoles sur une quelconque topologie de réseau. Le logiciel permet aux utilisateurs d'exercer et de créer leurs propres configurations avant de passer à la pratique. Nous avons choisi d'utiliser un simulateur car il permet de tester la fiabilité des configurations avant la mise en œuvre sur des périphériques couteux. Il facilite également la correction et mise à jour des configurations en cas d'inadéquation. Le Packet tracer fournit les fonctionnalités nécessaires qu'on trouve dans les réseaux réels, même les professionnels réseaux commencent par tester quelques configurations sur des simulateurs tels que Packet tracer, gns3, etc.

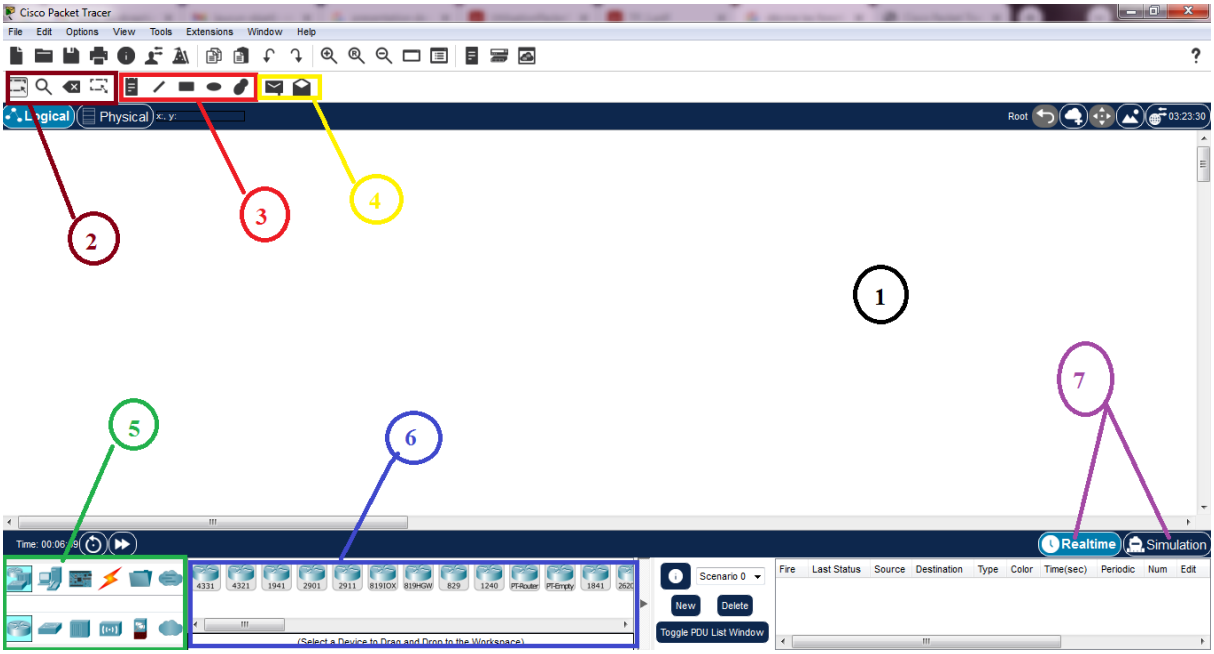

Figure 3.1 : capture de l'interface du simulateur Cisco Packet tracer 8.1.0.

Zone 1 : la partie dans laquelle on construit le réseau.

Zone2 : c'est un ensemble d'outils (sélection, inspection, suppression et redimensionner la forme).

Zone 3 : c'est la partie ou on trouve l'annotation du schéma et des palettes de dialogue.

Zone 4 : c'est la partie du test de communication.

Zone 5 : la partie dont on trouve le type des équipements.

Zone 6 : la partie des équipements.

Zone 7 : c'est la partie qui permet le passage du mode réel au mode simulation.

3.3.Présentation du réseau existant

A. Segmentation du réseau en VLAN

Le réseau a été divisé en plusieurs sections, chaque section représente un VLAN par cela il y aura naissances de plusieurs VLAN nous citons les suivant :

- DRH
- Achat
- IT
- RFreduction

- RFsucre
- DEE
- DFC
- Commercial
- Imprimante
- DG
- Serveur

B. Adressage des VLANs :

Nom des VLANs	VLAN ID	Adresse sous-réseau	Masque sous-réseau	Description
DRH	10	10.10.10.0/24	255.255.255.0	Direction des ressources humaines
Achat	11	10.10.11.0/24	255.255.255.0	/
IT	12	10.10.12.0/24	255.255.255.0	Technologie de l'information
RFreduction	13	10.10.13.0/24	255.255.255.0	Raffinerie réduction
RFsucre	14	10.10.14.0/24	255.255.255.0	Raffinerie sucre
DEE	15	10.10.15.0/24	255.255.255.0	
DFC	16	10.10.16.0/24	255.255.255.0	Direction finance et comptabilité
Commercial	17	10.10.17.0/24	255.255.255.0	/
Imprimante	18	10.10.18.0/24	255.255.255.0	/
DG	19	10.10.19.0/24	255.255.255.0	Direction général

Serveur	20	10.10.20.0/24	255.255.255.0	/

Tableau 3.1 : Liste des noms VLANs du réseau et leur plan d'adressage.

3.4. Partie 1 : le réseau existant

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

- La création des VLANs et de leurs interfaces.
- La configuration du protocole DHCP.
- La configuration des liens Trunk.
- La configuration de VTP.

A. Architecture de mise en œuvre

Nous avons reconfiguré l'architecture du réseau existant sur le simulateur CISCO Packet tracer 8.1.0. La topologie est représentée ci-dessous :

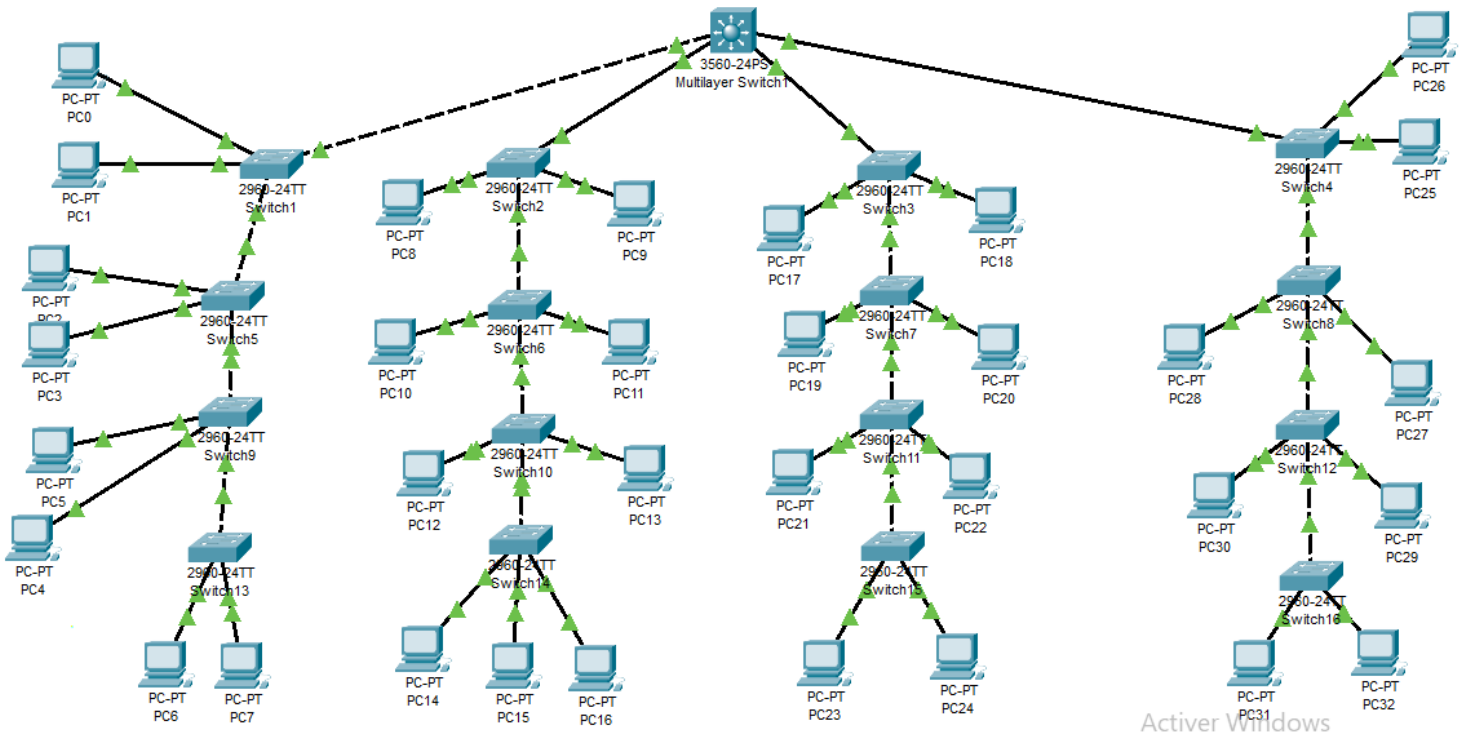

Figure 3.2 : Architecture du réseau local existant de CEVITAL.

B. Configuration des équipements du réseau existant

Dans cette topologie du réseau, nous allons utiliser principalement un switch Multiplier (Cisco Catalyst356) de niveau3 qui aura le rôle de switch Core et de distribution, des switches d'accès (Cisco Catalyst260) de niveau 2 ainsi que des PC. Et nous allons présenter un exemple de configuration de chaque équipement.

a) Configuration des Hostname et sécurité

Cette configuration nous permet d'abord de renommer l'équipement voulu par un nom significatif pour que ça soit plus facile de s'y retrouver. Elle nous donne aussi la possibilité aussi de limiter l'accès aux personnes étrangères en protégeant l'accès au mode privilégié. Ceci en sécurisant l'équipement avec un mot de passe robuste.

Dans **la figure 3.4** nous avons renommé le switch core de niveau 3 « Score » et nous l'avons sécurisé avec un mot de passe « CEVITAL ».

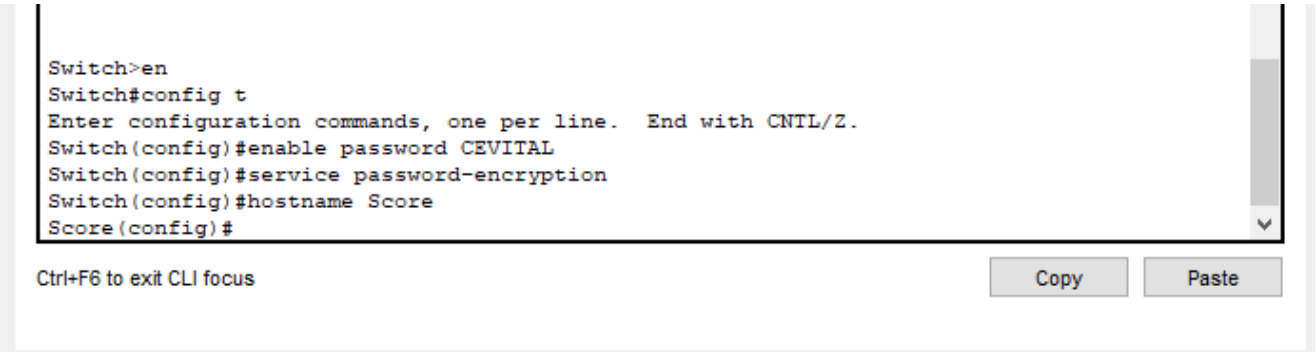

Figure 3.3 : Configuration des noms des hôtes et sécurité.

b) Création des VLANs

La création des VLAN se fait au niveau du switch Core. Nous avons créé les VLAN de l'entreprise au niveau du switch core. **Le listing 3.1** montre un exemple de la façon de créer

des VLANs. Pour monter tous les VLANs qui ont été créés nous avons utilisé la commande **show vlan brief,** le résultat est révélé dans **le Listing 3.2.**

```
Score(config)#vlan 10
Score(config-vlan)#name DRH
Score(config-vlan)#vlan 11
Score(config-vlan)#name achat
Score(config-vlan)#exit
```

***Listing 3.1** : Création des VLANs.*

```
10          DRH                 active
11          achat               active
12          IT                  active
13          RFreduction         active
14          RFsucre             active
15          DEE                 active
16          DFC                 active
17          commercial          active
18          imprimente          active
19          DG                  active
20          server              active
```

***Listing 3.2** : Vérification de la création de tous les VLANs.*

c) Configuration des interfaces VLANs

Le principe de la configuration des interfaces virtuelles des VLANs consiste à attribuer une adresse IP à chaque interface. L'opération se déroule au niveau du switch core.

Nous avons configuré les interfaces des VLANs précédemment créés. **Le listing 3.3** démontre la méthode avec la configuration des interfaces avec la configuration du VLAN 10. Après la configuration des interfaces de tous les VLAN, nous avons utilisé la commande **show running-config** pour vérifier toutes les interfaces. Le résultat se présente dans **Le listing 3.4**.

```
Score#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Score(config)#interface vlan 10
Score(config-if)#ip address 10.10.10.254 255.255.255.0
```

```
Score(config-if)#exit
```

***Listing 3.3**: configuration des interfaces au VLAN 10.*

```
interface  Vlan10
mac-address 000a.f3cc.8201
ip address 10.10.10.254 255.255.255.0
!
interface  Vlan11
mac-address 000a.f3cc.8202
ip address 10.10.11.254 255.255.255.0
!
interface  Vlan12
mac-address 000a.f3cc.8203
ip address 10.10.12.254 255.255.255.0
!
interface  Vlan13
mac-address 000a.f3cc.8204
ip address 10.10.13.254 255.255.255.0
!
interface  Vlan14
mac-address 000a.f3cc.8205
ip address 10.10.14.254 255.255.255.0
!
interface  Vlan15
mac-address 000a.f3cc.8206
ip address 10.10.15.254 255.255.255.0
!
interface  Vlan16
mac-address 000a.f3cc.8207
ip address 10.10.16.254 255.255.255.0
!
interface  Vlan17
mac-address 000a.f3cc.8208
ip address 10.10.17.254 255.255.255.0
!
interface  Vlan18
mac-address 000a.f3cc.8209
ip address 10.10.18.254 255.255.255.0
!
interface  Vlan19
mac-address 000a.f3cc.820a
ip address 10.10.19.254 255.255.255.0
!
interface  Vlan20
mac-address 000a.f3cc.820b
ip address 10.10.20.254 255.255.255.0
```

***Listing 3.4 :** Vérification de la configuration des interfaces des VLANs.*

d) Configuration du DHCP

Au lieu de configurer l'adresse IP manuellement sur chaque hôte connecté. Le DHCP nous permet de les attribuer directement via une configuration qui se fait sur le switch core.

Nous avons configuré le DHCP pour tous les VLANs. **Le listing 3.5** démontre la méthode pour activer ce protocole avec la configuration du DHCP pour le vlan 10. Après avoir appliqué la même méthode pour tous les autres VLANs, nous avons utilisé la commande **show running-config** pour vérifier leurs activations. **Le listing 3.6** révèle les résultats.

```
Score>en
Score#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Score(config)#ip dhcp pool vlan10
Score(dhcp-config)#network 10.10.10.0 255.255.255.0
Score(dhcp-config)#default-router 10.10.10.254
Score(dhcp-config)#exit
```

***Listing 3.5** : Configuration du DHCP*.

```
ip dhcp pool vlan10
network 10.10.10.0 255.255.255.0
default-router 10.10.10.254
ip dhcp pool vlan11
network 10.10.11.0 255.255.255.0
default-router 10.10.11.254
ip dhcp pool vlan12
network 10.10.12.0 255.255.255.0
default-router 10.10.12.254
ip dhcp pool vlan13
network 10.10.13.0 255.255.255.0
default-router 10.10.13.254
ip dhcp pool vlan14
network 10.10.14.0 255.255.255.0
default-router 10.10.14.254
ip dhcp pool vlan15
network 10.10.15.0 255.255.255.0
default-router 10.10.15.254
ip dhcp pool vlan16
network 10.10.16.0 255.255.255.0
default-router 10.10.16.254
ip dhcp pool vlan17
network 10.10.17.0 255.255.255.0
default-router 10.10.17.254
```

```
ip dhcp pool vlan18
network 10.10.18.0 255.255.255.0
default-router 10.10.18.254
ip dhcp pool vlan19
network 10.10.19.0 255.255.255.0
default-router 10.10.19.254
ip dhcp pool vlan20
network 10.10.20.0 255.255.255.0
default-router 10.10.20.254
```

***Listing 3.6** : Vérification de l'activation du DHCP.*

e) Configuration des liens Trunk

La configuration des liens Trunk permet de faire passer plusieurs flux venant de VLANs différents par un seul lien physique. Ici nous avons configuré tous liens vers les switch d'accès en mode Trunk à partir du switch Core**. Le listing 3.7** détaille cela.

Nous avons vérifié la configuration avec la commande **Show interface Trunk**. **Le listing 3.8** illustre le résultat.

```
Score(config)#interface fastEthernet 0/1
Score(config-if)#switchport trunk encapsulation dot1q
Score(config-if)#description TO_Switch1
Score(config-if)#description TO_Switch5
Score(config-if)#description TO_Switch9
Score(config-if)#description TO_Switch13
Score(config-if)#exit
Score(config)#interface fastEthernet 0/2
Score(config-if)#switchport trunk encapsulation dot1q
Score(config-if)#description TO_Switch2
Score(config-if)#description TO_Switch6
Score(config-if)#description TO_Switch10
Score(config-if)#description TO_Switch14
Score(config-if)#exit
Score(config)#interface fastEthernet 0/3
Score(config-if)#switchport trunk encapsulation dot1q
Score(config-if)#description TO_Switch3
Score(config-if)#description TO_Switch7
Score(config-if)#description TO_Switch11
Score(config-if)#description TO_Switch15
```

```
Score(config-if)#exit
Score(config)#interface fastEthernet 0/4
Score(config-if)#switchport trunk encapsulation dot1q
Score(config-if)#description TO_Switch4
Score(config-if)#description TO_Switch8
Score(config-if)#description TO_Switch12
Score(config-if)#description TO_Switch18
Score(config-if)#exit
```

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

```
Score#show interfaces trunk
Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q trunking 1
Fa0/2 on 802.1q trunking 1
Fa0/3 on 802.1q trunking 1
Fa0/4 on 802.1q trunking 1

Port Vlans allowed on trunk
Fa0/1 1-1005
Fa0/2 1-1005
Fa0/3 1-1005
Fa0/4 1-1005

Port Vlans allowed and active in management domain
Fa0/1 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/2 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/3 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/4 1,10,11,12,13,14,15,16,17,18,19,20

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/2 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/3 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/4 1,10,11,12,13,14,15,16,17,18,19,20
```

***Listing 3.8** : Vérification de la configuration des interfaces Trunk.*

f) Attribution des ports des commutateurs aux VLANs

L'opération consiste à attribuer un VLAN à chaque liaison physique reliée à un switch d'accès. Nous avons configuré toutes les interfaces des switches d'accès. **Le listing 3.9** représente la configuration des interfaces du Switch 1. Et démontre la méthode de configuration.

```
Switch1(config)#interface fastEthernet 0/3
```

```
Switch1(config-if)#switchport  mode access
Switch1(config-if)#switchport  access vlan 10
Switch1(config-if)#exit
Switch1(config)#interface  fastEthernet  0/4
Switch1(config-if)#switchport  mode access
Switch1(config-if)#switchport  access vlan 11
Switch1(config-if)#exit
```

***Listing 3.9** : Configuration des interfaces du switch Core en mode Accès.*

g) Configuration du protocole VTP

La configuration du protocole VTP sert à distribuer tous les VLANs à partir des commutateurs en mode serveur vers les commutateurs configurés en mode client de même domaine VTP.

Nous avons configuré le switch Core en mode serveur et les switches d'accès en mode client. **Le listing 3.10** représente la configuration du VTP server au niveau du switch cœur. **Le listing 3.11 représente** la configuration du Switch 1 en mode client.

Nous avons vérifié ces configurations avec la commande **Show vtp status**. **Le listing 3.12 et 3.13** illustrent le résultat.

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

***Listing 4.10**: Configuration du VTP server.*

```
Switch1(config)#vtp  mode client
Setting device to VTP CLIENT mode.
Switch1(config)#vtp  domain cev.com
Changing  VTP domain  name from NULL to cev.com
Switch1(config)#vtp  password cisco
Setting device  VLAN database password to cisco
```

***Listing 3.11** : Configuration du VTP client*

```
Score#show vtp status
VTP Version capable                 : 1 to 2
VTP version running                 : 1
VTP Domain Name                     : cev.com
VTP Pruning Mode                    : Disabled
VTP Traps Generation                : Disabled
Device ID                           : 0090.0C74.3300
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 10.10.10.254 on interface Vl10 (lowest numbered VLAN interface found)

Feature VLAN :
--------------
VTP Operating Mode                  : Server
Maximum VLANs supported locally     : 1005
Number of existing VLANs            : 16
Configuration Revision              : 264
MD5 digest                          : 0x14 0x5A 0x92 0xF9 0xA6 0x66 0x80 0x65
                                      0x49 0x7E 0xE4 0x43 0x8B 0x9B 0xBF0x9D
```

***Listing 3.12** : Vérification de la configuration du VTP server.*

```
Switch1#show vtp status
VTP Version capable                 : 1 to 2
VTP version running                 : 1
VTP Domain Name                     : cev.com
VTP Pruning Mode                    : Disabled
VTP Traps Generation                : Disabled
Device ID                           : 00D0.BC24.0900
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00


Feature VLAN :
--------------
VTP Operating Mode                  : Client
Maximum VLANs supported locally     : 255
Number of existing VLANs            : 16
Configuration Revision              : 264
MD5 digest                          : 0x14 0x5A 0x92 0xF9 0xA6 0x66 0x80 0x65
                                      0x49 0x7E 0xE4 0x43 0x8B 0x9B 0xBF 0x9D
```

***Listing 3.13**:Vérification de la configuration du VTP server.*

C. Vérification des adresses IP attribués par le DHCP

La figure 3.4 montre l'adresse IP attribuée par le DHCP au PC 4. La vérification se fera pour tous les PC.

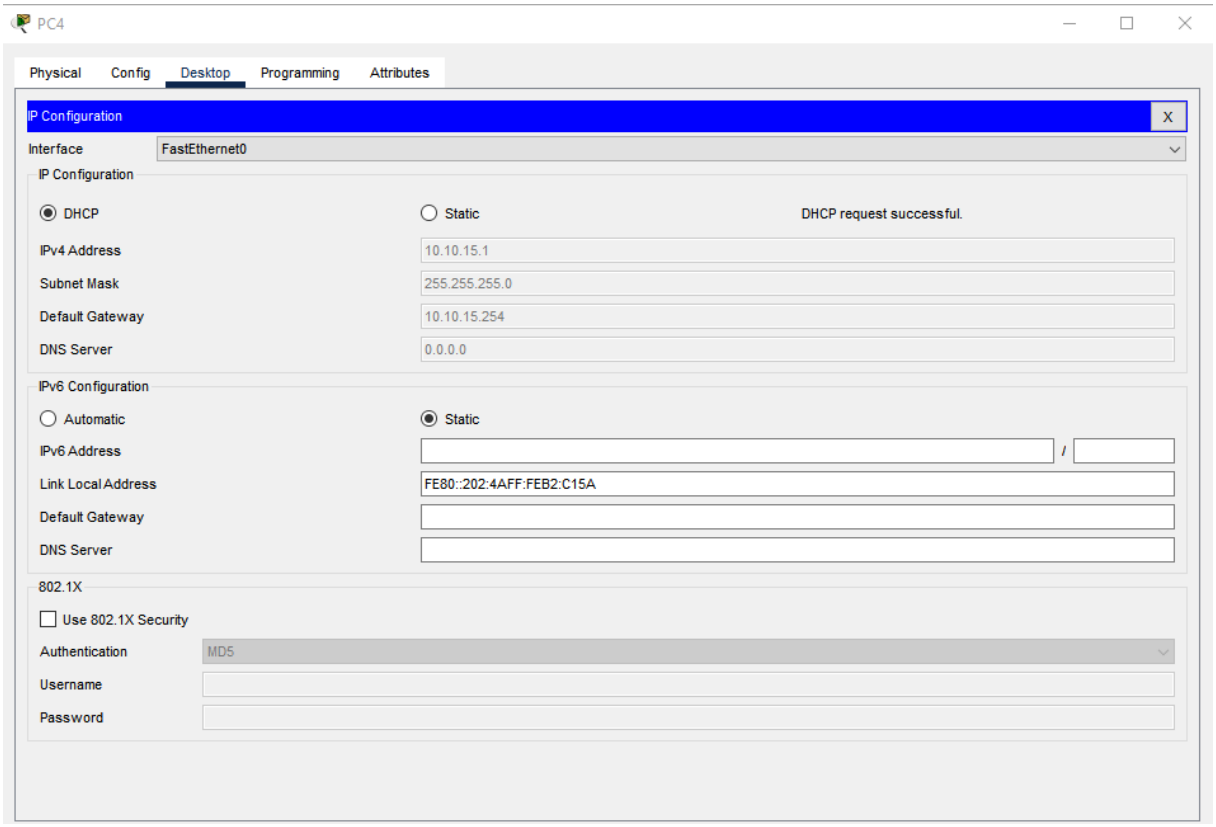

Figure 3.4: adresse IP attribuée automatiquement au PC 4.

D. Vérification de la connectivité

a) Test intra-VLANs

Nous avons vérifié la connectivité entre les PC qui appartiennent aux mêmes VLANs. Pour ce faire, nous avons effectué un Ping entre les adresses IP des PC appartenant aux mêmes VLANs.

Par exemple **la figure 3.5** représente le résultat du Ping entre l'adresse IP du PC 21 qui est : 10.10.12.2 et l'adresse IP du PC 29 qui est : 10.10.12.3.

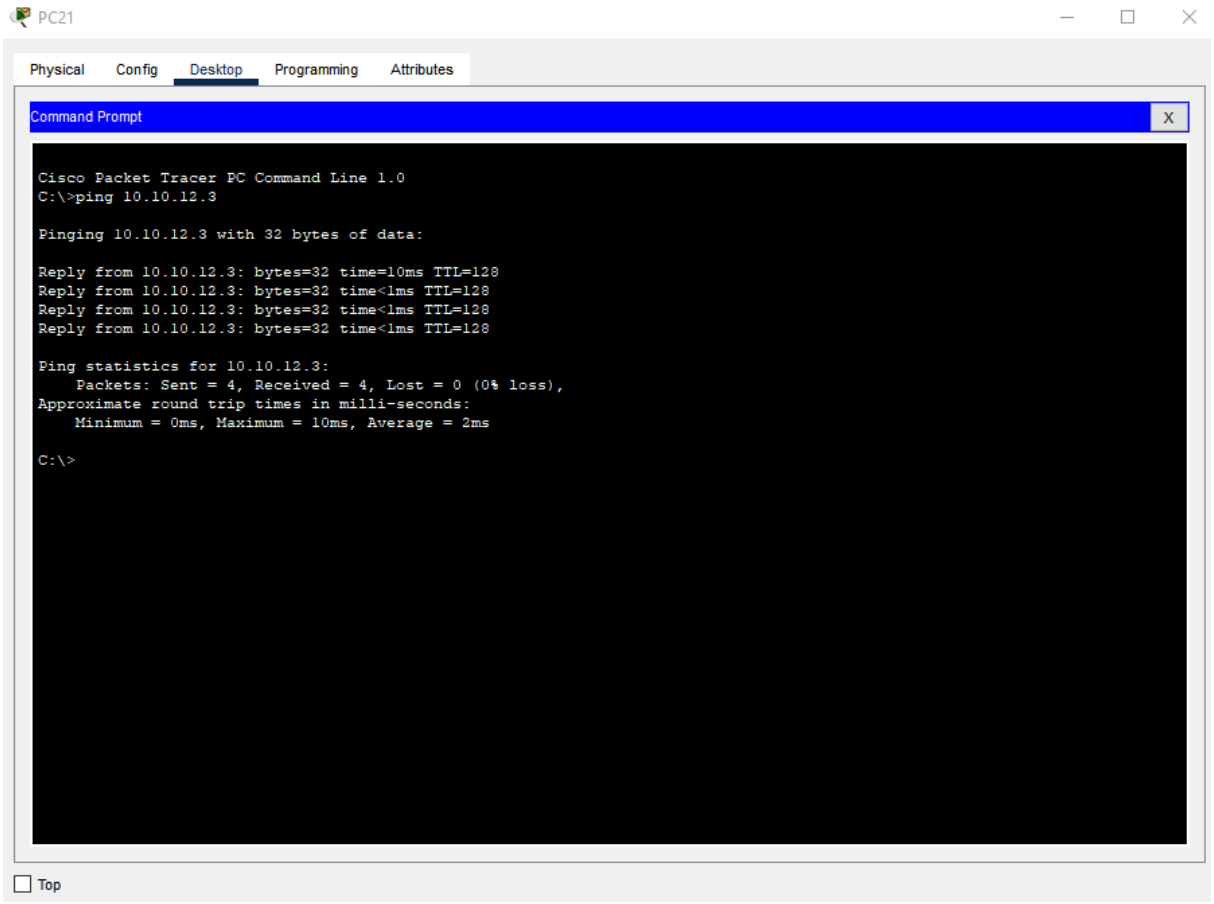

Figure 3.5: Test entre le PC 21 et le PC 29.

b) Test inter-VLANs

Nous avons vérifié la connectivité entre les PC qui appartiennent à des VLANs différents. Pour ce faire, nous avons effectué un Ping entre les adresses IP des PC appartenant à des VLANs différents.

Par exemple **la figure 3.6** représente le résultat du Ping entre l'adresse IP du PC 4 qui est : 10.10.15.1 et l'adresse IP du PC 13 qui est : 10.10.18.1.

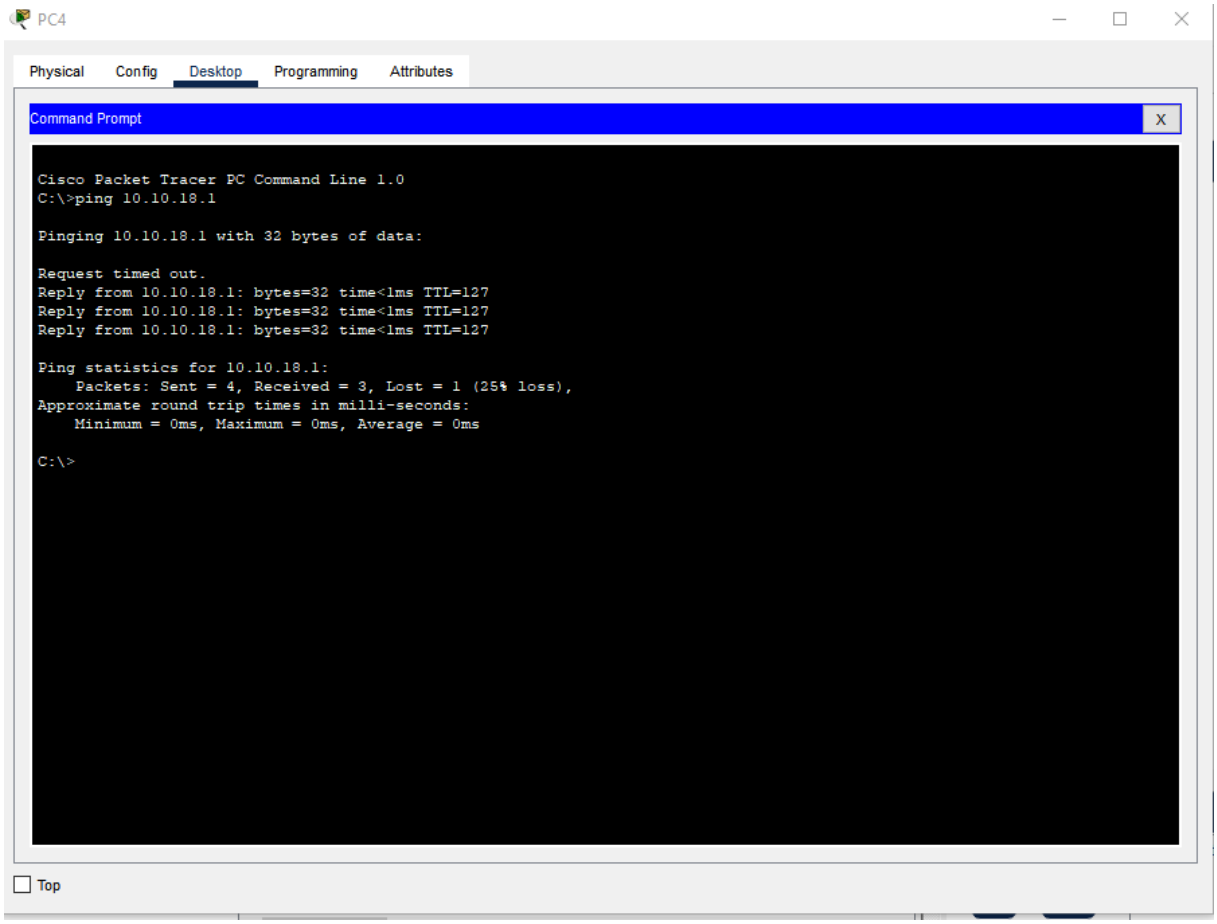

Figure 3.6 : Test de connectivité entre le PC 4 et le PC 13.

E. Déduction

Malgré le fait que cette topologie permette une connectivité intra et extra Vlan, elle ne permet pas une connectivité avec un site distant. Encore la solidité de cette configuration repose sur un seul et unique Switch Core ce qui implique qu'elle est très facilement exposée aux pannes ce qui induit un ralentissement ou un arrêt de l'activité, affectant ainsi le bon fonctionnement de l'équipe et sa productivité. C'est pour cela que dans la deuxième partie qui va suivre, nous allons proposer une nouvelle configuration du réseau Cevital, qui répondra à toutes les problématiques du réseau existant.

3.5. Partie 2 : Nouvelle architecture proposée au réseau CEVITAL

La partie 2 aura pour but d'exposer la nouvelle architecture proposée au réseau CEVITAL.

A. Architecture mise en œuvre

Nous avons configuré la nouvelle architecture proposée au réseau CEVITAL sur le simulateur CISCO Packet tracer 8.1.0. La topologie est représentée ci-dessous

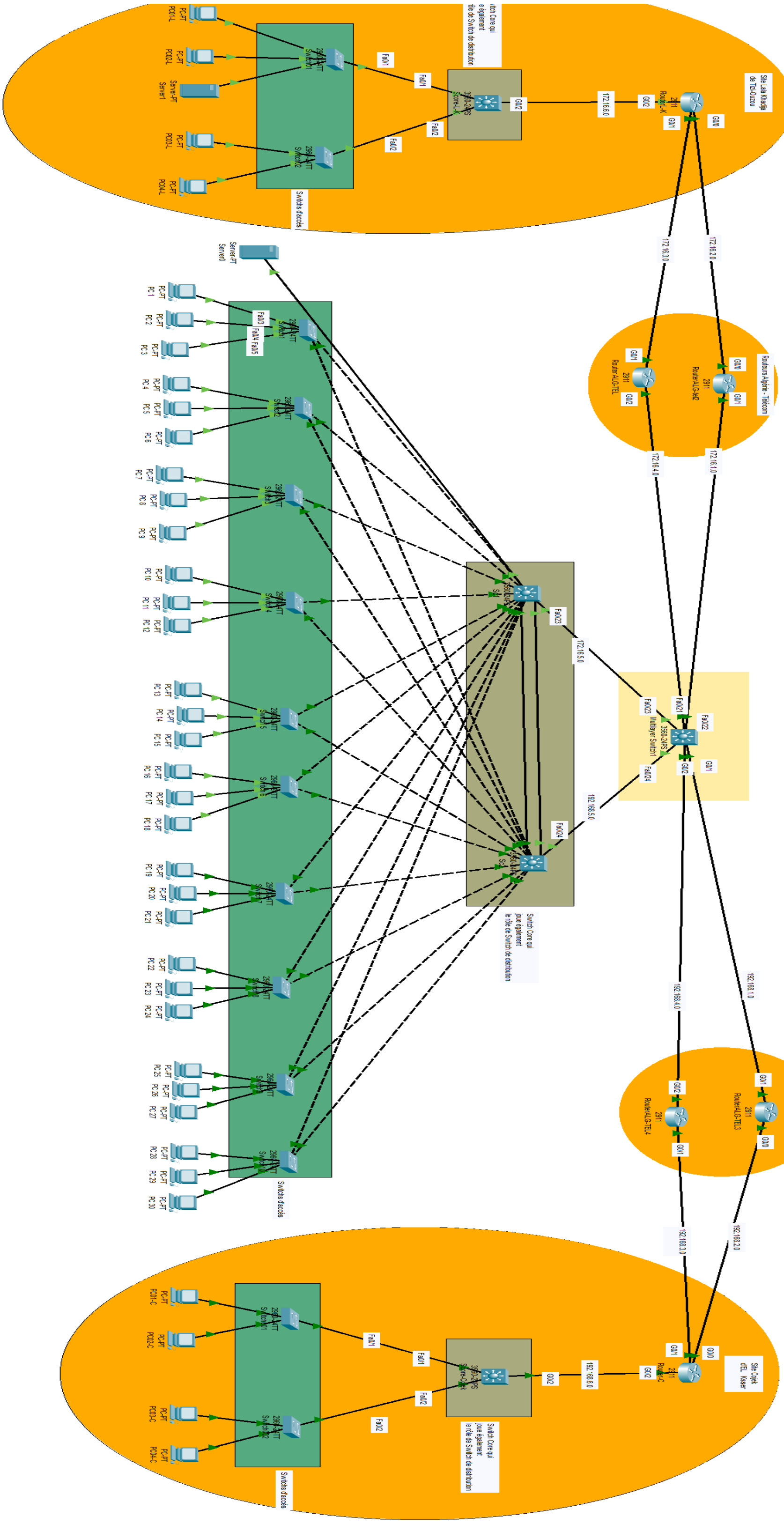

Figure 3.7 : Architecture proposée au réseau Cevital.

B. Configuration des équipements du réseau proposé

Dans la nouvelle topologie présentée, nous avons utilisé 2 switches de niveau 3 interconnectés entre eux. Ils ont le rôle de switches Core et de switches de distribution pour le site central de Cevital. Nous avons rajoutés dix (10) switches d'accès de niveau 2, une trentaine de PCs, ainsi qu'un serveur.

Nous avons également mis en places deux (2) réseaux appartenant à deux sites distants (site Cojek d'EL Kser et le site Lala Khadija de Tizi-Ouzou). Dans chacun d'entre eux, il y'a un switch Core de niveau 3, 2 switches d'accès de niveau 2, ainsi que des PCs.

Pour interconnecter le site central aux sites distants nous avons utilisé un switch de niveau 3 qui agira comme un routeur, ainsi que six (6) autres routeurs, dont quatre (4) appartiennent à Algérie Télécom.

a) Configuration des Hostname et sécurité

Comme dans la première partie nous avons sécurisé les switches de niveau 3 ainsi que les routeurs. **Le listing 3.14** représente la configuration du premier switch Core, que nous avons renommé « Score1 », et que nous avons sécurisé avec le mot de passe « CEVITAL ».

```
Switch >en
Switch #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch (config) #enable password CEVITAL
Switch (config) #service password-encryption
Switch (config) #hostname Score1
Score1 (config) #exit
Score1 #
```

Listing 3.14 : Configuration des noms hôtes et mot de passe.

b) Création des VLANs

La création des VLANs se fait au niveau des switchs Core de chaque site. **Le listing 3.15 et 3.16** représente la création du vlan 10 (DRH) au niveau du switch « Score1 » du site central, et des VLANs 30 (DRH) au niveau des sites distants.

Après avoir créé tous les VLANs, nous avons vérifié leur création « **listing 3.17** » « **listing 3.18** » avec la commande **show vlan brief.**

```
Score1 (config) #vlan 10
Score1 (config-vlan) #name DRH
Score1 (config-vlan) #vlan 11
Score1 (config-vlan) #name achat
Score1 (config-vlan) exit
```

Listing 3.15 : *Création des VLANs du site central.*

```
Score-Cojek (config) #vlan 30
Score-Cojek (config-vlan) #name DRH
Score-Cojek (config-vlan) #vlan 40
Score-Cojek (config-vlan) #name achat
Score-Cojek (config-vlan) #exit
```

```
Score-L-K (config) #vlan 30
Score-L-K (config-vlan) #name DRH
Score-L-K (config-vlan) #vlan 40
Score-L-K (config-vlan) #name achat
Score-L-K (config-vlan) #exit
```

Listing 3.16 : *Création des VLANs des sites distants.*

```
10    DRH           active
11    achat         active
12    IT            active
13    RFreduction   active
14    RFsucre       active
15    DEE           active
16    DFC           active
17    commercial    active
18    imprimente    active
19    DG            active
20    server        active
```

Listing 3.17 : *Vérification de la création des VLANs les sites de Central.*

```
30          DRH             active
40          achat           active
50          IT              active
60          RFreduction     active
70          RFsucre         active
80          DEE             active
90          DFC             active
100         commercial      active
110         imprimente      active
120         DG              active
130         server          active
```

Listing 3.18 : *Vérification de la création des VLANs des sites distants de CEVITAL.*

c) Configuration des interfaces VLANs

Comme dans la première partie, nous avons configuré les interfaces des VLANs précédemment créés. Ceci permettra le routage inter-VLAN. Nous avons activé ce routage avec la commande **IP routing.**

Sur le site central, les adresses des interfaces virtuelles des 2 switches Core, auront la particularité d'avoir le 252 sur la partie machine de chaque VLAN du « Score1 ». Le 253 lui sera sur la partie machine de chaque VLAN du « Score2 ».

Le listing 3.19 démontre la méthode avec la configuration des interfaces avec la configuration du VLAN 10 sur Score1.

Le listing 3.20 représente la configuration de l'interface du VLAN 10 sur Score2.

Le listing 3.21 représente la vérification de la configuration des interfaces VLANs sur les switchs Score1 et Score2.

Le listing 3.22 représente la configuration des interfaces des VLANs 30 au niveau des switchs Core des sites lala Khadija « Score-L-K » et Cojek « Score-Cojek ».

Le listing 3.23 représente la vérification de la configuration des interfaces VLANs sur les switchs Core des sites lala Khadija « Score-L-K » et Cojek « Score-Cojek ».

```
Score1 #config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Score1 (config)#interface vlan 10
```

```
Score1 (config-if)#ip  address 10.10.10.252 255.255.255.0
Score1 (config-if)#exit
```

Listing 3.19 : *Configuration de l'interfaces du VLAN 10 sur Score1.*

```
Score2 #config  terminal
Enter configuration commands, one per line. End with CNTL/Z.
Score2 (config)#interface  vlan  10
Score2 (config-if)#ip  address 10.10.10.253 255.255.255.0
Score2 (config-if)#exit
```

Listing 3.20 : *Configuration de l'interfaces du VLAN 10 sur Score2.*

Score1

```
interface  Vlan10
mac-address 0003.e42d.2602
ip address 10.10.10.252 255.255.255.0
!
interface  Vlan11
mac-address 0003.e42d.2603
ip address 10.10.11.252 255.255.255.0
!
interface  Vlan12
mac-address 0003.e42d.2604
ip address 10.10.12.252 255.255.255.0
!
interface  Vlan13
mac-address 0003.e42d.2605
ip address 10.10.13.252 255.255.255.0
!
interface  Vlan14
mac-address 0003.e42d.2606
ip address 10.10.14.252 255.255.255.0
!
interface  Vlan15
mac-address 0003.e42d.2607
ip address 10.10.15.252 255.255.255.0
!
interface  Vlan16
mac-address 0003.e42d.2608
ip address 10.10.16.252 255.255.255.0
!
interface  Vlan17
mac-address 0003.e42d.2609
ip address 10.10.17.252 255.255.255.0
!
```

Score2

```
interface  Vlan10
mac-address 000b.be69.8201
ip address 10.10.10.253 255.255.255.0
!
interface  Vlan11
mac-address 000b.be69.8202
ip address 10.10.11.253 255.255.255.0
!
interface  Vlan12
mac-address 000b.be69.8203
ip address 10.10.12.253 255.255.255.0
!
interface  Vlan13
mac-address 000b.be69.8204
ip address 10.10.13.253 255.255.255.0
!
interface  Vlan14
mac-address 000b.be69.8205
ip address 10.10.14.253 255.255.255.0
!
interface  Vlan15
mac-address 000b.be69.8206
ip address 10.10.15.253 255.255.255.0
!
interface  Vlan16
mac-address 000b.be69.8207
ip address 10.10.16.253 255.255.255.0
!
interface  Vlan17
mac-address 000b.be69.8208
ip address 10.10.17.253 255.255.255.0
!
```

```
interface  Vlan18
mac-address 0003.e42d.260a
ip address 10.10.18.252 255.255.255.0
!
interface  Vlan19
mac-address 0003.e42d.260b
ip address 10.10.19.252 255.255.255.0
interface  Vlan20
mac-address 0003.e42d.260c
ip address 10.10.20.252 255.255.255.0
```

```
interface  Vlan18
mac-address 000b.be69.8209
ip address 10.10.18.253 255.255.255.0
!
interface  Vlan19
mac-address 000b.be69.820a
ip address 10.10.19.253 255.255.255.0
interface  Vlan20
mac-address 000b.be69.820b
ip address 10.10.20.253 255.255.255.0
```

Listing 3.21 : *Vérification de la configuration des interfaces VLANs sur Score1 et Score2.*

```
Score-Cojek (config)#interface  vlan  30
Score-Cojek (config-if)#ip  address
      10.30.30.254 255.255.255.0
Score-Cojek (config-if)#exit
```

```
Score-L-K (config)#interface  vlan  30
Score-L-K (config-if)#ip  address
  10.20.20.254 255.255.255.0
Score-L-K (config-if)#exit
```

Listing 3.22 : *Configuration des interfaces VLANs sur Score-L-K et Score-Cojek.*

Score-L-K

```
interface  Vlan30
mac-address 000c.8550.0b02
ip address 10.20.30.254 255.255.255.0
!
interface  Vlan40
mac-address 000c.8550.0b03
ip address 10.20.40.254 255.255.255.0
!
interface  Vlan50
mac-address 000c.8550.0b04
ip address 10.20.50.254 255.255.255.0
!
interface  Vlan60
mac-address 000c.8550.0b05
ip address 10.20.60.254 255.255.255.0
!
interface  Vlan70
mac-address 000c.8550.0b06
ip address 10.20.70.254 255.255.255.0
!
interface  Vlan80
mac-address 000c.8550.0b07
ip address 10.20.80.254 255.255.255.0
!
interface  Vlan90
```

Score-Cojek

```
interface  Vlan30
mac-address 0002.17ae.0c01
ip address 10.30.30.254 255.255.255.0
!
interface  Vlan40
mac-address 0002.17ae.0c02
ip address 10.30.40.254 255.255.255.0
!
interface  Vlan50
mac-address 0002.17ae.0c04
ip address 10.30.50.254 255.255.255.0
!
interface  Vlan60
mac-address 0002.17ae.0c05
ip address 10.30.60.254 255.255.255.0
!
interface  Vlan70
mac-address 0002.17ae.0c06
ip address 10.30.70.254 255.255.255.0
!
interface  Vlan80
mac-address 0002.17ae.0c07
ip address 10.30.80.254 255.255.255.0
!
interface  Vlan90
```

```
mac-address 000c.8550.0b08
ip address 10.20.90.254 255.255.255.0
!
interface  Vlan100
mac-address 000c.8550.0b09
ip address 10.20.100.254 255.255.255.0
!
interface  Vlan110
mac-address 000c.8550.0b0a
ip address 10.20.110.254 255.255.255.0

interface  Vlan120
mac-address 000c.8550.0b0b
ip address 10.20.120.254 255.255.255.0
!
interface  Vlan130
mac-address 000c.8550.0b0c
ip address 10.20.130.254 255.255.255.0
```

```
mac-address 0002.17ae.0c08
ip address 10.30.90.254 255.255.255.0
!
interface  Vlan100
mac-address 0002.17ae.0c09
ip address 10.30.100.254 255.255.255.0
!
interface  Vlan110
mac-address 0002.17ae.0c0a
ip address 10.30.110.254 255.255.255.0

interface  Vlan120
mac-address 0002.17ae.0c0b
ip address 10.30.120.254 255.255.255.0
!
interface  Vlan130
mac-address 0002.17ae.0c0c
ip address 10.30.130.254 255.255.255.0
```

Listing 3.23 : *Vérification de la configuration des interfaces VLANs sur Score-L-K et Score-Cojek.*

d) Configuration du DHCP

Nous avons créé un pool d'adresse pour chaque VLAN. L'opération s'effectue au niveau des switches Core (distributions), puis nous avons défini la passerelle par défaut du sous-réseau.

```
Score1 #config  terminal
Enter configuration commands, one per line. End with CNTL/Z.
Score1 (config)  #ip dhcp pool vlan10
Score1 (dhcp-config)  #network  10.10.10.0 255.255.255.0
Score (dhcp-config)  #default-router  10.10.10.254
Score (dhcp-config)  #exit
```

Listing 3.24 : *configuration du DHCP sur Score1.*

```
Score2 #config  terminal
Enter configuration commands, one per line. End with CNTL/Z.
Score2 (config)  #ip dhcp pool vlan10
Score2 (dhcp-config)  #network  10.10.10.0 255.255.255.0
Score2 (dhcp-config)  #default-router  10.10.10.254
Score2 (dhcp-config)  #exit
```

Listing 3.25 : *configuration du DHCP sur Score2.*

```
Score-L-K #config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Score-L-K (config) #ip dhcp pool vlan30
Score-L-K (dhcp-config) #network 10.20.30.0 255.255.255.0
Score-L-K (dhcp-config) #default-router 10.20.30.254
Score-L-K (dhcp-config) #exit
```

Listing 3.26: *configuration du DHCP sur Score-L-K.*

```
Score-Cojek #config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Score-Cojek (config) #ip dhcp pool vlan30
Score-Cojek (dhcp-config) #network 10.30.30.0 255.255.255.0
Score-Cojek (dhcp-config) #default-router 10.30.30.254
Score-Cojek (dhcp-config) #exit
```

Listing 3.27: *configuration du DHCP sur Score-Cojek.*

Score1

```
ip dhcp pool vlan10
network 10.10.10.0 255.255.255.0
default-router 10.10.10.254
ip dhcp pool vlan11
network 10.10.11.0 255.255.255.0
default-router 10.10.11.254
ip dhcp pool vlan12
network 10.10.12.0 255.255.255.0
default-router 10.10.12.254
ip dhcp pool vlan13
network 10.10.13.0 255.255.255.0
default-router 10.10.13.254
ip dhcp pool vlan14
network 10.10.14.0 255.255.255.0
default-router 10.10.14.254
ip dhcp pool vlan15
network 10.10.15.0 255.255.255.0
default-router 10.10.15.254
ip dhcp pool vlan16
network 10.10.16.0 255.255.255.0
default-router 10.10.16.254
ip dhcp pool vlan17
network 10.10.17.0 255.255.255.0
default-router 10.10.17.254
ip dhcp pool vlan18
network 10.10.18.0 255.255.255.0
default-router 10.10.18.254
ip dhcp pool vlan19
```

Score2

```
ip dhcp pool vlan10
network 10.10.10.0 255.255.255.0
default-router 10.10.10.254
ip dhcp pool vlan11
network 10.10.11.0 255.255.255.0
default-router 10.10.11.254
ip dhcp pool vlan12
network 10.10.12.0 255.255.255.0
default-router 10.10.12.254
ip dhcp pool vlan13
network 10.10.13.0 255.255.255.0
default-router 10.10.13.254
ip dhcp pool vlan14
network 10.10.14.0 255.255.255.0
default-router 10.10.14.254
ip dhcp pool vlan15
network 10.10.15.0 255.255.255.0
default-router 10.10.15.254
ip dhcp pool vlan16
network 10.10.16.0 255.255.255.0
default-router 10.10.16.254
ip dhcp pool vlan17
network 10.10.17.0 255.255.255.0
default-router 10.10.17.254
ip dhcp pool vlan18
network 10.10.18.0 255.255.255.0
default-router 10.10.18.254
ip dhcp pool vlan19
```

```
network 10.10.19.0 255.255.255.0
default-router 10.10.19.254
ip dhcp pool vlan20
network 10.10.20.0 255.255.255.0
default-router 10.10.20.254
```

```
network 10.10.19.0 255.255.255.0
default-router 10.10.19.254
ip dhcp pool vlan20
network 10.10.20.0 255.255.255.0
default-router 10.10.20.254
```

Listing 3.28: *Vérification de la création des pools DHCP sur Score1 et Score2.*

Score-L-K

```
ip dhcp pool vlan30
network 10.20.30.0 255.255.255.0
default-router 10.20.30.254
ip dhcp pool vlan40
network 10.20.40.0 255.255.255.0
default-router 10.20.40.254
ip dhcp pool vlan50
network 10.20.50.0 255.255.255.0
default-router 10.20.50.254
ip dhcp pool vlan60
network 10.20.60.0 255.255.255.0
default-router 10.20.60.254
ip dhcp pool vlan70
network 10.20.70.0 255.255.255.0
default-router 10.20.70.254
ip dhcp pool vlan80
network 10.20.80.0 255.255.255.0
default-router 10.20.80.254
ip dhcp pool vlan90
network 10.20.90.0 255.255.255.0
default-router 10.20.90.254
ip dhcp pool vlan100
network 10.20.100.0 255.255.255.0
default-router 10.20.100.254
ip dhcp pool vlan110
network 10.20.110.0 255.255.255.0
default-router 10.20.110.254
ip dhcp pool vlan120
network 10.20.120.0 255.255.255.0
default-router 10.20.120.254
ip dhcp pool vlan130
network 10.20.130.0 255.255.255.0
default-router 10.20.130.254
!
```

Score-Cojek

```
ip dhcp pool vlan30
network 10.30.30.0 255.255.255.0
default-router 10.30.30.254
ip dhcp pool vlan40
network 10.30.40.0 255.255.255.0
default-router 10.30.40.254
ip dhcp pool vlan50
network 10.30.50.0 255.255.255.0
default-router 10.30.50.254
ip dhcp pool vlan60
network 10.30.60.0 255.255.255.0
default-router 10.30.60.254
ip dhcp pool vlan70
network 10.30.70.0 255.255.255.0
default-router 10.30.70.254
ip dhcp pool vlan80
network 10.30.80.0 255.255.255.0
default-router 10.30.80.254
ip dhcp pool vlan90
network 10.30.90.0 255.255.255.0
default-router 10.30.90.254
ip dhcp pool vlan100
network 10.30.100.0 255.255.255.0
default-router 10.30.100.254
ip dhcp pool vlan110
network 10.30.110.0 255.255.255.0
default-router 10.30.110.254
ip dhcp pool vlan120
network 10.30.120.0 255.255.255.0
default-router 10.30.120.254
ip dhcp pool vlan130
network 10.30.130.0 255.255.255.0
default-router 10.30.130.254
!
```

Listing 3.29: *Vérification de la création des pools DHCP sur Score-L-K et Score-Cojek.*

Pour un meilleur succès de ce protocole, nous avons exclu les adresses de 128 à 253 sur Score1, ce qui voudra dire que le Score1 va attribuer les adresses de 1 à 127. Les adresses de 1 à 127 sont quant à elles exclues sur Score2, ce qui voudra dire que le Score2 va attribuer les adresses de 128 à 253. Cette opération a pour but d'éviter les conflits au moment de l'attribution des adresses.

```
Score1 (config)  #ip dhcp excluded-address  10.10.10.128 10.10.10.253
Score1 (config)  #ip dhcp excluded-address  10.10.11.128 10.10.11.253
Score1 (config)  #ip dhcp excluded-address  10.10.12.128 10.10.12.253
```

***Listing 3.30** : Configuration des adresses exclus sur Score1.*

```
Score2 (config)  #ip dhcp excluded-address  10.10.10.1 10.10.10.127
Score2 (config)  #ip dhcp excluded-address  10.10.11.1 10.10.11. 127
Score2 (config)  #ip dhcp excluded-address  10.10.12.1 10.10.12. 127
```

***Listing 3.31** : Configuration des adresses exclus sur Score2.*

```
ip dhcp excluded-address  10.10.10.128 10.10.10.253
ip dhcp excluded-address  10.10.11.128 10.10.11.253
ip dhcp excluded-address  10.10.12.128 10.10.12.253
ip dhcp excluded-address  10.10.13.128 10.10.13.253
ip dhcp excluded-address  10.10.14.128 10.10.14.253
ip dhcp excluded-address  10.10.15.128 10.10.15.253
ip dhcp excluded-address  10.10.16.128 10.10.16.253
ip dhcp excluded-address  10.10.17.128 10.10.17.253
ip dhcp excluded-address  10.10.18.128 10.10.18.253
ip dhcp excluded-address  10.10.19.128 10.10.19.253
ip dhcp excluded-address  10.10.20.128 10.10.20.253
!
```

***Listing 3.32 :** Vérifications des adresses exclus sur Score1.*

```
ip dhcp excluded-address  10.10.10.1 10.10.10.127
ip dhcp excluded-address  10.10.11.1 10.10.11.127
ip dhcp excluded-address  10.10.12.1 10.10.12.127
ip dhcp excluded-address  10.10.13.1 10.10.13.127
ip dhcp excluded-address  10.10.14.1 10.10.14.127
ip dhcp excluded-address  10.10.15.1 10.10.15.127
ip dhcp excluded-address  10.10.16.1 10.10.16.127
ip dhcp excluded-address  10.10.17.1 10.10.17.127
ip dhcp excluded-address  10.10.18.1 10.10.18.127
ip dhcp excluded-address  10.10.19.1 10.10.19.127
ip dhcp excluded-address  10.10.20.1 10.10.20.127
!
```

***Listing 3.33 :** Vérifications des adresses exclus sur Score2.*

e) Configuration des liens Trunk

Nous avons configuré tous les liens vers les switches d'accès en mode Trunk à partir des switchs Core**. Le Listing 3.34** démontre comment configurer, avec un exemple de la configuration des liens liés au Score1. **Le Listing 3.35** illustre tous les liens configurés sur Score1. **Le Listing 3.36** illustre quant à elle, les liens configurés sur Score-L-K et Score-Cojek.

```
Score1 (config) #interface fastEthernet 0/1
Score1 (config-if) #switchport trunk encapsulation dot1q
Score1 (config-if) #exit
Score1 (config) #interface fastEthernet 0/2
Score1 (config-if) #switchport trunk encapsulation dot1q
Score1 (config-if) #exit
Score1 (config) #interface fastEthernet 0/3
Score1 (config-if) #switchport trunk encapsulation dot1q
Score1 (config-if) #exit
```

Listing 3.34: *Configuration des liens Trunk sur Score1.*

```
Score1#show interfaces trunk
Port Mode Encapsulation Status Native vlan
Po1 on 802.1q trunking 1
Fa0/1 on 802.1q trunking 1
Fa0/2 on 802.1q trunking 1
Fa0/3 on 802.1q trunking 1
Fa0/4 on 802.1q trunking 1
Fa0/5 on 802.1q trunking 1
Fa0/6 on 802.1q trunking 1
Fa0/9 on 802.1q trunking 1
Fa0/10 on 802.1q trunking 1
Fa0/11 on 802.1q trunking 1
Fa0/12 on 802.1q trunking 1

Port Vlans allowed on trunk
Po1 1-1005
Fa0/1 1-1005
Fa0/2 1-1005
Fa0/3 1-1005
Fa0/4 1-1005
Fa0/5 1-1005
Fa0/6 1-1005
Fa0/9 1-1005
Fa0/10 1-1005
Fa0/11 1-1005
Fa0/12 1-1005
```

```
Port Vlans allowed and active in management domain
Po1 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/1 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/2 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/3 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/4 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/5 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/6 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/9 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/10 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/11 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/12 1,10,11,12,13,14,15,16,17,18,19,20

Port Vlans in spanning tree forwarding state and not pruned
Po1 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/1 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/2 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/3 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/4 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/5 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/6 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/9 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/10 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/11 1,10,11,12,13,14,15,16,17,18,19,20
Fa0/12 1,10,11,12,13,14,15,16,17,18,19,20
```

Listing 3.35 : *Vérification de la configuration des interfaces Trunk sur Score1.*

```
Score-L-K#show interfaces trunk
Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q trunking 1
Fa0/2 on 802.1q trunking 1

Port Vlans allowed on trunk
Fa0/1 1-1005
Fa0/2 1-1005

Port Vlans allowed and active in management domain
Fa0/1
1,30,40,50,60,70,80,90,100,110,120,130
Fa0/2
1,30,40,50,60,70,80,90,100,110,120,130

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1
1,30,40,50,60,70,80,90,100,110,120,130
```

```
Score-Cojek#show interfaces trunk
Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q trunking 1
Fa0/2 on 802.1q trunking 1

Port Vlans allowed on trunk
Fa0/1 1-1005
Fa0/2 1-1005

Port Vlans allowed and active in management domain
Fa0/1
1,30,40,50,60,70,80,90,100,110,120,130
Fa0/2
1,30,40,50,60,70,80,90,100,110,120,130

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1
1,30,40,50,60,70,80,90,100,110,120,130
```

Fa0/2 1,30,40,50,60,70,80,90,100,110,120,130	Fa0/2 1,30,40,50,60,70,80,90,100,110,120,130

***Listing 3.36** : Vérifications des liens Trunk sur Score-L-K et Score-Cojek.*

f) Attribution des ports des commutateurs aux VLANs

Nous avons configuré les interfaces de tous les switches d'accès du site central et des sites distants en mode Access.

Le Listing 3.37 représente la configuration des interfaces du premier switch d'accès au niveau du site central. Et illustre la méthode de configuration utilisée dans tous les autres switches.

```
Saccess1 (config) #interface fastEthernet 0/3
Saccess1 (config-if) #switchport mode acces
Saccess1 (config-if) #switchport acces vlan 10
Saccess1 (config-if) #exit
Saccess1 (config) #interface fastEthernet 0/4
Saccess1 (config-if) #switchport mode acces
Saccess1 (config-if) #switchport acces vlan 11
Saccess1 (config-if) #exit
```

***Listing 3.37 :** Configuration des interfaces du switch en mode Access.*

g) Configuration du protocole VTP

La configuration du protocole VTP en mode server a été configurée au niveau de switch Score1, ainsi qu'au niveau des switches Core des autres sites distants. Le mode client a lui été configuré au niveau des switches restants, afin d'accueillir les VLANs distribués à partir des switches en mode serveur.

Le Listing 3.38 représente la configuration du VTP server niveau du Score1, et illustre la méthode de configuration adoptée sur les switchs Core des sites distants.

Le listing 3.39 représente la configuration du « Saccess1 » en mode client, et illustre la méthode de configuration adoptée au niveau des switches.

Nous avons vérifié les configurations VTP serveur et client sur le site central, ainsi que sur les sites distants avec la commande **Show vtp status**. **Les listings 3.40, 3.41, 3.42, 3.43, 3.44, 3.45** illustrent les résultats.

```
Score1 (config) #vtp mode server
Device mode already VTP SERVER.
Score1 (config) #vtp domain cev.com
Changing VTP domain name from NULL to cev.com
Score1 (config) #vtp password cisco
Setting device VLAN database password to cisco
Score1 (config) #exit
```

***Listing 3.38**: Configuration du VTP server niveau du Score1.*

```
Saccess1 (config)#vtp mode client
Setting device to VTP CLIENT mode.
Saccess1 (config)#vtp domain cev.com
Changing VTP domain name from NULL to cev.com
Saccess1 (config)#vtp password cisco
Setting device VLAN database password to cisco
```

***Listing 3.39** : Configuration du VTP client au niveau du Sacces1.*

```
Score1#show vtp status
VTP Version capable                    : 1 to 2
VTP version running                    : 1
VTP Domain Name                        : cev.com
VTP Pruning Mode                       : Disabled
VTP Traps Generation                   : Disabled
Device ID                              : 00D0.58E3.C500
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 10.10.10.252 on interface Vl10 (lowest numbered VLAN interface found)

Feature VLAN :
--------------
VTP Operating Mode                     : Server
Maximum VLANs supported locally        : 1005
Number of existing VLANs               : 16
Configuration Revision                 : 510
MD5 digest                             : 0x58 0x4C 0x6A 0xBC 0x47 0x5E 0x65 0x2A
                                         0x55 0xC7 0x5D 0xB2 0xED 0x7C 0xC4 0xEE
```

***Listing 3.40 :** Vérification de la configuration du VTP server au niveau du site central.*

```
Saccess1# show vtp status
VTP Version capable                    : 1 to 2
VTP version running                    : 1
VTP Domain Name                        : cev.com
VTP Pruning Mode                       : Disabled
VTP Traps Generation                   : Disabled
Device ID                              : 0000.0CE3.5D00
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00

Feature VLAN :
--------------
VTP Operating Mode                     : Client
Maximum VLANs supported locally        : 255
Number of existing VLANs               : 16
Configuration Revision                 : 510
MD5 digest                             : 0x58 0x4C 0x6A 0xBC 0x47 0x5E 0x65 0x2A
                                         0x55 0xC7 0x5D 0xB2 0xED 0x7C 0xC4 0xEE
```

Listing 3.41 : *Vérification de la configuration du VTP client au niveau du site central.*

```
core-L-K #show vtp status
VTP Version capable                    : 1 to 2
VTP version running                    : 1
VTP Domain Name                        : cev.com
VTP Pruning Mode                       : Disabled
VTP Traps Generation                   : Disabled
Device ID                              : 0006.2A1C.6C00
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 10.20.30.254 on interface Vl30 (lowest numbered VLAN interface found)

Feature VLAN :
--------------
VTP Operating Mode                     : Server
Maximum VLANs supported locally        : 1005
Number of existing VLANs               : 16
Configuration Revision                 : 198
MD5 digest                             : 0xF1 0x32 0x6C 0x2A 0x00 0xE6 0x51 0xFB
                                         0x6E 0xA4 0x0A 0x80 0x71 0xCC 0x2C 0x24
```

Listing 3.42 : *Vérification de la configuration du VTP server au niveau du site Lala Khadija.*

```
Score-Cojek #show vtp st
Score-Cojek #show vtp status
VTP Version capable                    : 1 to 2
VTP version running                    : 1
VTP Domain Name                        : cev.com
VTP Pruning Mode                       : Disabled
VTP Traps Generation                   : Disabled
```

```
Device ID                                   : 0001.4395.3200
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 10.30.30.254 on interface Vl30 (lowest numbered VLAN interface found)

Feature VLAN :
--------------
VTP Operating Mode                  : Server
Maximum VLANs supported locally     : 1005
Number of existing VLANs            : 16
Configuration Revision              : 154
MD5 digest                          : 0xEB 0x7A 0xE3 0x4C 0x10 0xF6 0xD9 0x3A
                                      0x59 0xC4 0xAF 0x88 0x7B 0xD8 0x36 0x58
```

Listing 3.43 : *Vérification de la configuration du VTP server au niveau du site Cojek.*

```
Switch01#show vtp status
VTP Version capable                 : 1 to 2
VTP version running                 : 1
VTP Domain Name                     : cev.com
VTP Pruning Mode                    : Disabled
VTP Traps Generation                : Disabled
Device ID                           : 000C.CFD8.5A00
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00

Feature VLAN :
--------------
VTP Operating Mode                  : Client
Maximum VLANs supported locally     : 255
Number of existing VLANs            : 16
Configuration Revision              : 198
MD5 digest                          : 0xF1 0x32 0x6C 0x2A 0x00 0xE6 0x51 0xFB
                                      0x6E 0xA4 0x0A 0x80 0x71 0xCC 0x2C 0x24
```

Listing 3.44 : *Vérification de la configuration du VTP client au niveau du site Lala Khadija.*

```
Switch001# show vtp status
VTP Version capable                 : 1 to 2
VTP version running                 : 1
VTP Domain Name                     : cev.com
VTP Pruning Mode                    : Disabled
VTP Traps Generation : Disabled
Device ID                           : 0060.4784.A400
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00

Feature VLAN :
--------------
```

```
VTP Operating Mode                  : Client
Maximum VLANs supported locally     : 255
Number of existing VLANs            : 16
Configuration Revision              : 154
MD5 digest                          : 0xEB 0x7A 0xE3 0x4C 0x10 0xF6 0xD9 0x3A
                                      0x59 0xC4 0xAF 0x88 0x7B 0xD8 0x36 0x58
```

Listing 3.45 : *Vérification de la configuration du VTP client au niveau du site Cojek.*

h) Configuration du Spanning-Tree Protocol (STP)

Le protocole STP a pour but d'affecter un root primaire ou secondaire à un VLAN. Nous l'avons configuré sur le Score1 et Score2.

Le Score1 a été configuré afin d'être le root pour les VLANs 10-14 et le bridge pour les VLANs 15-20. Inversement le Score2 sera root pour les VLANs 15-20 et le bridge pour les VLANs 10-14.

Les Listings 3.46 et 3.47 illustrent les commandes qui permettent de configurer cela.

```
Score1 (config) #spanning-tree mode pvst
Score1 config) #spanning-tree vlan 10-14 priority 8192
Score1 (config) #spanning-tree vlan 15-20 priority 16384
```

Listing 3.46 *: Configuration de STP sur Score1*

```
Score2 (config) #spanning-tree mode pvst
Score2 (config) #spanning-tree vlan 15-20 priority 8192
Score2 (config) #spanning-tree vlan 10-14 priority 16384
```

Listing 3.47 : *Configuration de STP sur Score1*

i) Configuration du Hot standby Router Protocol (HSRP)

La configuration de la haute disponibilité s'effectue au niveau des Switches de distribution (dans notre cas, c'est les switches Core qui ont le rôle de distribution) dans le but d'élire le routeur actif pour chaque VLAN, il est élu au moyen d'une priorité mise en place.

Nous avons configuré l'HSRP sur Score1 en mode « actif » pour les VLANs 10-14, et en mode « Standby » pour les VLANs 15-20. **Le listing 3.48** détaille la méthode de configuration

en mode actif pour le VLAN 10, et **le listing 3.49** détaille la méthode de configuration en mode passif pour le VLAN 15.

Nous avons configuré l'HSRP sur Score2 en mode « actif » pour les VLANs 15-20, et en mode « Standby » pour les VLANs 10-14. **Le listing 3.50** détaille la méthode de configuration en mode actif pour le VLAN 15 et **le listing 3.51** détaille la méthode de configuration en mode passif pour le VLAN 10.

- VLAN 10-14 sur Score1 : mode « **Actif** » :

```
Score1 (config) #interface Vlan 10
Score1 config-if) #standby 10 ip 10.10.10.254
Score1 (config-if) #standby 10 priority 105
Score1 (config-if) # standby 10 preempt
Score1 (config-if) #
```

***Listing 3.48**: Configuration du HSRP sur Score1 (VLAN 10).*

- VLAN 15-20 sur Score1 : mode « **Standby** » :

```
Score1 (config) # interface Vlan 15
Score1 config-if) #standby 15 ip 10.10.15.254
Score1 (config-if) #
```

***Listing 4.49**: Configuration du HSRP sur Score1 (VLAN 15).*

- VLAN 15-20 sur Score2 : mode « **Actif** » :

```
Score2 (config) #interface Vlan 15
Score2 config-if) #standby 15 ip 10.10.15.254
Score2 (config-if) #standby 15 priority 105
Score2 (config-if) # standby 15 preempt
Score2 (config-if) #
```

***Listing 3.50**: Configuration du HSRP sur Score2 (VLAN 15).*

- VLAN 10-14 sur Score2 : mode « **Standby** » :

```
Score2 (config) # interface Vlan 10
Score2 config-if) #standby 10 ip 10.10.10.254
Score2 (config-if) #
```

***Listing 3.51**: Configuration du HSRP sur Score2 (VLAN 10).*

Nous avons vérifié la configuration pour tous les VLANs avec la commande **Show standby brief** sur les deux switches. Les résultats sont présentés sur les listings ci-dessous :

```
Score1#show standby brief
                     P indicates  configured  to preempt.
|
Interface   Grp  Pri P State    Active          Standby         Virtual  IP
Vl10        10   105 P Active   local           10.10.10.253    10.10.10.254
Vl11        11   105 P Active   local           10.10.11.253    10.10.11.254
Vl12        12   105 P Active   local           10.10.12.253    10.10.12.254
Vl13        13   105 P Active   local           10.10.13.253    10.10.13.254
Vl14        14   105 P Active   local           10.10.14.253    10.10.14.254
Vl15        15   100  Standby   10.10.15.253    local           10.10.15.254
Vl16        16   100   Standby  10.10.16.253    local           10.10.16.254
Vl17        17   100   Standby   10.10.17.253   local           10.10.17.254
Vl18        18   100   Standby   10.10.18.253   local           10.10.18.254
Vl19        19   100   Standby   10.10.19.253   local           10.10.19.254
Vl20        20   100   Standby  10.10.20.253    local           10.10.20.254
```

***Listing 3.52**: Verification du HSRP sur Score1.*

```
Score2#show standby brief
                     P indicates  configured  to preempt.
Interface   Grp  Pri P State    Active          Standby         Virtual  IP
Vl10        10   100   Standby  10.10.10.252    local           10.10.10.254
Vl11        11   100   Standby  10.10.11.252    local           10.10.11.254
Vl12        12    100   Standby  10.10.12.252   local           10.10.12.254
Vl13        13   100   Standby   10.10.12.252   local           10.10.13.254
Vl14        14   100   Standby   10.10.14.252   local           10.10.14.254
Vl15        15   105 P Active   local           10.10.15.252    10.10.15.254
Vl16        16   105 P Active   local           10.10.16.252    10.10.16.254
Vl17        17   105 P Active   local           10.10.17.252    10.10.17.254
Vl18        18   105 P Active   local           10.10.18.252    10.10.18.254
Vl19        19   105 P Active   local           10.10.19.252    10.10.19.254
Vl20        20   105 P Active   local           10.10.20.252    10.10.20.254
```

***Listing 3.53 :** Vérification du HSRP sur Score2.*

j) Agrégation des liens EtherChannel

Comme cité dans le chapitre 2, le but de L'EtherChannel est d'augmenter la vitesse en procurant des liaisons à haut débit, de fournir une redondance et d'augmenter la tolérance aux pannes entre les commutateurs. Nous avons donc mis e place une agrégation des lies FasteEthernet entre Score1 et Score2. Les détails de la configuration sont étalés dans **le Listing 3.54**.

```
Score1 (config)#interface range fastEthernet 0/7-8
Score1 (config-if-range)#channel-group 1 mode on
Score1 (config-if-range)#
Creating a port-channel interface Port-channel 1

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

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

Score1 (config-if-range)#exit
Score1 (config)#interface port-channel 1
Score1 (config-if)#switchport trunk encapsulation dot1q
Score1 (config-if)#switchport mode trunk
```

Listing 3.54 : *Configuration de l'EtherChannel.*

k) Configuration de l'OSPF (Open Shortest Path First)

Afin d'assurer ce protocole qui garantit le routage du réseau, nous avons configuré le protocole OSPF au niveau des switches Core du site central et des sites distants. Ainsi que sur les routeurs qui relient les différents sites entre eux.

Nous avons alloué un groupe 1 et une aire 10 dans chaque configuration, et avons saisi les réseaux directement connectés dans chaque Switch ou routeur. Pour les VLANs, nous avons saisi le réseau 10.10.0.0 pour le site central, 10.20.0.0 pour le site de lala Khadija et 10.30.0.0 pour le site Cojek, avec un masque inversé 0.0.255.255 pour tous les sites qui englobera tous les VLANs.

Le Listing 3.55 illustre la méthode de configuration de l'OSPF avec sa configuration au niveau du switch Multiplayer de niveau 3 « Switch-Routeur » qui relie tous les sites entre eux et qui joue le rôle d'un routeur.

Le Listing 3.56 illustre la méthode de configuration de l'OSPF avec sa configuration au niveau du « Score1 ».

Nous avons vérifié la configuration de l'OSPF sur les autres équipements avec la commande **Show running-config**. Les résultats sont affichés sur **les listings 3.57 - 3.62.**

```
Switch-Routeur (config)#router ospf 1
Switch-Routeur (config-router)#network 192.168.1.0 0.0.0.3 area 10
Switch-Routeur (config-router)#network 192.168.4.0 0.0.0.3 area 10
Switch-Routeur (config-router)#network 172.16.1.0 0.0.0.3 area 10
Switch-Routeur (config-router)#network 172.16.4.0 0.0.0.3 area 10
Switch-Routeur (config-router)#network 192.168.5.0 0.0.0.3 area 10
Switch-Routeur (config-router)#network 172.16.5.0 0.0.0.3 area 10
```

Listing 3.55 : *Configuration de l'OSPF sur le Switch-Routeur*

```
Score1 (config)# router ospf 1
Score1 (config-router)# network 172.16.5.0 0.0.0.3 area 10
Score1 (config-router)# network 10.10.0.0 0.0.255.255 area 10
```

Listing 3.56 : *Configuration de l'OSPF sur le Score1*

```
!
router ospf 1
log-adjacency-changes
network 192.168.1.0 0.0.0.3 area 10
network 192.168.4.0 0.0.0.3 area 10
network 172.16.1.0 0.0.0.3 area 10
network 172.16.4.0 0.0.0.3 area 10
network 192.168.5.0 0.0.0.3 area 10
network 172.16.5.0 0.0.0.3 area 10
!
```

Listing 3.57 : *Vérification de la configuration de l'OSPF sur le Switch-Routeur.*

```
router ospf 1
log-adjacency-changes
```

```
network 172.16.5.0 0.0.0.3 area 10
network 10.10.0.0 0.0.255.255 area 10
!
```

Listing 3.58 : *Vérification de la configuration de l'OSPF sur le Score1.*

```
!
router ospf 1
log-adjacency-changes
network 172.16.5.0 0.0.0.3 area 10
network 10.10.0.0 0.0.255.255 area 10
!
```

Listing 3.58 : *Vérification de la configuration de l'OSPF sur le score2*

```
!
router ospf 1
log-adjacency-changes
network 172.16.1.0 0.0.0.3 area 10
network 172.16.2.0 0.0.0.3 area 10
!
```

```
!
router ospf 1
log-adjacency-changes
network 172.16.4.0 0.0.0.3 area 10
network 172.16.3.0 0.0.0.3 area 10
!
```

Listing 3.59 : *Vérification de la configuration de l'OSPF sur les routeurs Algérie –Télécom 1 et 2.*

```
!
router ospf 1
log-adjacency-changes
network 192.168.1.0 0.0.0.3 area 10
network 192.168.2.0 0.0.0.3 area 10
!
```

```
!
router ospf 1
log-adjacency-changes
network 192.168.3.0 0.0.0.3 area 10
network 192.168.4.0 0.0.0.3 area 10
!
```

Listing 3.60 : *Vérification de la configuration de l'OSPF sur les routeurs Algérie –Télécom 3 et 4.*

```
!
router ospf 1
log-adjacency-changes
network 172.16.2.0 0.0.0.3 area 10
network 172.16.3.0 0.0.0.3 area 10
network 172.16.6.0 0.0.0.3 area 10
!
```

```
!
router ospf 1
log-adjacency-changes
network 192.168.2.0 0.0.0.3 area 10
network 192.168.3.0 0.0.0.3 area 10
network 192.168.6.0 0.0.0.3 area 10
!
```

Listing 3.61 : *Vérification de la configuration de l'OSPF sur les routeurs des sites Lala Khadija et Cojek.*

```
!
router ospf 1
log-adjacency-changes
network 172.16.6.0 0.0.0.3 area 10
network 10.20.0.0 0.0.255.255 area 10
```

```
!
router ospf 1
log-adjacency-changes
network 192.168.6.0 0.0.0.3 area 10
network 10.30.0.0 0.0.255.255 area  10
```

Listing 3.62 : *Vérification de la configuration de l'OSPF sur les Switch Core des sites Lala Khadija et Cojek*

C. Vérification de la communication

Après avoir mis en place notre réseau, nous passons à l'étape la plus importante qui est la vérification de son bon fonctionnement. Nous allons d'abord vérifier que la connexion inter-sites est opérationnelle. Pour ce faire nous avons simulé un Ping entre l'adresse IP du PC02-L du site lala Khadija qui est : 10.20.60.1 et l'adresse IP du PC 3 du site central qui : 10.10.11.1, et également avec l'adresse IP du PC01-C du site Cojek qui est : 10.30.40.1.

Ensuite nous avons simulé un Ping entre l'adresse IP du PC0-1 du site Cojek qui est : 10.30.40.1 et l'adresse IP du PC 5 du site central qui : 10.10.1.14, et également avec l'adresse IP du PC01-L du site lala Khadija qui est : 10.20.30.1.

Les résultats affichés sur les **figures 3.8 et 3.9 démontrent** que les Pings fonctionnent, donc la connexion inter-sites est opérationnelle.

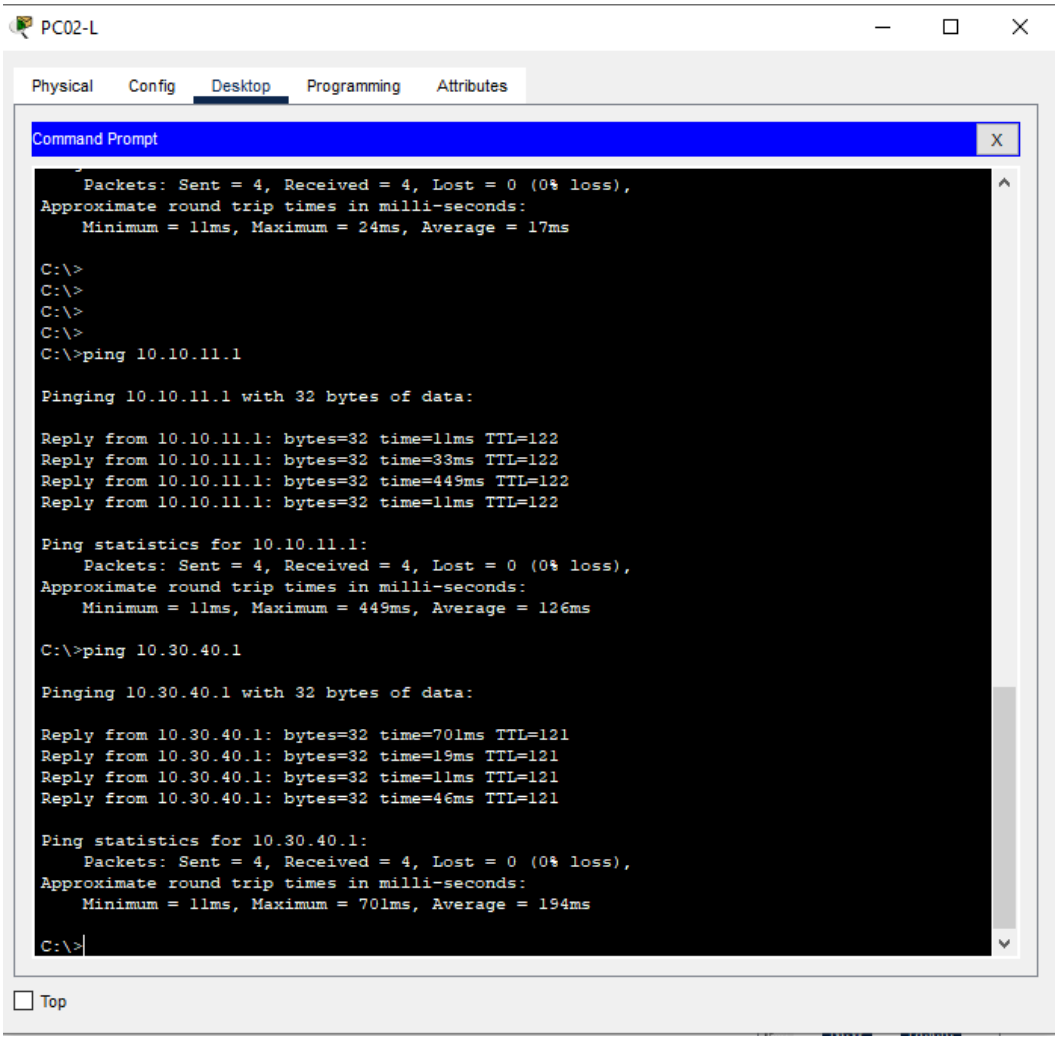

Figure 3.8 : Test de connectivité entre le PC du site lala Khadija et les PCs des sites distants.

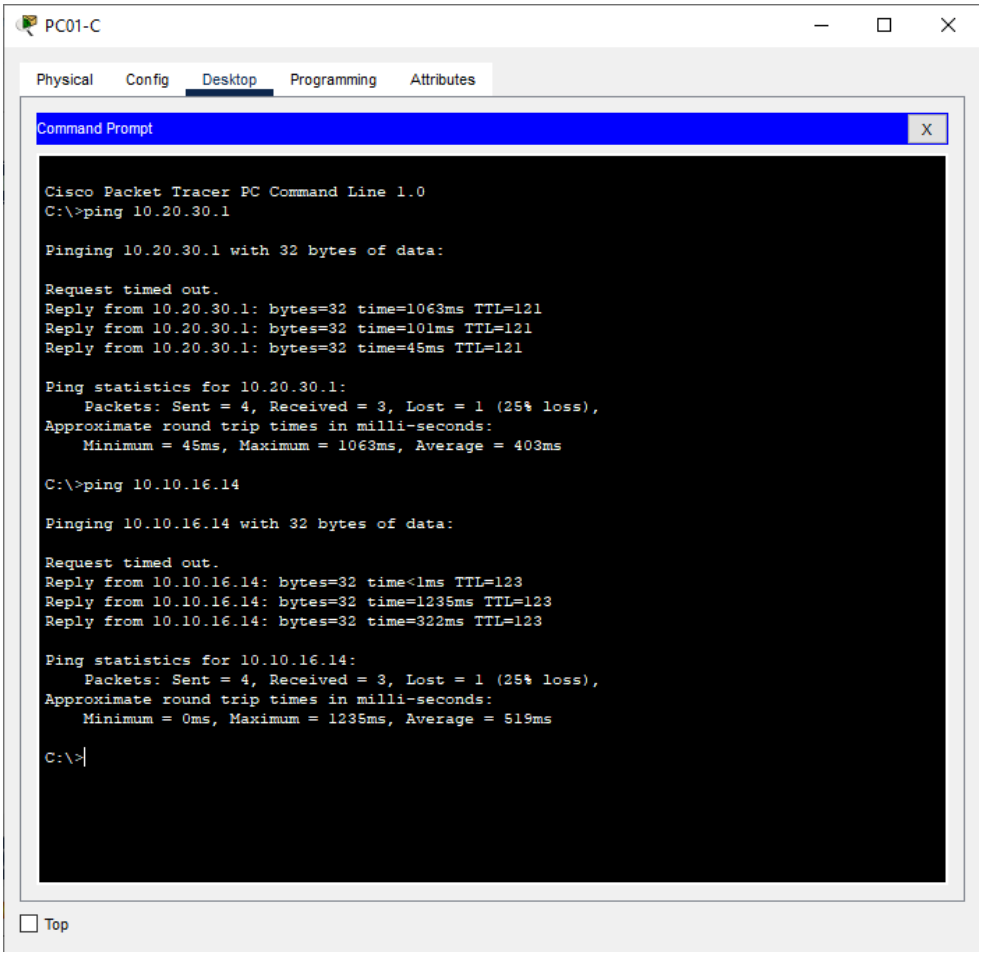

Figure 3.9 : Test de connectivité entre le PC du site Cojek et les PCs des sites distants.

Après nous être assuré que l'interconnexion entre sites est opérationnelle, nous avons vérifié le fonctionnement du nouveau réseau mis en place sur le site central, qui a été configuré avec différents protocoles visant à améliorer les défaillances du réseau existant.

Afin de vérifier cela, nous avons simulé un Ping continue entre l'adresse IP du PC1 du site central qui est : 10.10.10.7 et l'adresse IP du PC 9 du site central qui : 10.10.13.3. Puis nous avons simulé une panne en mettant le root principal de ce VLAN en « **Shutdown** ».

La figure 3.10 illustre le résultat du Ping après cette panne. Nous constatons donc que le Ping s'arrête instantanément et ne passe plus.

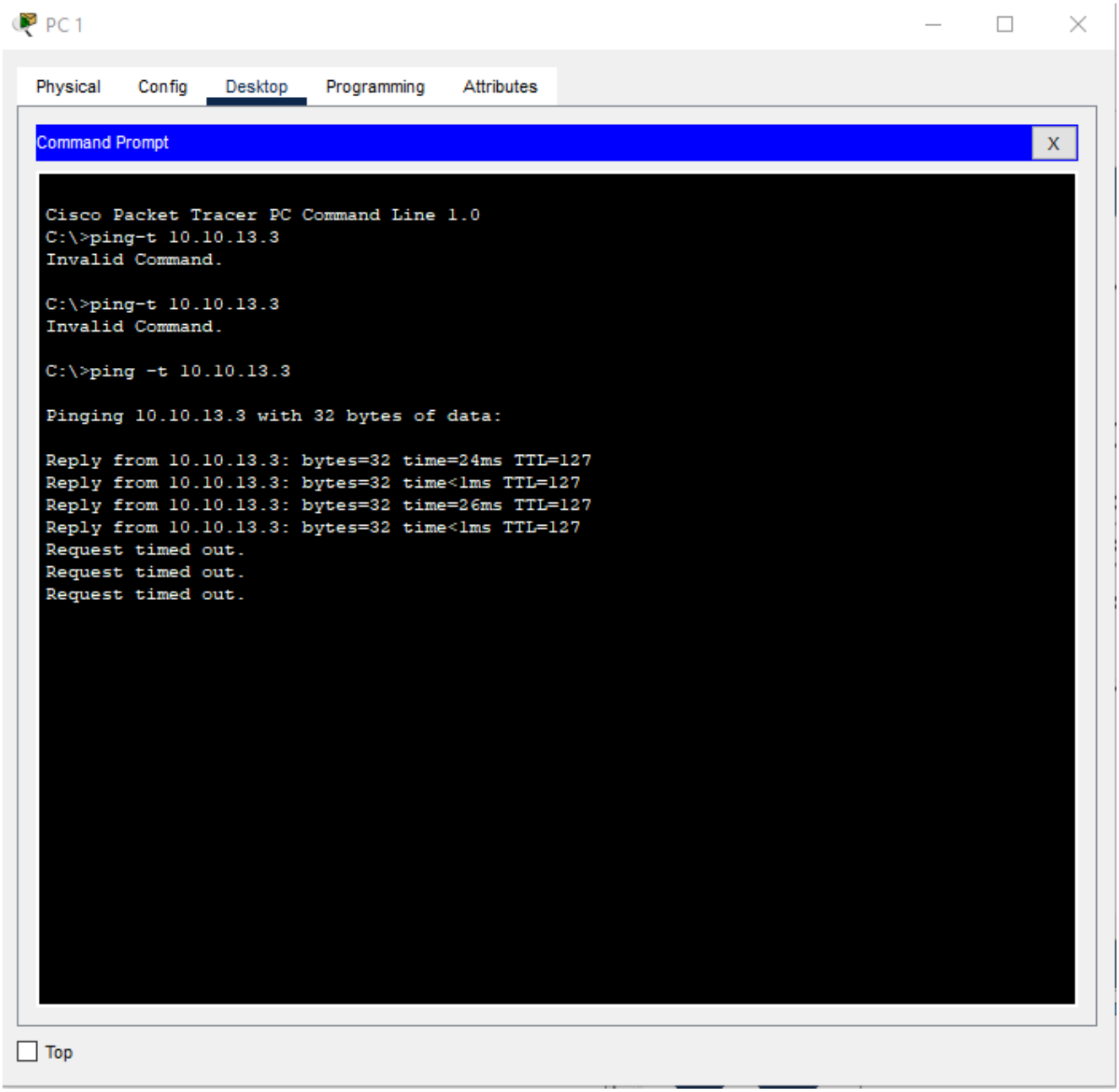

Figure 3.10 : Ping lors de la désactivation du port vers Score1.

Après quelques arrêts, grâce au protocole HSRP le Score1 communique avec le Score2 et l'informe qu'il est tombé en panne. Le Score2 active donc automatiquement le root en « standby » pour qu'il devienne « actif ». Dans **la figure 3.11** on constate alors que le Ping reprend. Ce qui prouve que la route est convertie vers Score2.

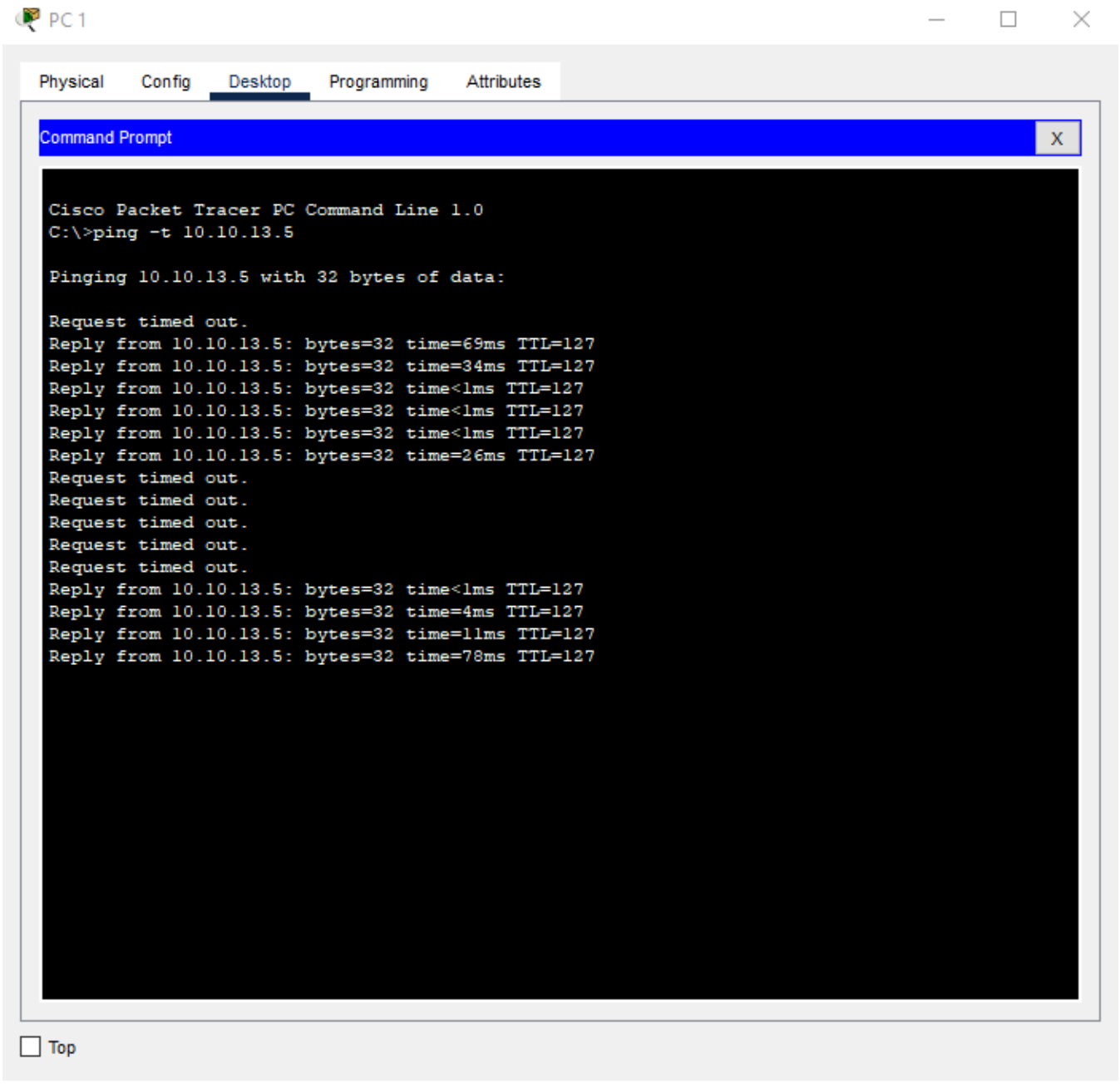

Figure 3.11 : Reprise du Ping après la conversion de la route vers Score2.

Pour s'assurer que le **preempt** du HSRP fonctionne parfaitement, nous avons réactivé l'interface principale sur Score1 pour vérifier s'il reprendra sa route principale.

La figure 3.12 illustre le résultat du Ping après la réactivation de l'interface principale. Nous constatons donc que le Ping s'arrête instantanément de nouveau pendant 5 requêtes, le temps que les deux Switches se discutent les priorités, puis reprend directement. Ceci nous démontre que les protocoles HSRP et OSPF mis en place pour rétablir les défaillances du réseau existant fonctionnent parfaitement.

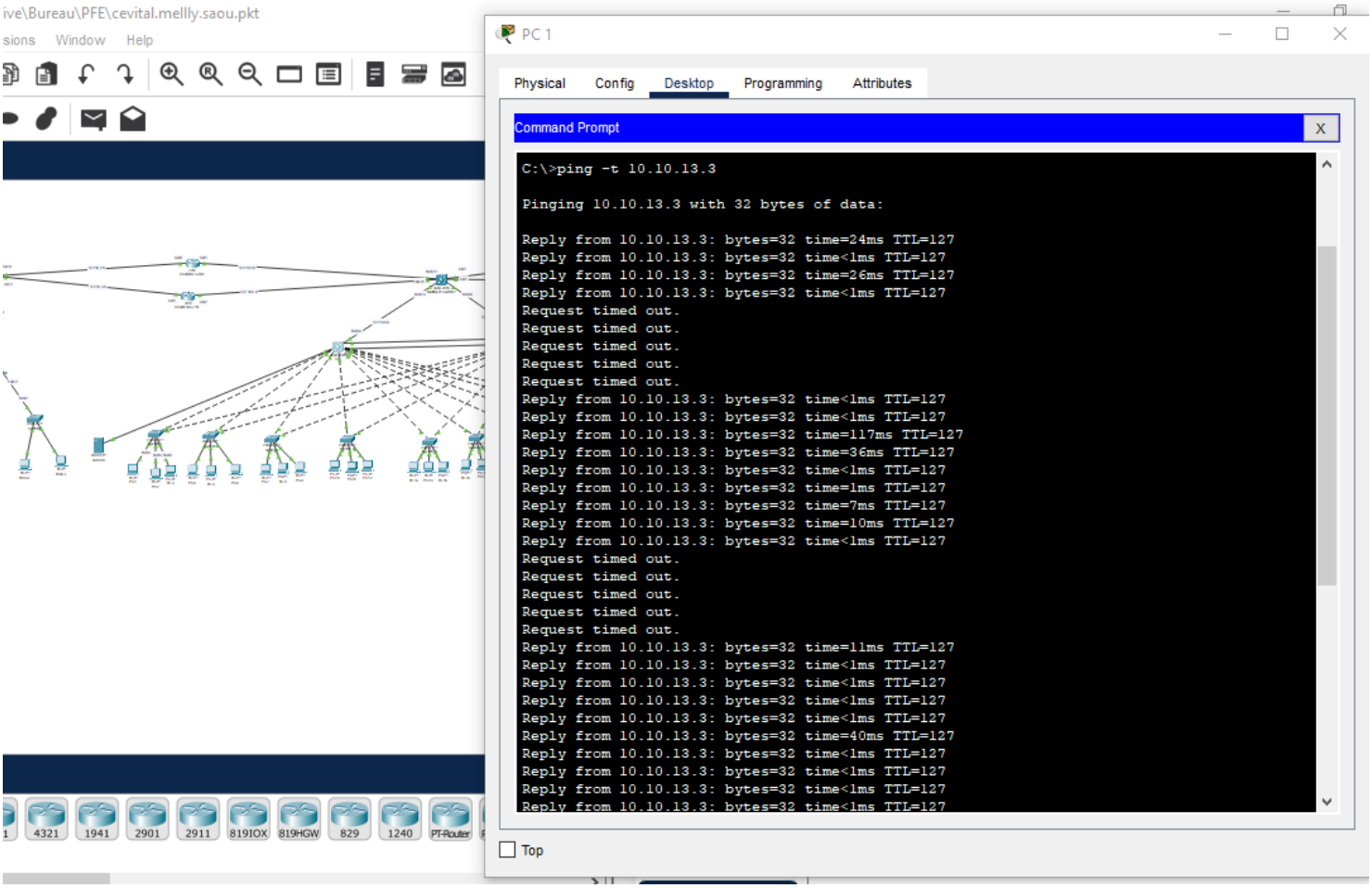

Figure 3.12: Ping lors de la réactivation du port vers Score1.

3.6.Conclusion

Ce chapitre s'est scindé en deux parties. Dans la première nous avons configuré le réseau déjà existant de Cevital. Nous avons mis en avant les configurations et protocoles utilisés, à savoir la configuration des VLANs, des liens Trunk, les protocoles VTP, DHCP…etc. Nous avons remarqué dans cette partie que la fonction de ce réseau est réduite et peut présenter des défaillances. C'est pourquoi nous nous sommes tournés dans la deuxième partie vers une proposition et configuration d'un nouveau réseau pour améliorer le réseau existant avec des protocoles tels que le STP, HSRP, OSPF. Les résultats obtenus et détaillés dans ce chapitre démontrent que le réseau proposé est la solution adéquate à la problématique citée en chapitre 2.

Conclusion générale

Conclusion générale

L'objectif de notre travail était proposer une nouvelle architecture protégée en cas de panne du réseau, et mettre en place des solutions fiables en utilisant des liens virtuels, des connexions aux sites distants pour assurer un meilleur fonctionnement et de partage de ressources. Ce projet nous a permis de mettre en pratique les connaissances acquises durant la période de notre stage pratique au sein de l'entreprise Cevital de Bejaia.

Afin d'accomplir notre travail et d'aboutir au résultat recherché, nous avons choisi d'utiliser le simulateur Packet Tracer pour les différents avantages qu'il présente, à savoir la mise en évidence avec une grande exactitude de l'architecture du système à réaliser en précisant les différents composants, ainsi que la simplicité et la clarté des matériels dont on aura besoin, ce qui facilite considérablement la configuration sur Packet Tracer.

En travaillant sur ce projet, nous avons acquis les connaissances nécessaires à la création d'un réseau d'entreprise efficace et extensible. Nous avons approfondi les fonctionnalités des commutateurs de niveau 2 et multi-niveaux tels que les VLANs, les trunks, le routage inter-VLAN, l'agrégation des ports, le Spanning Tree ainsi avec des protocoles tels que le HSRP, et l'OSPF.

Les résultats obtenus et détaillés dans ce mémoire avec la configuration du nouveau réseau proposé, démontrent que ce réseau est la solution adéquate à la problématique indiquée.

Bibliographie

[1] Philippe Atelin « Réseaux informatiques – Notions fondamentales », Eni éditions

[2] GUY Pujolle. Cours réseaux et télécoms. Edition Eyrolles, 2004

[3] FOROUZAN B., « Local Area Network, Mc GRAW Hill » éditions, 2009.

[4] Bertrand PETIT ; architecture des réseaux, 2006.

[5] Badéche A. classification selon l'architecture, Mémoire master Département informatique, université Bejaia. 2012

[6] Christian Draux, Les réseaux.2006.

[7] Initiation aux réseaux (cours et exercices) de « GUY Pujolle édition Eyrolles (nov 2000).

[8] Soumia chelihi. Les équipements d'interconnexion, mémoire master département informatique université de guelma 2015

[9] Pujolle GUY, « les réseaux) Eyrolles Edition 2008

[10] Atelin, Philippe et DORDOIGNE, José. Réseaux informatiques : Notions fondamentales Normes, Architecture, Modèle OSI, TCP/IP, Ethernet, Wi-Fi,... Editions Eni, 2006

[11] Source interne de CEVITAL.

[12] Gerardo Rubino, Laurent Toutain, Réseaux locaux sans fil, Edition 8mai 1998.

[13] VAUCAMPS A., "Cisco CCNA", ENI édition, 2010.

[14] LI, T., COLE, B., MORTON, P., et al.RFC2281 : Cisco Hot standby Routeur Protocol (HSRP).

[15] Richard TRABELSI Froom, Balaji Sivasubramanian, and Erum Frahim. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide : Foundation Learning for SWITCH 642-813. Cisco Press, 2010.

[16] VETRISELVAN, V., PATIL, Pravin R., et MAHENDRAN, M. Survey on the RIP, OSPF, EIGRP routing protocols. International Journal of computer Science and information Technologies, 2014, vol. 5, no 2, p. 1058-1065.

Webographie

[W1] https://www.techno-science.net/definition/1363.html

[W2] https://www.edawsoft.com/fr/network-protocol.html

[W3] https://www.techno-science.net/definition/3758.html

[W4] http://www.chicoree.fr/w/full-dplex

[W5] https://charlestech.fr/la-redondance-du-reseau-un-element-de-securite-essentiel/

[W6]= https://www.supinfo.com/articles/single/596-introduction-au-protocoles-hsrp

Bibliographie des figures

[F1] Garg Arushi, LAN MAN WAN Ppt final,Linkedh Slideshare,21 nov 2013.

[F2] Vincent Séretaine, Jean-manacessé Pouadou, Les réseaux de zéros, Edition Eyrolles, 8 février 2022.

[F3] Pujolle GUY, Initiation aux réseaux, Edition Eyrolles, 2014.

[F4]https://www.samomoi.com/reseauxinformatiques/lesprincipauxcomposantdinterconnexion.php

[F5] https://wiki-tech.io/R%C3%A9seau/Protocoles/HSRP

[F6] https://forum.huawei.com/enterprise/en/what-is-vrrp-and-example-configuration/thread/741607-861?page=1

Résumé

Ce mémoire fait l'objet de stage de fin d'étude au sein de l'entreprise CEVITAL Bejaia ou nous avons proposé une solution qui permet de centraliser les équipements et les ressources utilisées par les employés au sein de l'entreprise. Dans le premier temps nous avons décrit les généralités sur les réseaux, puis nous avons présenté l'organisme d'accueil. Ensuite, nous avons proposé de nouvelles améliorations au réseau de l'entreprise tout en étudiant les solutions adéquates. Et en fin nous avons mis en œuvre ces dernières.

Mots clés : VTP, VLAN, DHCP, HSRP, OSPF, PACKET TRACER.

Abstract

This thesis is the subject of an end-of-study internship within the company CEVITAL Bejaia where we have proposed a solution, which makes it possible to centralize the equipment and the resources used by the employees within the company. At first, we described the generalities on the networks, and then we presented the host organization. Then, we proposed new improvements to the company's network while studying the appropriate solutions. And in the end we implemented these.

Keywords: VTP, VLAN, DHCP, HSRP, OSPF, PACKET TRACER