

REBUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTRE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE
SCIENTIFIQUE



UNIVERSITE A. MIRA-BEJAIA
FACULTE DE TECHNOLOGIE
DEPARTEMENT GENIE ELECTRIQUE



MEMOIRE DE FIN D'ETUDES EN VUE DE L'OBTENTION DU DIPLOME DE MASTER

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

Thème

Installation, Configuration et Administration
d'un Réseau Local (CEVITAL)



Soutenu le 11 octobre 2020

Présenté par :

- ♣ M^{elle} GHERBI Nadjette
- ♣ M^{elle} HAMCHAOUI Dalia

Encadré par :

- ♣ M^r BENNAIMIROUCHE Nadir
- ♣ M^r SLIMANI Mennad

Membres du jury :

- ♣ M^{me} ACHOUR Lyakout
- ♣ M^r MEKHMOUKH Abdenour

Présidente
Examineur

Année universitaire : 2019-2020

Dédicace

Je dédie ce mémoire

A mes chers parents, quoi que je fasse ou que je dise, je ne saurai point vous remercier comme il se doit. Votre affection me couvre, votre bienveillance me guide et votre présence à mes côtés a toujours été ma source de force pour affronter les différents obstacles.

A mon frère et ma sœur, pour leur soutien qu'ils trouvent ici l'expression de ma haute gratitude.

A mon fiancé, pour sa patience, son amour et qui a toujours été à mes côtés pour me soutenir et m'encourager.

A ma famille et mes chers amis(es), qui m'ont toujours encouragés et à qui je souhaite plus de réussite et de succès.

Puisse Dieu vous donne santé, bonheur, courage et surtout réussite.

DALIA

Dédicaces

*Avec un énorme plaisir, un cœur ouvert et une immense
joie, que je dédie ce modeste travail*

*A mes très chers parent, pour leurs patiences, leurs amour,
leurs encouragements et leurs sacrifices tout au long de mon
parcoure ;*

A mes deux frères ;

A mon cher ami S.NADIR;

A toute ma famille GHARBI ;

A tous mes amis ;

*ET à tous ceux qui m'ont aidé dans l'élaboration de ce
travail.*

NADJETTE

Remerciement

Avant tout, nous remercions Dieu tout puissant de nous avoir donné la force, le courage et la patience d'accomplir notre travail en cette période de pandémie.

Nous présentons nos sincères gratitudees à nos très chers parents et nos familles pour leurs soutient et leurs encouragement car sans eux on n'aurait pas pu arriver jusqu'à là.

Nous tenons à adresser nos vifs remerciements à tous ceux qui nous ont aidées de près ou de loin à élaborer notre mémoire de fin d'études.

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

Nos sincères remerciements aux personnels de l'entreprise CEVITAL Bejaia, spécialement à M^r SLIMANI Mennad notre encadreur de stage pour sa patience, son sérieux et sa grande disponibilité tout au long de notre stage au sein de l'entreprise.

Nous remercions profondément notre encadreur de l'université M^r BENNAMIROUCHE Nadir pour sa confiance, son encouragement et ses conseils afin de terminer notre travail.

Nous présentons tous nos respects et nos sincères remerciements aux membres du jury M^{me} ACHOUR Lyakout et M^r MEKHMOUKH Abdenour de nous avoir honoré en acceptant de juger notre modeste travail.

Nous tenons à remercier tous nos amis (es) et surtout le groupe princesses pour les meilleurs et pires moments passés ensemble.

Table des matières

Sommaire

TABLE DES MATIERES	i
LISTE DES FIGURES	iv
LISTE DES TABLEAUX	vi
LISTE DES ABREVIATIONS	vii
Introduction générale	1
CHAPITRE 1 : Généralités sur les réseaux informatiques	
1.1.Introduction	3
1.2.Un réseau informatique	3
1.3.Objectif d'un réseau informatique	3
1.3.1.Le partage de ressource.....	3
1.3.2.La fiabilité	3
1.3.3.La réduction des coûts	3
1.4.Classification des réseaux informatiques	4
1.4.1.Les réseaux locaux (LAN)	4
1.4.2.Les réseaux métropolitains (MAN)	5
1.4.3.Les réseaux étendus (WAN)	5
1.5.Les topologies des réseaux informatiques	5
1.5.1.Les topologies physiques	6
1.5.2.Les topologies logiques	10
1.6.Les architectures des réseaux informatiques	11
1.6.1.Architecture poste à poste	11
1.6.2.Architecture client/serveur	12
1.7.Les équipements d'interconnexion	13
1.7.1.La carte réseau	13
1.7.2.Le répéteur	14
1.7.3.Le concentrateur	14
1.7.4.Le commutateur (Switch)	14
1.7.5.Le pont	15
1.7.6.Le routeur	15
1.7.7.La passerelle	15
1.8.Modèles OSI – TCP/IP	15
1.9.Conclusion	16

Sommaire

CHAPITRE 2 : Etude du réseau existant

2.1.Introduction	17
2.2.Partie 1 : l'organisme d'accueil	17
2.2.1.Présentation de l'entreprise et son historique	17
2.2.2.Situation géographique	17
2.2.3.Organisme CEVITAL	18
2.2.4.Architecture du réseau CEVITAL	20
2.2.5.Matériels utilisés dans l'architecture existante	22
2.2.6.Les liaisons inter-sites	24
2.2.7.VLAN de l'entreprise	25
2.2.8.Utilisation du réseau informatique	26
2.2.9.Critique de l'existant	26
2.2.10.Problématique	27
2.2.11.Propositions	27
2.2.12.Solution optée	28
2.3.Partie 2 : étude de l'existant	28
2.3.1.La redondance	28
2.3.2.Les protocoles de redondance	28
2.3.3.STP (Spanning Tree Protocol)	31
2.3.4.EtherChannel	32
2.3.5.VTP (VLAN Trunking Protocol)	32
2.3.6.Les protocoles de routage	33
2.4.Conclusion	33

CHAPITRE 3 : Installation et configuration du réseau CEVITAL

3.1.Introduction	35
3.2.Présentation du simulateur	35
3.3.Présentation du réseau	36
3.3.1.Segmentation du réseau en VLAN	36
3.3.2.Adressage des VLANs	37
3.4.Partie 1 : le réseau existant	37
3.4.1.Architecture de mise en œuvre	38
3.4.2.Configuration des équipements	38

Sommaire

3.4.3. Vérification des adressages IP attribuées par le DHCP	44
3.4.4. Vérification de la connectivité	45
3.5. Partie 2 : nouvelle architecture proposée au réseau CEVITAL	46
3.5.1. Architecture de mise en œuvre	46
3.5.2. Configuration des équipements	48
3.5.3. Vérification des adressages IP attribuées par le DHCP	57
3.5.4. EIGRP (Enhanced Interior Gateway Routing Protocol)	57
3.5.5. Configuration du Spanning Tree Protocol (STP)	59
3.5.6. Configuration du Hot Standby Router Protocol (HSRP)	59
3.5.7. Agrégation des liens EtherChannel	61
3.5.8. Vérification de la communication	62
3.6. Conclusion	65
Conclusion générale	66
Bibliographie	67
Webographie	68

Liste des figures

Liste des figures

1.1	Classification des réseaux	4
1.2	Réseau local (LAN)	4
1.3	Réseau métropolitain (MAN)	5
1.4	Réseau étendu (WAN)	5
1.5	Topologie en bus	6
1.6	Topologie en anneau	7
1.7	Topologie en étoile	8
1.8	Topologie hybride	9
1.9	Topologie maillée	10
1.10	Architecture poste à poste	11
1.11	Architecture client/serveur	12
1.12	Carte réseau	13
1.13	Répéteur	14
1.14	Concentrateur	14
1.15	Commutateur	15
1.16	Le pont	15
1.18	Modèles OSI - TCP/IP	16
2.1	Image satellitaire de CEVITAL Bejaia	18
2.2	Organigramme de l'organisation administrative de CEVITAL Bejaia	19
2.3	Architecture du réseau informatique du site CEVITAL-Bejaia	21
2.1	Switch Core /distributeur	22
2.2	Switch d'accès	22
2.3	Switch en cascade	23
2.4	Routeur Cisco 2900	23

Liste des figures

2.5	Point d'accès WIFI CISCO	23
2.6	Pare feu Palo Alto 3020	24
2.7	Connexion inter-sites du groupe CEVITAL Bejaia	25
2.8	Le Protocole HSRP vue d'un hôte du réseau	30
2.12	Le schéma physique et virtuel d'un réseau HSRP	30
3.1	Capture de l'interface du simulateur Cisco Packet Tracer 7.2.1	35
3.2	Architecture du réseau local existant	38
3.3	Configuration du Hostname et mot de passe	39
3.4	Création des VLANs	40
3.5	Configuration des interfaces VLANs	41
3.6	Configuration du DHCP	41
3.7	Vérification de l'activation du DHCP	42
3.8	Configuration des interfaces du switch Core en mode Trunk	43
3.9	Configuration des interfaces du switch en mode Access	43
3.10	Configuration du VTP serveur	44
3.11	Configuration du VTP client	44
3.12	Adresse IP attribué automatiquement	44
3.13	Test entre le PC ₁₂ et le PC ₆	45
3.14	Test entre le PC ₁₀ et le PC ₁₅	46
3.15	L'architecture proposée au réseau CEVITAL Bejaia	47
3.16	Configuration du Hostname et Password	48
3.17	Création des VLANs	48
3.18	Vérification des VLANs	49
3.19	Configuration des interfaces VLANs sur SD ₁	49

Liste des figures

3.20	Vérification des interfaces VLANs de SD ₁	50
3.21	Configuration des interfaces VLANs sur SD ₂	50
3.22	Vérification des interfaces VLANs sur SD ₂	51
3.23	Configuration du DHCP sur SD ₁	51
3.24	Configuration du DHCP sur SD ₂	51
3.25	Vérification de la création des pools DHCP sur SD ₁	52
3.26	Vérification de la création des pools DHCP sur SD ₂	53
3.27	Adresses exclues sur le SD ₁	53
3.28	Adresses exclues sur le SD ₂	54
3.29	Configuration des liens Trunk	54
3.30	Vérification des liens Trunk	55
3.31	Configuration des interfaces du switch en mode Access	55
3.32	Configuration du VTP serveur	56
3.33	Vérification de la configuration du VTP serveur	56
3.34	Configuration du VTP client	56
3.35	Vérification de la configuration du VTP client	57
3.36	Adresse IP attribué automatiquement	57
3.37	Configuration d'EIGRP sur SD ₁	58
3.38	Configuration d'EIGRP sur SD ₂	58
3.39	Configuration d'EIGRP sur SC ₁	58
3.40	Configuration d'EIGRP sur SC ₂	59
3.41	Configuration de STP sur SD ₁	59
3.42	Configuration de STP sur SD ₂	59

Liste des figures

3.43	Configuration du HSRP sur SD ₁ (VLAN 10-17)	60
3.44	Configuration du HSRP sur SD ₁ (Vlan 18-25)	60
3.45	Configuration du HSRP sur SD ₂ (Vlan 18-25).....	60
3.46	Configuration du HSRP sur SD ₂ (Vlan 10-17)	60
3.47	Vérification du HSRP sur SD ₁	61
3.48	Vérification du HSRP sur SD ₂	61
3.49	Configuration d'EtherChannel	62
3.50	Capture explicative du Ping	63
3.51	Ping lors de désactivation du port vers SD ₁	64
3.52	Reprise du Ping après discussion avec SD ₂	64
3.53	Ping lors de réactivation du port vers SD ₁	65

Liste des tableaux

LISTE DES TABLEAUX

2.1	Liste des VLANs de l'entreprise	26
3.1	Liste des noms VLANs du réseau et leur plan d'adressage	37

Liste des abréviations

Liste des abréviations

ARP : Address Resolution Protocol.

AVF : Active Virtual Forwarder.

AVG : Active Virtual Gateway.

BPDU : Bridge Protocol Data Units.

CSMA/CD : Carrier Sense Multiple Access With Collision Direct.

DFC : Direction Finances Comptabilité.

DG : Direction Générale.

DHCP : Dynamic Host Configuration Protocol.

DMZ : Demilitaried Zone.

DSI : Direction Système d'Information.

EIGPR : Enhanced Interior Gateway Routing Protocol.

GLBP: Getway Load Blancing Protocol.

HSRP : Hot Standby Router Protocol.

IBM : International Business Machines.

IGRP : Interior Gateway Routing Protocol.

IP : Internet Protocol.

LAN : Local Area Network.

LED: Light-Emitting Diode.

MAC : Medium Access Control.

MAN: Metropolitan Area Network.

NIC : Network Interface Card.

OSI : Open System Interconnection.

OSPF : Open Shortest Path First.

PC :Personal Computer.

Liste des abréviations

RIP: Routing Information Protocol.

RJ45 : registered jack 45.

STP : Spanning Tree Protocol.

SPA : Société Par Action.

TCP/IP : Transmission Control Protocol/ Internet Protocol.

UDP : User Datagram Protocol.

VLAN : Virtual Local Area Network.

VRRP: Virtual Router Redundancy Protocol.

VSAT: Very Small Aperture Terminal.

VTP : Virtual Trunking Protocol.

VPN: Virtual Private Network.

WAN : Wide Area Network.

WI-FI: Wireless Fidelity.

WIMAX: Worldwide Interoperability for Microwave Access.

*Introduction
générale*

Introduction générale

L'avènement du réseau informatique est devenu un élément historique très important dans toute institution, qu'elle soit, commerciale, industrielle, gouvernementale ou éducative, mais l'utilité est presque la même. Ceci est dû principalement au fait que ce dernier apporte une extraordinaire contribution pour l'utilisateur en lui offrant l'accès à distance aux différents services numériques possibles avec plus souplesse et en un temps record.

Le besoin d'échange de données est apparu immédiatement, après l'apparition des ordinateurs, puis l'idée de les relier entre eux, c'est là qu'apparaît le premier concept du réseau informatique. Dans toute entreprise, le concept du réseau est simple, chaque entreprise qui existe dispose généralement d'un réseau informatique LAN ou WAN, ce qui lui permet de partager des ressources et des données protégées avec des procédures de sécurité, de confidentialité, d'intégrité, de disponibilité et de non-répudiation. Pour cela, de nombreux outils matériels ou logiciels associés aux différents protocoles d'échange, comme de partage ou d'accès sont disponibles comme solutions, tels que : VLAN, HSRP, ...etc [1].

L'entreprise CEVITAL de Bejaia est une organisation à grande échelle, qui joue un rôle primordial dans l'économie du pays.

A l'arrivée des nouvelles technologies de l'information, l'entreprise CEVITAL, s'est lancée dans la modernisation en renouvelant son réseau de télécommunication. Ce processus de modernisation en harmonie avec les technologies de l'information fait face à de nombreuses difficultés liées à une mauvaise distribution d'architecture et de partage de ressources. En effet, cela est dû divers problèmes liés aux collisions et congestions dans le trafic de données.

L'objectif de notre projet est de proposer une nouvelle architecture sécurisée en cas de panne du réseau de l'entreprise, et mettre en place des mécanismes et des solutions fiables en utilisant des liens virtuels pour assurer un meilleur fonctionnement et partage de ressources. Afin de réaliser les objectifs visés, nous avons organisé notre travail en trois chapitres, à savoir :

- Le premier chapitre est consacré à des descriptions et des généralités sur les réseaux informatiques, en décrivant les types de réseau, ainsi que, ses modèles et les différents protocoles.
- Le deuxième chapitre est dédié à une étude préliminaire dans laquelle nous avons présenté l'organisme d'accueil site CEVITA Bejaia, ainsi que les différents équipements et les ressources informatiques que dispose l'entreprise. De plus, nous avons exposé la problématique et proposer une solution efficace à cette dernière.

Introduction générale

- Le troisième chapitre, décrit la première partie pratique de notre projet, dont nous avons présenté le réseau existant, ainsi que la configuration et la segmentation du réseau en questions sur des VLANs en fonction de différentes directions administratives. Dans la deuxième partie pratique, nous avons proposé une nouvelle architecture, ainsi que la configuration de certains protocoles clé, tels que : le HSRP, le EIGRP et le STP.

Enfin, notre mémoire se termine par une conclusion générale qui résume les connaissances acquises lors de la réalisation de notre projet de fin d'études.

Chapitre 01

*Généralités sur les réseaux
informatiques*

1.1. Introduction

Les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux et en fin des machines terminal, telles que des stations de travail ou des serveurs.

Dans ce premier chapitre, nous allons mettre en revue quelques notions de base, que nous jugeons nécessaire de les rappeler très brièvement pour une meilleure compréhension de l'avancement du sujet posé.

1.2. Un réseau informatique

Un réseau informatique est un ensemble d'équipement matériel et logiciel interconnectés les uns avec les autres dans le but de partager des données.

Il existe deux types de réseaux :

- Le réseau filaire : c'est un réseau qui utilise une connexion avec fil, il utilise des câbles pour relier des ordinateurs et des périphériques.
- Le réseau sans fil : c'est un réseau qui n'utilise pas de câbles, c'est une technique aux particuliers, aux réseaux de télécommunications et aux entreprises de limiter l'utilisation de câbles entre divers localisation [2].

1.3. Objectif d'un réseau informatique [2]

1.3.1. Le partage de ressource

Rendre accessible à une communauté d'utilisateurs des programmes, des données et des équipements informatiques indépendamment de leur localisation.

1.3.2. La fiabilité

Permet le fonctionnement même en cas de problèmes matériels (sauvegardes, duplication, ...).

1.3.3. La réduction des coûts

Les petits ordinateurs (pc par exemple) ont un meilleur rapport prix/performances que les gros. Aujourd'hui, nous trouvons surtout des architecture client/serveur plus économique, plus souple et permettant un déploiement incrémental aisé.

Un réseau est aussi une infrastructure de communication permettant le travail collaboratif et/ou les échanges entre personnes géographiquement séparées.

1.4. Classification des réseaux informatiques

Il existe différents types de réseaux, selon leur taille, leur vitesse de transfert de données ainsi que leur étendue. On peut distinguer trois types de réseaux selon leur étendue :

- LAN (Local Area Network)
- MAN (Metropolitan Area Network)
- WAN (Wide Area Network)



Figure 1.1 : Classification des réseaux.

1.4.1. Les réseaux locaux (LAN)

Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique. La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbit/s et 1Gbit/s (exemple : WIFI) [3].



Figure 1.2 : Réseau local (LAN).

1.4.2. Les réseaux métropolitains (MAN)

Sont des réseaux qui couvrent une métropole (ville), interconnectant plusieurs LAN géographiquement proche à des débits supérieurs à 100Mb/S (exemple : WIMAX) [3].

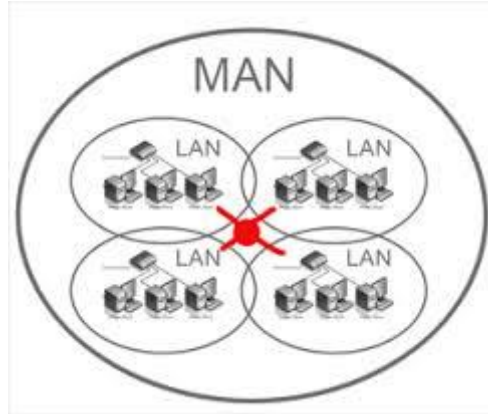


Figure 1.3 : Réseau métropolitain (MAN).

1.4.3. Les réseaux étendus (WAN)

Sont des réseaux de communication de données, couvrent une zone géographique étendu sur des milliers de kilomètre [4].

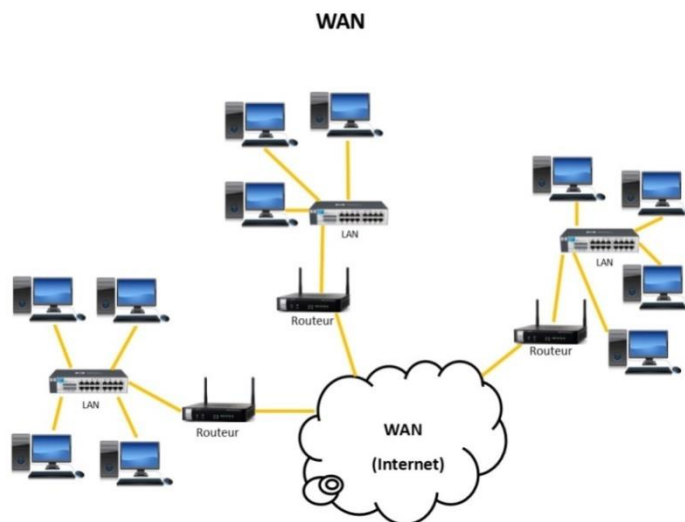


Figure 1.4 : Réseau étendu (WAN).

1.5. Les topologies des réseaux informatiques

Un réseau informatique est constitué d'ordinateurs interconnectés et reliés entre eux, ce type de topologie est appelé la topologie physique. Il existe un autre type de topologie qui s'appelle la topologie logique, elle décrit la manière dont les équipements communiquent [4].

1.5.1. Les topologies physiques

Les plus répandues sont [5] :

a. Topologie en bus

La topologie en bus est la topologie la plus simple d'un réseau. En effet, les machines sont reliées à une même ligne de transmission. Lorsqu'une machine émet des données, la trame circule sur toute la longueur du bus jusqu'à ce qu'elle arrive au destinataire. Une seule station émet en même temps. A chaque extrémité, le réseau est terminé par un bouchon, qui empêche l'apparition de signaux parasites.

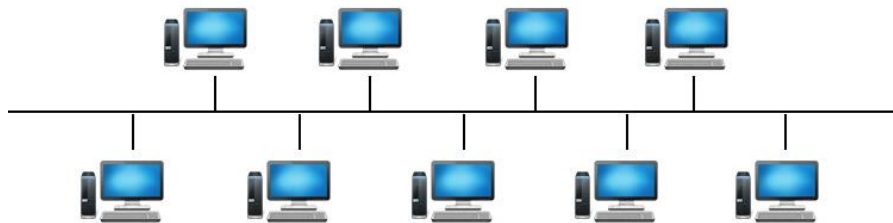


Figure 1.5 : Topologie en bus.

Les avantages :

- Facile à mettre en œuvre ;
- L'ajout d'un terminal n'interrompt pas le fonctionnement du système ;
- La panne d'une station est sans conséquence ;
- Economique en câble ;
- Coût pas cher.

Les inconvénients :

- Temps d'attente imprévisible ;
- Un seul ordinateur peut envoyer un signal à la fois ;
- Défaillance du réseau en cas de panne du support ;
- Performance réduite en cas de charges importantes ;
- Sécurité faible.

b. Topologie en anneau

La topologie en anneau est également l'une des topologies les plus anciennes, développée par IBM (International Business Machines), principalement utilisée par les réseaux Token Ring qui utilise la technique d'accès par jeton. Les données circulent sur l'anneau d'un nœud à l'autre, 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.

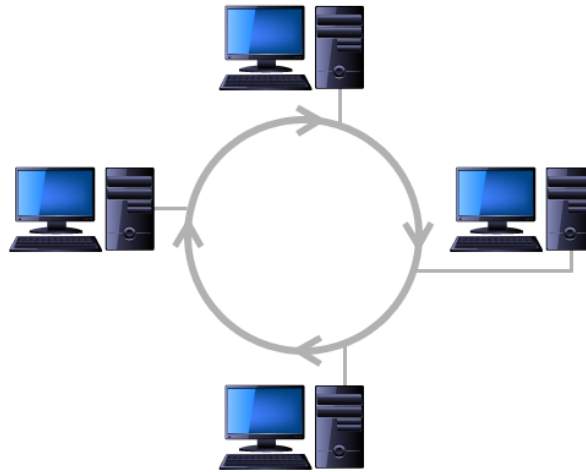


Figure 1.6 : Topologie en anneau.

Les avantages :

- Bonnes performances avec forte charge (bande passante à un débit proche de 90%) ;
- Evite la gestion des collisions ;
- Fonctionne mieux que la topologie en bus ;
- Facile à installer.

Les inconvénients :

- Performance réduite pour chaque nœud supplémentaire ;
- Le retrait ou la panne d'une unité active paralyse le trafic du réseau.

c. Topologie en étoile

La topologie en étoile est la topologie la plus utilisée dans les réseaux locaux. Les câbles sont raccordés à un point central (switch ou hub) par exemple un RJ45.

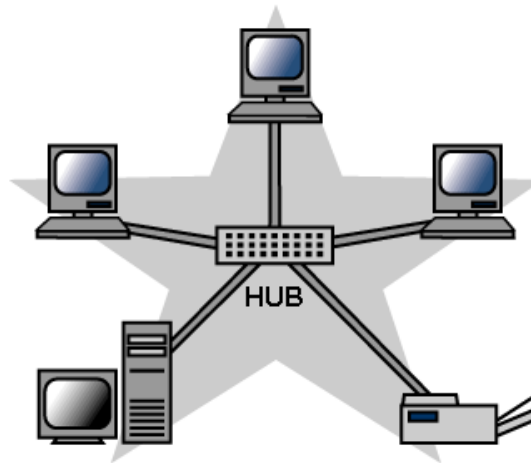


Figure 1.7 : Topologie en étoile.

Les avantages :

- Ajout facile de postes ;
- Localisation facile des pannes ;
- Le débranchement d'une connexion ne paralyse pas le reste du réseau ;
- Les performances sont en fonction du terminal ou du nœud central.

Les inconvénients :

- Repose entièrement sur le nœud central ;
- Coût élevé pour les réseaux étendus.

d. Topologie hybride

La topologie hybride combine une topologie avec une autre. Les topologies hybrides existent en plusieurs types, physique et physique-logique.

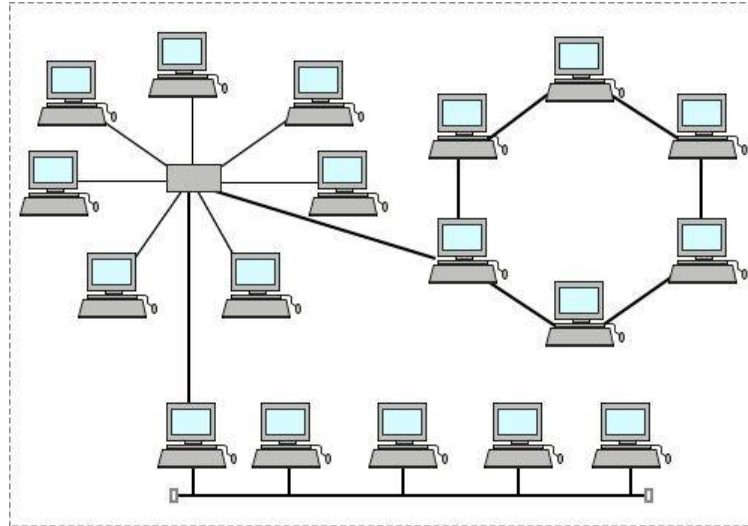


Figure 1.8 : Topologie hybride.

Dans la topologie hybride physique, on dispose d'un réseau contenant deux topologies physiques ou plus au sein du réseau. Par exemple, plusieurs commutateurs au sein d'un même réseau et chacun de ces commutateurs sera relié en tant que bus, mais chaque commutateur donnera une étoile, le résultat est que nous avons une connexion de bus avec des commutateurs et à partir de ces derniers des étoiles logiques.

Dans la topologie hybride physique-logique, on a un réseau qui ressemble physiquement à une topologie, mais fonctionne comme une technologie différente. En d'autres termes les fils sont disposés dans un sens, mais le schéma de données en est un autre. C'est un réseau qui fonctionne comme un anneau, mais il ressemble à une étoile.

e. Topologie maillée

La topologie maillée est adaptée par la plupart des réseaux étendus mais correspond à plusieurs liaisons point à point. Chaque terminal est relié à tous les autres de manière directe ou indirecte. Il n'y a pas d'hierarchie centrale, formant ainsi une structure en forme de filet et l'information peut ainsi parcourir des chemins différents pour arriver au même destinataire, cette méthode garantit le transfert des données en cas de panne d'un nœud.

L'avantage principal de ce type de réseau est qu'il est tolérant aux pannes et très évolutif. L'inconvénient est qu'à chaque fois on ajoute des terminaux le nombre de liaisons, augmente. La topologie maillée se rencontre dans les réseaux de grande distribution par exemple internet.

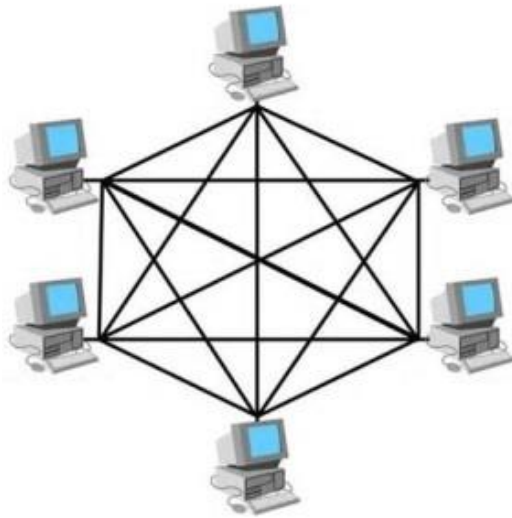


Figure 1.9 : Topologie maillée.

1.5.2. Les topologies logiques

Une topologie logique s'appelle aussi un système de transport réseau. Les éléments d'une topologie logique appartiennent à la couche physique et à la couche liaison de données du modèle OSI (Open System Interconnection).

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

a. Ethernet

Ethernet est un protocole de réseau local (LAN), appelé aussi CSMA/CD (Carrier Sense Multiple Access With Collision Direct), permet aux appareils connectés de communiquer entre eux. La propagation de ces trames est bidirectionnelle, les débits prévus par la norme sont de 1Mbps et maintenant 100Mbps.

Pour qu'une station puisse émettre, elle doit d'abord écouter et vérifier que le média est libre, c'est-à-dire aucune autre station n'émette au même moment. Si une trame est en circulation, alors l'émetteur continue la phase de détection jusqu'à ce que le média soit libre.

Mais si deux ou plusieurs stations tentent de communiquer au même temps, il y aura une collision. Pour gérer ce problème, la norme prévoit une technique des collisions (Collision Detect). Cette technique commence par détecter la collision puis les machines à l'origine de la collision. Les stations arrêtent d'émettre et attendent pendant un certain temps aléatoire puis toutes les stations se remettent en mode d'émission [W1].

b. Token Ring

Le terme 'Token Ring' qui signifie 'anneau à jeton' caractérise la technique liée pour attribuer la parole, est un protocole le plus répandu après Ethernet. Il a été développé par IBM. Le Token Ring utilise la technologie du jeton non adressé sur anneau, chaque station est physiquement reliée à la station précédente et à la suivante, le jeton passe d'une station active en une autre en suivant l'unique sens de transmission prédéfini.

Chaque station de l'anneau reçoit la trame de son prédécesseur et la répète vers son successeur [W1].

1.6. Les architectures des réseaux informatiques

1.6.1. Architecture poste à poste

L'architecture poste à poste appelée aussi égale à égale, permet de mettre en place un réseau à moindre coût, son principe s'agit de relier les postes entre eux en utilisant une topologie physique, sachant que chaque utilisateur du réseau est libre de partager ces ressources et les données ne sont pas centralisées [6].

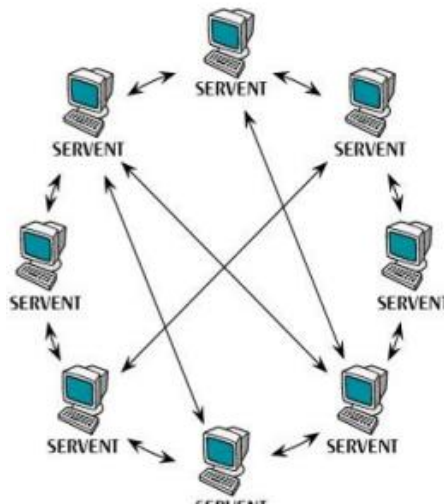


Figure 1.10 : Architecture poste à poste.

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

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

Le réseau poste à poste a énormément d'inconvénient :

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

1.6.2. Architecture client/serveur

C'est la description du processus collaboration entre un serveur et un client.

Les services internet sont conçus selon cette architecture. Ainsi, chaque application est composée de logiciel serveur et logiciel client. A un logiciel serveur peut correspondre plusieurs logiciels clients développés dans différents environnements [7].

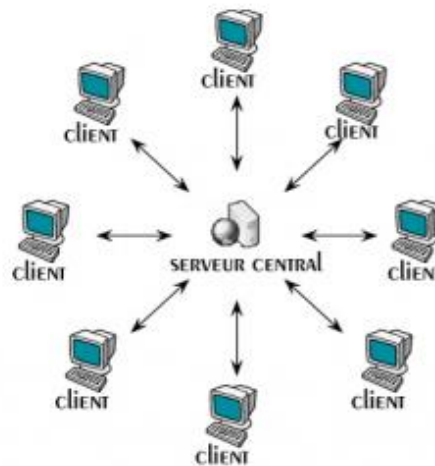


Figure 1.11 : Architecture client/serveur.

L'architecture client/serveur est particulièrement recommandée pour des réseaux nécessitant un grand niveau de fiabilité, ses principaux atouts sont :

Des ressources centralisées : étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs.

- **Meilleure sécurité:** Lors de la connexion un PC client ne voit que le serveur, et non les autres PC clients. De même, les serveurs sont en général très sécurisés contre les attaques de pirates.
- **Facilité d'évolution :** Une architecture client/serveur est évolutive car il est très facile de rajouter ou d'enlever des clients, et même des serveurs.

Inconvénients

Si trop de clients veulent communiquer sur le serveur en même temps, ce dernier risque de ne pas supporter la charge.

Si le serveur n'est plus disponible, plus aucun des clients ne fonctionne (le réseau pair à pair continue à fonctionner, même si plusieurs participants quittent le réseau).

Les coûts de mise en place et de maintenance sont élevés. En aucun cas les clients ne peuvent communiquer entre eux, entraînant une asymétrie de l'information au profit des serveurs [7].

1.7. Les équipements d'interconnexion

Il existe plusieurs équipements réseaux dont :

1.7.1. La carte réseau

La carte réseau (appelée Network Interface Card en anglais et notée NIC) constitue l'interface entre l'ordinateur et le câble du réseau. La fonction d'une carte réseau est de préparer, d'envoyer et de contrôler les données sur le réseau.



Figure 1.12 : Carte réseau.

La carte réseau possède généralement deux témoins lumineux (LEDs) :

- La LED verte correspond à l'alimentation de la carte ;
- La LED orange (10 Mb/s) ou rouge (100 Mb/s) indique une activité du réseau (envoi ou réception de données).

Il existe des cartes réseaux filaires et des cartes réseaux sans fils. la carte réseau travaille au niveau de la couche 2 du modèle OSI [8].

1.7.2. Le répéteur

Permettant de régénérer automatiquement un signal, ce qui permet de prolonger la portée du support. Le répéteur travaille uniquement au niveau physique (couche 1 du modèle OSI) [8].



Figure 1.13 : Répéteur.

1.7.3. Le concentrateur

Le concentrateur (appelé Hub en anglais) est un élément matériel qui permet de relier plusieurs ordinateurs entre eux. Son rôle c'est de prendre les données binaires parvenant d'un port et les diffuser sur l'ensemble des ports [8].



Figure 1.14 : Concentrateur.

1.7.4. Le commutateur (Switch)

Le commutateur réseau est un équipement qui permet de connecter plusieurs appareils sur un même réseau. Sa seule différence avec le Hub, est qu'il est capable de connaître l'adresse physique des machines qui lui sont connectés et d'analyser les trames reçues pour les diriger vers la machine de destination, il travaille au niveau 2 du modèle OSI [9].



Figure 1.15 : Commutateur.

1.7.5. Le pont

Le pont ou bridge c'est un élément réseau capable d'assurer la mise en relation d'un port d'entrer et un port de sortie tout en autorisant la diffusion des messages de Broadcaste et Multicaste.

Le pont est utilisé pour interconnecter deux ou plusieurs segments d'un réseau local de même type, il travaille au niveau 2 du modèle OSI (couche liaison de données) [8].



Figure 1.16 : Le pont.

1.7.6. Le routeur

Le routeur travaille au niveau de la couche 3 du modèle OSI, et s'occupe du routage des unités de données. Il permet d'interconnecter deux réseaux de type différents. C'est l'outil le plus élaboré pour acheminer les données [9].

1.7.7. La passerelle

La passerelle (en anglais Gateway) est un système matériel et logiciel permettant de faire la liaison entre deux réseaux qui peuvent être totalement différents [8].

1.8. Modèles OSI – TCP/IP

Le modèle OSI : est utilisé pour décrire les environnements. Les produits proposés par les fournisseurs pour les réseaux sont conçus d'après les spécifications (règles) de modèle OSI.

Le modèle OSI est un modèle en 7 couches, qui sont réparties en couches hautes, couches intermédiaires et couches basses [2].

Le modèle TCP/IP désigne communément une architecture réseau, ce modèle est étroitement lié à deux protocoles : le protocole TCP (Transmission Control Protocol) qu'on utilise par-dessus un protocole réseau et le protocole IP (Internet Protocol). Ceci est en partie dû au fait que sont les deux protocoles les plus utilisés pour internet, c'est une architecture réseau en quatre couches dans laquelle les protocoles jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante [10].

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

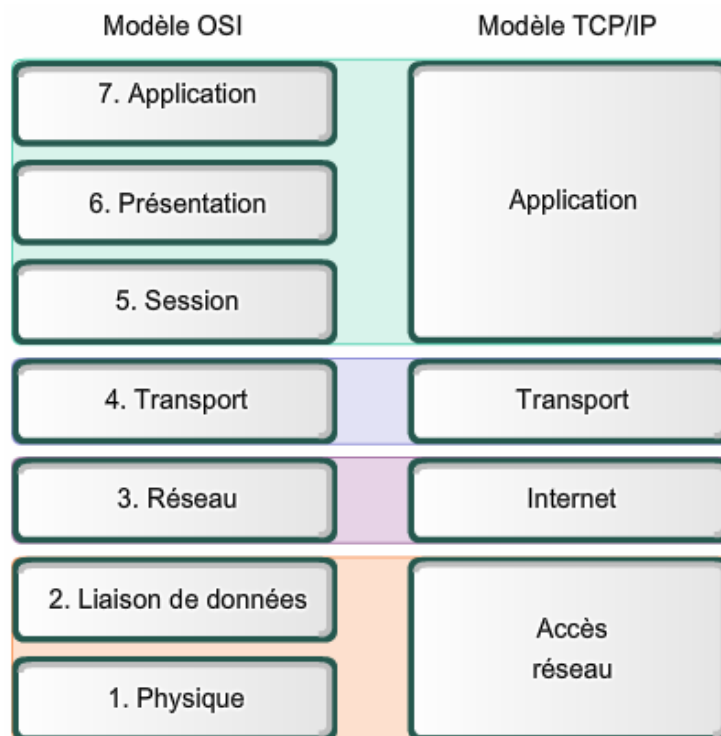


Figure 1.17 : Modèles OSI - TCP/IP.

1.9. Conclusion

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

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

Chapitre 02

Etude du réseau existant

2.1. Introduction

Le réseau d'entreprise permet de relier chaque ordinateur entre eux, via un serveur qui va gérer l'accès à Internet, les e-mails, les droits d'accès aux documents partagés et le travail collaboratif. Chaque utilisateur du réseau se connecte avec un nom d'utilisateur et un mot de passe et est authentifié par le serveur. L'utilisateur peut accéder à ses données et au partage de fichiers.

Dans ce chapitre, nous allons présenter un bref historique sur l'entreprise CEVITAL Bejaia, avec un aperçu global sur les différents départements qui la constituent. De plus, nous allons décortiquer la problématique au tour de laquelle notre projet est principalement axé.

2.2. Partie 1 : l'organisme d'accueil [11]

2.2.1. Présentation de l'entreprise et son historique

CEVITAL est une entreprise privée spécialisée dans la production agro-alimentaire, créé en 1998, sous classification juridique d'une société par action (SPA) dont les principaux actionnaires sont Monsieur ISSAD REBRAB et fils. Implantée au sein du port de Bejaia (Algérie), CEVITAL Agro-industrie est composée 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 a créé 3494 emplois sur 9 ans (1999-2008), soit en moyenne 388 emplois par an, sans compter plusieurs dizaines de milliers d'emplois indirects que génère l'activité de CEVITAL. Elle a plusieurs centaines de sous-traitants, et elle loue chaque jour près de 100 à 200 semi-remorques.

2.2.2. Situation géographique

CEVITAL est implantée au nouveau quai du port de BEJAIA à 3 KM du sud-ouest de cette ville, approximer de la route national 26 soit 280 KM d'Alger, ce qui fait que cet emplacement géographique lui est bénéfique car elle se trouve approximer de l'aéroport, du port de Bejaia, et de la zone industrielle d'AKBOU.

Cet emplacement lui permet aussi de posséder un quai privé, la prédisposant à l'accostage de cargo de 40 000 à 60 000 tonnes.



Figure 2.1 : Image satellitaire de CEVITAL Bejaia.

2.2.3. Organisme de CEVITAL

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

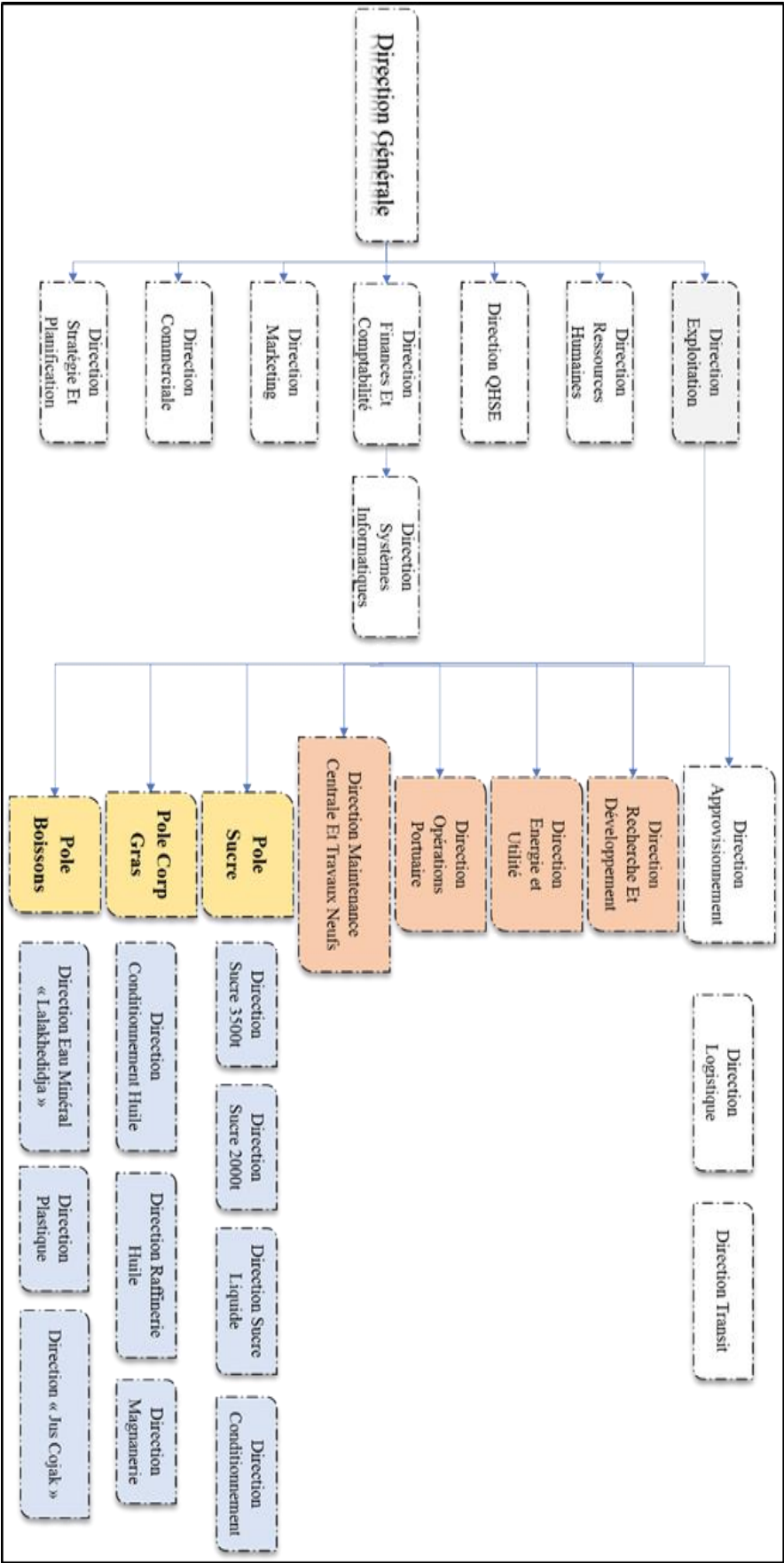


Figure 2.2 : Organigramme de l'organisation administrative de CEVITAL Bejaia.

2.2.4. Architecture du réseau CEVITAL

CEVITAL dispose d'un réseau interne assez vaste permettant de relier les différents bâtiments, unités de production et les directions du complexe. Nous pouvons le décomposer en plusieurs parties : Le backbone (dorsal) du réseau, un pare-feu, une DMZ, une zone de couverture Wi-Fi, un routeur et enfin un data-center (ou sont placés les serveurs de l'entreprise). Le réseau est composé de plusieurs équipements dont la plupart sont de marque Cisco (Switch, Catalyst, Routeur) interconnectés entre eux grâce à la fibre optique, ou paire de cuivre torsadée. Nous tenons à préciser que tout au long de ce manuscrit l'entité CEVITAL désigne pour la plupart des citations le site de Bejaia.

2.3.1. Matériels utilisés dans l'architecture existante

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

C'est la partie centrale du réseau, car elle supporte le trafic de données le plus important du réseau CEVITAL, avec une bande passante très large, sur lequel les commutateurs d'accès, le pare-feu, serveurs et routeurs de l'entreprise y sont connectés. Il s'occupe du routage inter-Vlan. Il permet l'accès à internet via le pare-feu et c'est généralement un serveur DHCP.



Figure 2.4 : Switch Core/ distributeur.

- **Switch d'accès : Cisco Catalyst 2960 et 2950**

Ils sont connectés au backbone et installés dans les différentes sections de l'entreprise.



Figure 2.5 : Switch d'accès.

- **Switch en cascade : Cisco Catalyst 2950 et 2960**

Les différents commutateurs (switchs) de cette couche sont connectés en cascade entre eux et aux switches d'accès, fournissent ainsi l'accès aux réseaux pour les utilisateurs. En outre, sur les switches d'accès, un ensemble de VLANs sont configurés permettant de définir plusieurs sous-réseaux virtuels en fonction des services de l'entreprise.



Figure 2.6 : Switch en cascade.

- **Routeur : Cisco 2900**

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

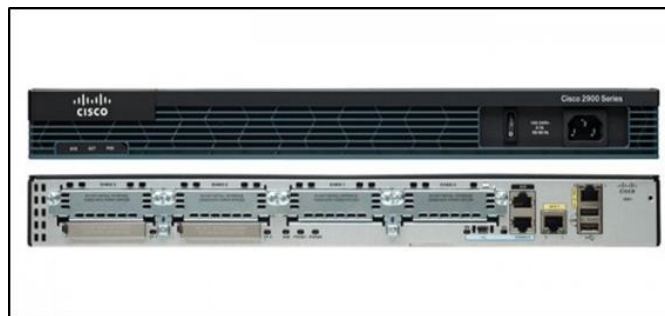


Figure 2.7 : Routeur CISCO 2900.

- **Point d'accès Wi-Fi**

L'entreprise possède plusieurs points d'accès Wi-Fi, créant ainsi une couverture réseau sans fil au niveau de certaines zones du complexe.



Figure 2.8 : Point d'accès WiFi CISCO.

- **Pare feu**

Il existe deux pare-feu liés en redondance et ils permettent de sécuriser le réseau, d'isoler certains segments de celui-ci et enfin la supervision et la sécurisation de l'accès Internet.



Figure 2.9 : Pare feu Palo Alto 3020.

▪ Data-center

La data-center est une pièce sécurisée, l'accès est restreint, car seul les responsables et les techniciens de la DSI (Direction Système d'Information) ont accès. En outre, une climatisation des équipements est aussi assurée grâce au contrôle de la température par un système d'air conditionné avec une alimentation électrique doublée pour veiller à son fonctionnement sans coupure.

En fait, le data-center de CEVITAL est le noyau central du réseau de l'entreprise où se trouvent les équipements suivants,

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

2.3.2. Les liaisons inter-sites

Afin d'assurer le partage des ressources et une communication interne au sein de l'entreprise, CEVITAL dispose des connexions qui permettent de relier le site de Bejaïa aux différents annexes de l'entreprise à savoir,

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

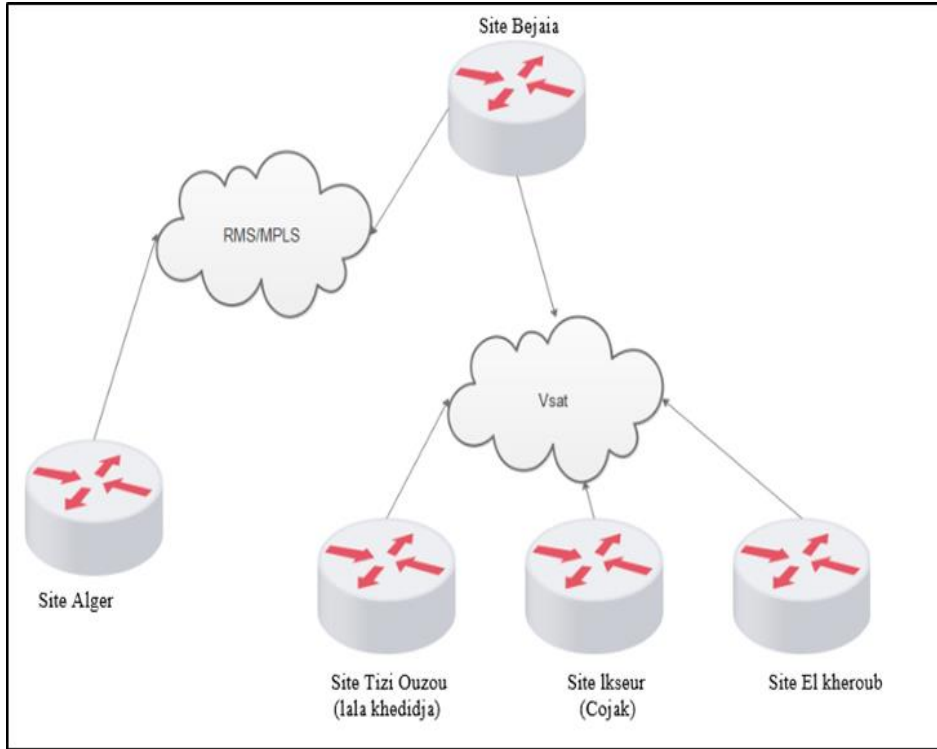


Figure 2.10 : Connexion inter-sites du site CEVITAL Bejaia.

2.3.3. Vlan de l'entreprise

L'administrateur réseau a divisé le réseau en plusieurs VLANs selon différentes divisions, un VLAN-Management a été créé pour permettre l'administration (configuration, mise à jour et équipement de sauvegarde) du réseau distant.

L'adressage utilisé dans l'architecture est de classe A, divisé en sous-réseaux **10.10.0.0/24**. Le tableau suivant présente la liste des VLAN,

VLAN		Description
ID	NOM	
10	Direction	Direction
11	Margarinerie	Raffinerie de Margarine
12	Server2	/
13	Vision	Equipements de visioconférence
14	Management	/

15	Commercial	/
16	DFC	Direction Finances et Comptabilité
17	DG	Direction Générale
18	QHSE	Département de Qualité Hygiène et Sécurité et Environnement
19	Sucre3500T	Raffinerie de Sucre
20	GEUST	Réseau destiné aux utilisateurs non employé par CEVITAL
21	CEVITAL-WIFI	Wifi destiné au collaborateur de CEVITAL
22	Controle-Acces	/
23	NUMILOG	/
24	MOBILE-WIFI	Wifi téléphonique
25	Firewall-Datacenter	Pare-feu du Datacenter

Tableau 2.1 : Liste des VLANs de l'entreprise.

2.3.4. Utilisation du réseau informatique

L'entreprise de CEVITAL compte au moins mille utilisateurs du réseau informatique ; ces différents collaborateurs utilisent chaque jour divers applications et service offerts par le réseau pour permettre le bon fonctionnement de leurs travaux. Nous pouvons citer les applications et services suivants :

- Applications de gestion de production assistée par ordinateur ;
- Partage des documents via un serveur dédié (cloud privé) ;
- Service postal ;
- Compatibilité des applications et gestion des stocks ;
- Donne accès aux collaborateurs.

2.3.5. Critique de l'existant

Après avoir décortiqué le réseau de CEVITAL, en l'occurrence le réseau informatique existant, de nombreuses insuffisances ont été découvertes. Ceci nous a permis de définir un

nombre important de contraintes fonctionnelles, cependant celles-ci peuvent réduire significativement les performances du réseau existant, voir même des dysfonctionnements fréquents. Les constats résultants de notre étude par rapport au réseau existant sont les suivants :

- Un seul backbone centralise le réseau, ce qui implique la surcharge de ce dernier,
- La liaison en cascade des switches limite la bande passante, ce qui ralentit davantage les applications en place, les ressources et une simple défaillance logicielle ou matérielle de l'un des switches couperait la connexion au réseau pour tous les utilisateurs,
- Absence de serveurs en redondance qui assurera la tolérance aux pannes et garantira des liaisons secours aux équipements, d'ailleurs cela induit plusieurs points de défaillances dans l'architecture du réseau.

2.3.6. Problématique

La gestion et la maintenance des réseaux informatiques, en particulier ceux de grandes entreprises, indiquent qu'il est important d'assurer leur continuels bon fonctionnement et la continuité du réseau, assurant ainsi des services de collecte, de stockage, de traitement et de communication d'informations parmi les employés qui non seulement représentent un grand nombre mais sont également répartis sur plusieurs sites.

D'autre part, sinon cela ralentira ou arrêtera ses activités et affectera négativement la bonne performance de son équipe et sa productivité.

L'infrastructure du réseau d'entreprise, devient alors vitale pour CEVITAL, ceci dit, comment assurer la continuité et le bon fonctionnement du réseau CEVITAL, quelle topologie, et comment faire face aux pannes d'un ou plusieurs équipements matériels ou logiciels ?

2.3.7. Propositions

Afin de remédier aux problèmes cités dans les constats annoncés auparavant, nous proposons les solutions suivantes :

- ✓ Utiliser une architecture redondante en utilisant deux backbones interconnectés en redondances avec un protocole de routage au niveau du cœur du réseau afin de minimiser le nombre des switches branchés en cascade.

- ✓ Utiliser un protocole de hautes disponibilités afin de régler le problème de défaillance d'un ou plusieurs équipements.

2.3.8. Solution optée

D'après les critiques précédentes, nous étions convaincus que la solution la plus appropriée est d'utiliser une architecture à quatre switch de niveau 3 améliorée avec le protocole de routage EIGRP, en plus d'un protocole de haute disponibilité au niveau de la distribution, nous avons donc choisi HSRP. De plus, nous avons décidé de réduire les switches connectés en cascade, en connectant le plus grand nombre de switch aux backbones de distribution.

2.3. Partie 2 : La haute disponibilité

2.3.1. La redondance

Ce que les entreprises recherchent de nos jours, c'est un réseau fiable et disponible à tout moment. Une telle solution n'est pas forcément très simple à mettre en place, de plus elle peut être relativement coûteuse pour l'entreprise. Le mieux est d'avoir un réseau qui supporte la charge sans interruption d'utilisation et une redondance de pannes. Cela signifie avoir plusieurs appareils qui remplissent la même fonction, tout en étant aussi transparent que possible pour les utilisateurs.

2.3.2. Les protocoles de redondance

Les protocoles réseau transportent les données d'application sur un réseau d'entreprise. Ces protocoles sont basés sur l'architecture réseau qui fournit la hiérarchie, les adresses et les informations de topologie pour les périphériques clients. La passerelle ou le routeur multi-protocole fournit toutes ces informations. Les postes de travail, les routeurs et les serveurs de fichiers doivent communiquer entre eux, à cet effet, les protocoles ont mis en œuvre des méthodes de recherche pour trouver et stocker l'adresse de la passerelle [W2].

a. HSRP (Hot Standby Router Protocol)

HSRP est un protocole de Cisco pour assurer la haute disponibilité de la passerelle réseau, ce protocole peut être mis en place sur un routeur ou un commutateur de niveau 3. L'objectif est qu'une défaillance potentielle du routeur ne perturbe pas le routeur. Il se met en

place en regroupant le fonctionnement de plusieurs routeurs physiques (au moins 2) qui se prennent automatiquement en charge entre eux, c'est-à-dire d'un routeur à un autre [12].

- **Fonctionnement de HSRP [W3]**

Le protocole HSRP permet aux routeurs situés dans un même groupe que l'on nomme « standby group » de former un seul routeur virtuel qui sera l'unique passerelle des hôtes du réseau local. En se cachant derrière ce routeur virtuel aux yeux des hôtes, les routeurs garantissent en effet qu'il y est toujours un routeur qui assure le travail de l'ensemble du groupe. Un routeur dans ce groupe est donc désigné comme « actif » et c'est lui qui fera passer les requêtes d'un réseau à un autre. Pendant que le routeur « actif » travaille, il envoie également des messages aux autres routeurs indiquant qu'il est toujours opérationnel. Si le routeur principal (élu actif) vient de tomber en panne, il sera automatiquement remplacé par un routeur qui était alors jusqu'à présent passif et lui aussi membre du groupe HSRP. Aux yeux des utilisateurs toutefois, cette réélection et ce changement de passerelle le routeur virtuel que forment les routeurs membres du groupe HSRP. Le routeur virtuel aura donc toujours la même adresse IP et adresse MAC aux yeux des hôtes du réseau même si en réalité il y a un changement du chemin par lequel transitent les paquets.

Afin d'illustrer cela, nous allons schématiser la vision que les hôtes auront du réseau ainsi que l'état réel du réseau.

Ce que voient les hôtes du réseau :

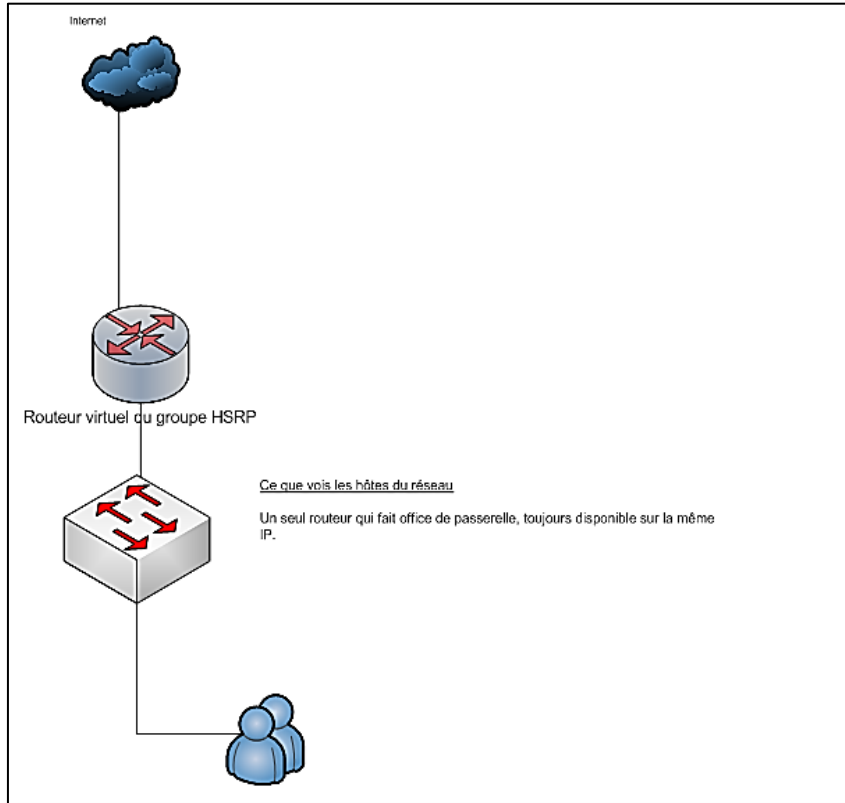


Figure 2.11 : Le protocole HSRP vue d'un hôte du réseau.

L'état réel du réseau :

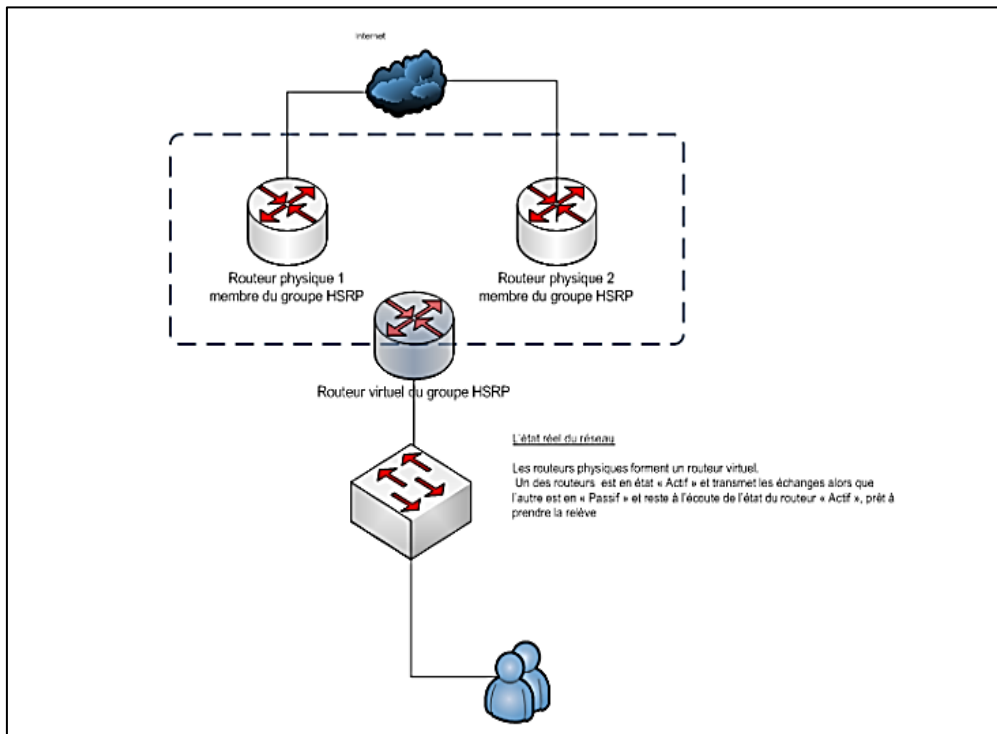


Figure 2.12 : le schéma physique et virtuel d'un réseau HSRP.

b. VRRP (Virtual Router Redundancy Protocol)

Le protocole VRRP élimine le point de défaillance unique inhérent à l'environnement de routage virtuel et statique. VRRP définit un protocole d'élection qui attribue dynamiquement des responsabilités pour un routeur virtuel à un hub VPN provenant d'un LAN. Le routeur VRRP, qui contrôle les adresses IP associées au routeur virtuel, est appelé le routeur maître et les transferts de paquets sont transmis à ses propres adresses IP. Lorsque le programme principal n'est pas disponible, un condensateur VPN de secours remplace le maître [W3].

c. GLBP (Gateway Load Blancing Protocol)

Il s'agit d'un protocole propriétaire Cisco qui inclut les concepts de base de HSRP et VRRP. Contrairement à ces deux protocoles, tous les routeurs du groupe GLBP sont activement impliqués dans le routage alors qu'en VRRP ou HSRP il n'y en a qu'un en mode actif, tandis que les autres sont en attente. Plus spécifiquement, au sein du groupe GLBP, le routeur de priorité la plus élevée ou l'adresse IP la plus élevée du groupe prendra le statut « AVG » (Active Virtual Gateway). Ce routeur interceptera toutes les requêtes ARP faites par les clients pour l'adresse MAC de la passerelle par défaut, et grâce à son algorithme d'équilibrage de charge préconfiguré, il retournera l'adresse MAC virtuelle de l'un des routeurs du groupe GLBP. De plus, le routeur AVG est celui qui attribuera les adresses MAC virtuelles aux routeurs de groupe, ils ont donc le statut « AVF » (Active Virtual Forwarder). Un maximum de 4 adresses MAC par défaut, elles sont définies par groupe, tandis que d'autres routeurs ont des rôles de sauvegarde en cas de panne d'AVF [W3].

2.3.3. STP (Spanning Tree Protocol)

Le protocole STP est un protocole de couche 2 qui est conçu pour les commutateurs. Il crée un chemin sans boucles car elles sont fatales au réseau et permet de garder une topologie physique redondante.

Avec STP, il est impératif que tous les commutateurs du réseau choisissent un pont, la racine qui deviendra le point central du réseau. Toutes les autres décisions relatives au réseau, telles que le port à bloquer ou le port à déplacer en mode de transfert, est pris à partir de ce pont racine. Un environnement commuté, qui diffère de l'environnement de pont, gère à la place plusieurs VLAN. Lorsqu'un pont racine est implémenté dans un réseau commuté, il le fait il agit généralement comme une clé racine. Chaque VLAN doit avoir son propre pont racine car

chacun d'eux est un domaine de diffusion distinct. Les VLAN peuvent être enracinés différemment ils sont tous contenus dans une ou plusieurs commutateur(s).

Tous les commutateurs échangent des informations concernant la sélection de commutateur racine et configuration réseau ultérieure. Les BPDU (Bridge Protocol Data Units) diffusent cette information. Chaque commutateur compare les paramètres BPDU qu'il envoie à un voisin avec les paramètres BPDU qu'il reçoit de ce voisin [13].

2.3.4. EtherChannel

EtherChannel est une technologie d'agrégation de liens qui combine plusieurs liaisons Ethernet physiques identiques en une seule liaison logique. L'objectif est d'augmenter la vitesse et la tolérance aux pannes entre les commutateurs, les routeurs et les serveurs. Il simplifie la topologie Spanning Tree en diminuant le nombre de liens [12].

2.3.5. VTP (VLAN Trunking Protocol)

VTP permet d'ajouter, renommer ou supprimer un ou plusieurs réseaux locaux virtuels sur un seul commutateur (le serveur) qui propagera cette nouvelle configuration à l'ensemble des autres commutateurs du réseau (clients). VTP permet ainsi d'éviter toute incohérence de configuration des VLAN sur l'ensemble d'un réseau local.

VTP fonctionne sur les commutateurs Cisco dans un de ces 3 modes :

- Client ;
- Serveur ;
- Transparent.

Les administrateurs peuvent changer les informations de VLAN sur les commutateurs fonctionnant en mode serveur uniquement. Une fois que les modifications sont appliquées, elles sont distribuées à tout le domaine VTP au travers des liens « trunk ». En mode transparent, le switch reçoit les mises à jour et les transmet à ses voisins sans les prendre en compte. Il peut créer, modifier ou supprimer ses propres VLAN mais ne les transmet pas. Les switches en mode client appliquent automatiquement les changements reçus du domaine VTP [14].

2.3.6. Les protocoles de routage

Un protocole de routage est un système de communication utilisé entre les routeurs, il permet de partager des informations entre ces derniers. Les protocoles de routage aident à construire et à mettre à jour une table de routage. On en trouve plusieurs tel que RIP, EIGRP et OSPF [15].

a. RIP (Routing Information Protocol)

Le RIP est un protocole de routage IP de type vecteur distance, il permet à chaque router de communiquer aux routeurs voisins. Il utilise le nombre de saut pour calculer la valeur de la mesure, qui détermine le meilleur chemin pour atteindre un réseau.

b. EIGRP (Enhanced Interior Gateway Routing Protocol)

EIGRP est un protocole de routage propriétaire développé par Cisco à partir du protocole IGRP original. Par conséquent, EIGRP ne peut être utilisé que sur des équipements Cisco, mais est en partie devenu un protocole, EIGRP est un protocole de routage à vecteur de distance IP, avec une amélioration pour réduire l'instabilité de routage due au changement également. La topologie de la bande passante du routeur et la consommation d'énergie du processeur.

c. OSPF (Open Shortest Path First)

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

2.4. Conclusion

Ce chapitre est globalement axé sur la présentation de l'organisme d'accueil, en l'occurrence le site de CEVITAL Bejaia. Cependant, dans la première partie de ce chapitre, nous avons pu donner un aperçu de CEVITAL, nous avons mis en avant un problème qui nous a amené à proposer une solution. Ce dernier se résume essentiellement à proposer une nouvelle architecture ainsi qu'à mettre en œuvre la haute disponibilité.

La deuxième partie de ce chapitre est consacrée à la définition des différents protocoles utilisés lors de notre projet et à la compréhension du processus, ainsi que des avantages qu'il apporte au réseau.

Chapitre 3
Installation et
configuration du
réseau CEVITAL

3.1. Introduction

Dans ce chapitre, nous allons présenter les différentes configurations nécessaires à la mise en œuvre d'un nouveau réseau LAN, basé sur le simulateur Cisco Packet Tracer 7.2.1.

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

3.2. Présentation du simulateur

Packet Tracer est un logiciel open source autorisant à construire un réseau physique virtuel, et de simuler les comportements des protocoles sur une quelconque topologie de réseau. Le simulateur permet aux utilisateurs de créer et de configurer leurs propres réseaux à l'aide des équipements Cisco avant de passer à la configuration réelle.

La figure 3.1, ci-contre montre un aperçu général de Packet Tracer, dont on définit les zones :

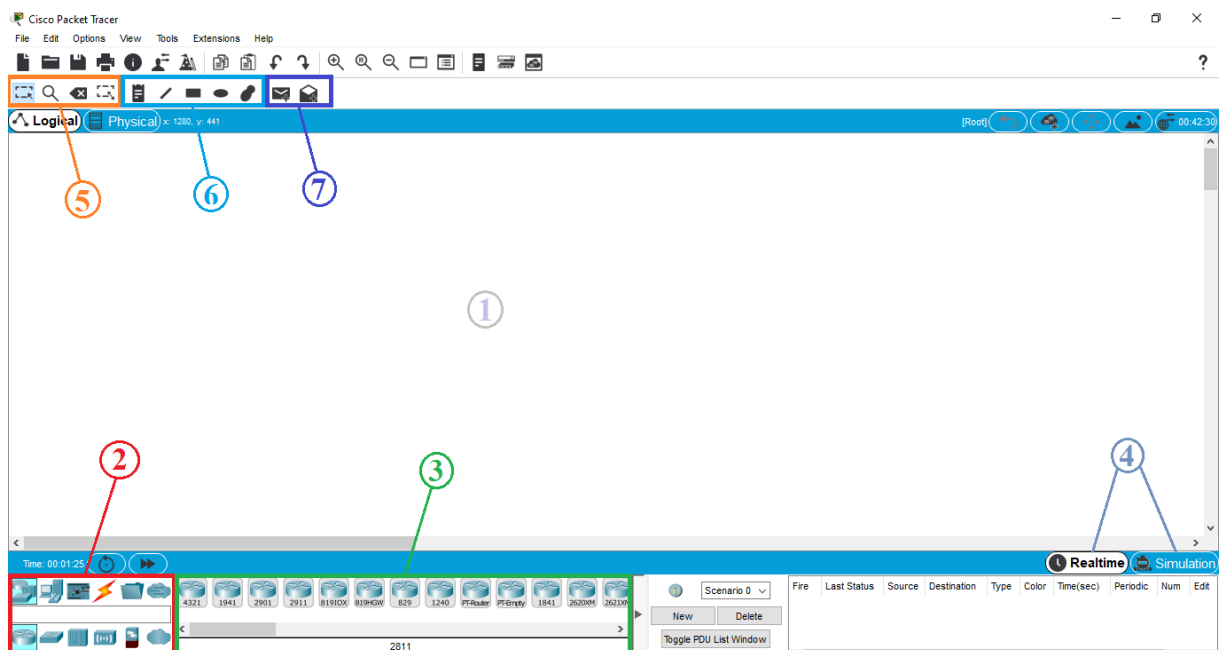


Figure 3.1 : Capture de l'interface du simulateur Cisco Packet Tracer 7.2.1.

Zone 1 : la partie dans laquelle le réseau est construit ;

Zone 2 : la partie où le type des équipements sont choisis ;

Zone 3 : la partie où les équipements sont choisis ;

Zone 4 : permet de passer du mode réel au mode simulation ;

Zone 5 : contient un ensemble d'outils (sélection, inspection, suppression et redimensionner la forme) ;

Zone 6 : contient l'annotation du schéma et des palettes de dialogues ;

Zones 7 : concerne les tests de communication (envoi de la trame et personnalisation de la trame).

3.3. Présentation du réseau

3.3.1. Segmentation du réseau en VLAN

Le réseau a été divisé en plusieurs section chacune représentent un VLAN. Par conséquent, il y'aura naissance de 16 VLANs à savoir :

- DIRECTION,
- MARGARINERIE,
- SERVER2,
- VISION,
- MANAGMENT,
- COMERCIAL,
- DFC,
- DG,
- QHCE,
- SUCRE3500T,
- GUST,
- CEVITAL-WIFI,
- CONTROL-ACCESS,
- NUMILOG,
- MOBILE-WIFI,
- Firewall-Datacenter.

3.3.2. Adressage des VLANs

Nom des VLAN	VLAN-ID	Adresse sous-réseau	Masque sous-réseau	Description
DIRECTION	10	10.10.10.0/24	255.255.255.0	Direction
MARGARINERIE	11	10.10.11.0/24	255.255.255.0	Raffinerie de margarine
SERVER2	12	10.10.12.0/24	255.255.255.0	/
VISION	13	10.10.13.0/24	255.255.255.0	Equipements de visioconférence
MANAGEMENT	14	10.10.14.0/24	255.255.255.0	/
COMMERCIAL	15	10.10.15.0/24	255.255.255.0	/
DFC	16	10.10.16.0/24	255.255.255.0	Direction Finance Comptabilité
DG	17	10.10.17.0/24	255.255.255.0	Direction Générale
QHSE	18	10.10.18.0/24	255.255.255.0	Département de Qualité Hygiène et Sécurité et Environnement
SUCRE3500T	19	10.10.19.0/24	255.255.255.0	Raffinerie de sucre
GEUST	20	10.10.20.0/24	255.255.255.0	Réseau destiné aux utilisateurs non employé par CEVITAL
CEVITAL-WiFi	21	10.10.21.0/24	255.255.255.0	WiFi destiné aux collaborateurs de CEVITAL
CONTROL-ACCES	22	10.10.22.0/24	255.255.255.0	/
NUMILOG	23	10.10.23.0/24	255.255.255.0	/
MOBILE-WiFi	24	10.10.24.0/24	255.255.255.0	WiFi téléphonique
Firewall-Datacenter	25	10.10.25.0/24	255.255.255.0	Pare-feu du Datacenter

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 déjà en place :

- La création des vlan et ces interfaces,
- La configuration du protocole DHCP,
- La configuration de lien Trunk,

- La configuration de VTP.

3.4.1. Architecture de mise en œuvre

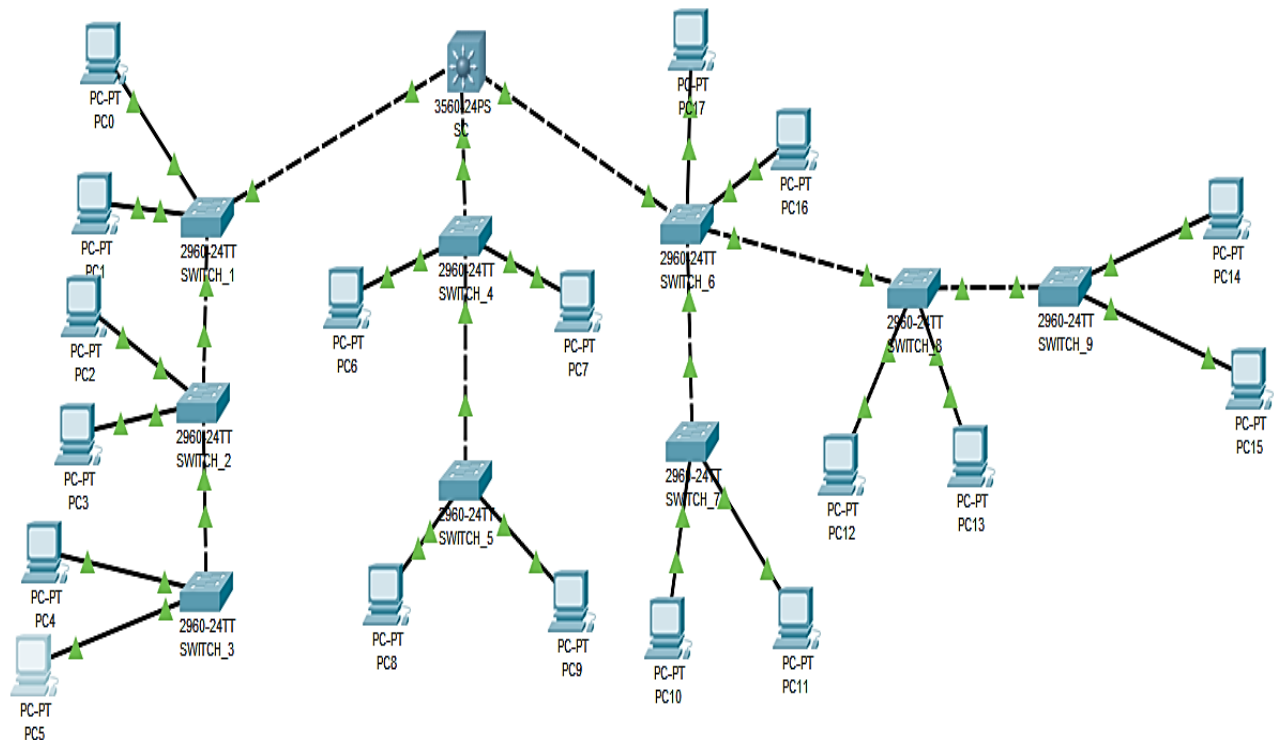


Figure 3.2 : Architecture du réseau local existant.

3.4.2. Configuration des équipements

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

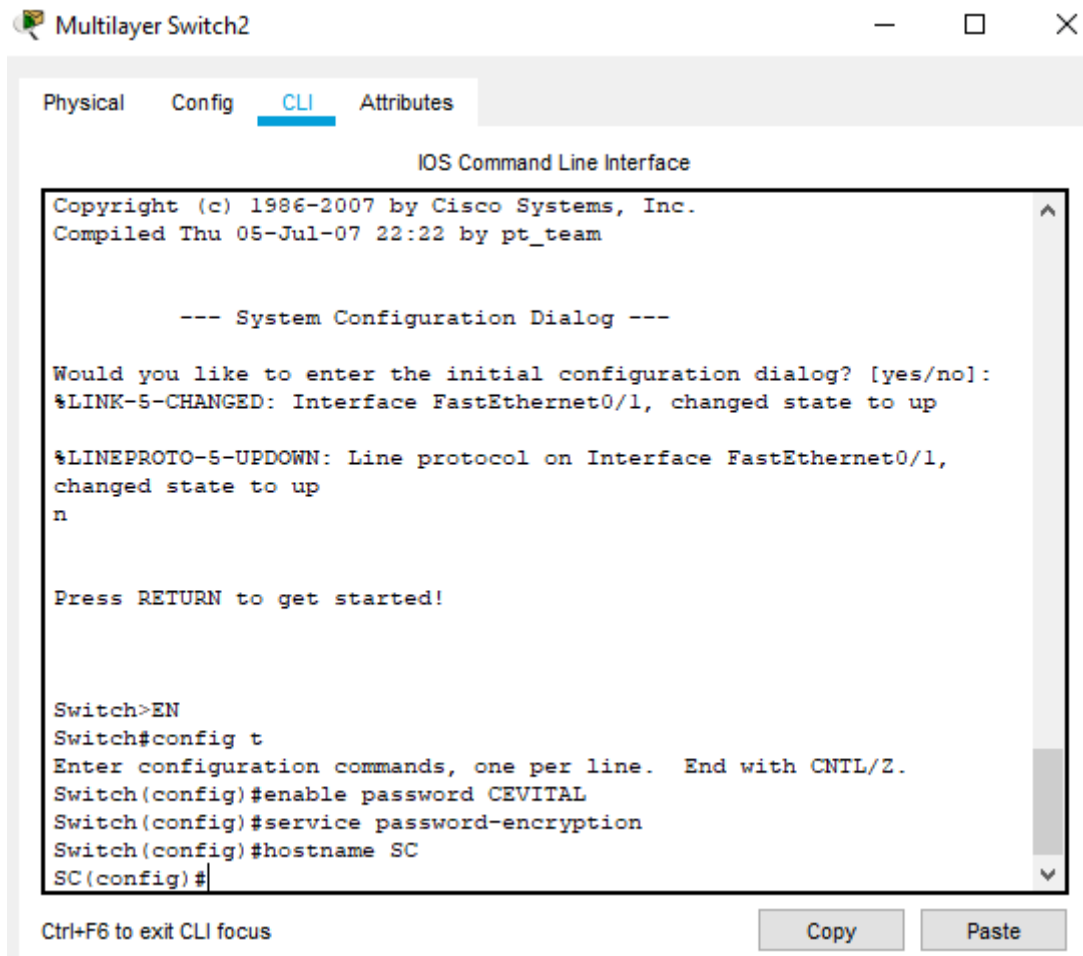
Lorsqu'un équipement est ajouté, il est possible de le configurer en cliquant dessus, une fois ajouté dans le réseau. Une nouvelle fenêtre s'ouvre comportant différents onglets : Physical, config, desktop, CLI ... etc.

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

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

a. Configuration des Hostname et sécurité

Cette configuration consiste à renommer les équipements par des noms significatifs, prenons comme exemple la nomination d'un switch Core ainsi que le sécuriser avec un mot de passe et le crypter afin de limiter l'accès aux personnes étrangères. La figure 3.3 ci-dessous l'explique.



```
Multilayer Switch2
Physical Config CLI Attributes
IOS Command Line Interface
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 05-Jul-07 22:22 by pt_team

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
n

Press RETURN to get started!

Switch>EN
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#enable password CEVITAL
Switch(config)#service password-encryption
Switch(config)#hostname SC
SC(config)#
```

Figure 3.3 : Configuration du Hostname et mot de passe.

b. Création des VLANs

La création des VLANs se fait au niveau du switch Multilayer comme le montre la figure 3.4 suivante sur la création de certains VLANs mis en place.

```
SC(config)#vlan 10
SC(config-vlan)#name Direction
SC(config-vlan)#exit
SC(config)#vlan 11
SC(config-vlan)#name Margarinerie
SC(config-vlan)#exit
SC(config)#vlan 12
SC(config-vlan)#name Server2
SC(config-vlan)#exit
SC(config)#vlan 13
SC(config-vlan)#name Vision
SC(config-vlan)#exit
SC(config)#vlan 14
SC(config-vlan)#name Management
SC(config-vlan)#exit
SC(config)#vlan 15
SC(config-vlan)#name Commercial
SC(config-vlan)#exit
SC(config)#vlan 16
SC(config-vlan)#name DFC
SC(config-vlan)#exit
SC(config)#vlan 17
SC(config-vlan)#name DG
SC(config-vlan)#exit
```

Figure 3.4 : Création des VLANs.

c. Configuration des interfaces VLANs

La configuration des interfaces virtuelles de VLANs est faite au niveau de Switch Core (SC) en attribuant une adresse IP à chaque interface. La figure 3.5, illustre le principe de configuration de ces interfaces pour quelques VLANs.

```
SC(config)#interface vlan 10
SC(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

SC(config-if)#ip address 10.10.10.254 255.255.255.0
SC(config-if)#exit
SC(config)#interface vlan 11
SC(config-if)#
%LINK-5-CHANGED: Interface Vlan11, changed state to up

SC(config-if)#ip address 10.10.11.254 255.255.255.0
SC(config-if)#exit
SC(config)#interface vlan 12
SC(config-if)#
%LINK-5-CHANGED: Interface Vlan12, changed state to up

SC(config-if)#ip address 10.10.12.254 255.255.255.0
SC(config-if)#exit
SC(config)#interface vlan 13
SC(config-if)#
%LINK-5-CHANGED: Interface Vlan13, changed state to up

SC(config-if)#ip address 10.10.13.254 255.255.255.0
SC(config-if)#exit
SC(config)#interface vlan 14
SC(config-if)#
%LINK-5-CHANGED: Interface Vlan14, changed state to up

SC(config-if)#ip address 10.10.14.254 255.255.255.0
SC(config-if)#exit
SC(config)#interface vlan 15
SC(config-if)#
%LINK-5-CHANGED: Interface Vlan15, changed state to up

SC(config-if)#ip address 10.10.15.254 255.255.255.0
SC(config-if)#exit
```

Figure 3.5 : Configuration des interfaces VLANs.

d. Configuration du DHCP

Le DHCP consiste à attribuer dynamiquement les adresses IP aux hôtes connectés, au lieu de les configurer manuellement sur chaque poste utilisateur. La figure 3.6, montre les commandes permettant d'activer ce protocole.

```
SC(config)#ip dhcp pool VLAN_Direction
SC(dhcp-config)#network 10.10.10.0 255.255.255.0
SC(dhcp-config)#default-router 10.10.10.254
SC(dhcp-config)#
```

Figure 3.6 : Configuration du DHCP.

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

```
!  
ip dhcp pool VLAN_Direction  
  network 10.10.10.0 255.255.255.0  
  default-router 10.10.10.254  
ip dhcp pool VLAN_Margarinerie  
  network 10.10.11.0 255.255.255.0  
  default-router 10.10.11.254  
ip dhcp pool VLAN_Server2  
  network 10.10.12.0 255.255.255.0  
  default-router 10.10.12.254  
ip dhcp pool VLAN_Vision  
  network 10.10.13.0 255.255.255.0  
  default-router 10.10.13.254  
ip dhcp pool VLAN_Management  
  network 10.10.14.0 255.255.255.0  
  default-router 10.10.14.254  
ip dhcp pool VLAN_Commercial  
  network 10.10.15.0 255.255.255.0  
  default-router 10.10.15.254  
ip dhcp pool VLAN_DFC  
  network 10.10.16.0 255.255.255.0  
  default-router 10.10.16.254  
ip dhcp pool VLAN_DG  
  network 10.10.17.0 255.255.255.0  
  default-router 10.10.17.254  
ip dhcp pool VLAN_QHSE  
  network 10.10.18.0 255.255.255.0  
  default-router 10.10.18.254  
ip dhcp pool VLAN_Sucre3500T  
  network 10.10.19.0 255.255.255.0  
  default-router 10.10.19.254  
ip dhcp pool VLAN_GEUST  
  network 10.10.20.0 255.255.255.0  
  default-router 10.10.20.254  
ip dhcp pool VLAN_Cevital_WiFi  
  network 10.10.21.0 255.255.255.0  
  default-router 10.10.21.254  
ip dhcp pool VLAN_Controle_Acces  
  network 10.10.22.0 255.255.255.0  
  default-router 10.10.22.254  
ip dhcp pool VLAN_NUMILOG  
  network 10.10.23.0 255.255.255.0  
  default-router 10.10.23.254  
ip dhcp pool VLAN_MOBILE_WiFi  
  network 10.10.24.0 255.255.255.0  
  default-router 10.10.24.254  
ip dhcp pool VLAN_Firewall_Datacenter  
  network 10.10.25.0 255.255.255.0  
  default-router 10.10.25.254  
'
```

Figure 3.7 : Vérification de l'activation du DHCP.

e. Configuration des liens Trunk

Le lien Trunk est un mode d'accès qui permet à plusieurs VLANs de passer par une seule liaison physique. En effet, la plupart des liaisons entre l'ensemble des switch d'accès et le switch Core sont en mode Trunk.

```
SC(config)#interface fa 0/1
SC(config-if)#switchport trunk encapsulation dot1q
SC(config-if)#description TO_SWITCH_1
SC(config-if)#description TO_SWITCH_2
SC(config-if)#description TO_SWITCH_3
SC(config-if)#exit
SC(config)#interface fa 0/2
SC(config-if)#switchport trunk encapsulation dot1q
SC(config-if)#description TO_SWITCH_4
SC(config-if)#description TO_SWITCH_5
SC(config-if)#exit
SC(config)#interface fa 0/3
SC(config-if)#switchport trunk encapsulation dot1q
SC(config-if)#description TO_SWITCH_6
SC(config-if)#description TO_SWITCH_7
SC(config-if)#description TO_SWITCH_8
SC(config-if)#description TO_SWITCH_9
SC(config-if)#exit
```

Figure 3.8 : Configuration des interfaces du switch Core en mode Trunk.

f. Attribution des ports des commutateurs au VLANs

Cette opération se fait au niveau des switches d'accès, chaque port appartiendra à un VLAN donné. Les commandes suivantes nous permettent d'associer les ports aux VLANs en mode Access.

```
SWITCH_1(config)#interface fa 0/3
SWITCH_1(config-if)#switchport mode access
SWITCH_1(config-if)#switchport access vlan 10
SWITCH_1(config-if)#exit
SWITCH_1(config)#interface fa 0/4
SWITCH_1(config-if)#switchport mode access
SWITCH_1(config-if)#switchport access vlan 11
SWITCH_1(config-if)#exit
SWITCH_1(config)#exit
```

Figure 3.9 : Configuration des interfaces du switch en mode Access.

g. Configuration du protocole VTP

Le Switch-Core (SC) sera configuré comme VTP serveur, c'est lui qui va gérer l'administration de l'ensemble des VLANs. La figure 3.10, illustre la configuration du protocole VTP au niveau de SC.

```
SC(config)#vtp mode server
Device mode already VTP SERVER.
SC(config)#vtp domain CEVITAL.COM
Changing VTP domain name from NULL to CEVITAL.COM
SC(config)#vtp password CEVITAL
Setting device VLAN database password to CEVITAL
SC(config)#exit
```

Figure 3.10 : Configuration du VTP server

h. Configuration du protocole VTP sur le switch d'accès :

Le switch d'accès sera configuré comme VTP client, tel qu'il est donné par la figure 3.11.

```
SWITCH_1(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWITCH_1(config)#vtp domain CEVITAL.COM
Domain name already set to CEVITAL.COM.
SWITCH_1(config)#vtp password CEVITAL
Setting device VLAN database password to CEVITAL
```

Figure 3.11 : Configuration du VTP client

3.4.3. Vérification des adressages IP attribués par le DHCP

La vérification s'effectue pour tous les ordinateurs, la figure 3.12 ci-dessous nous montre un exemple :

The screenshot shows a network configuration window with several tabs: Physical, Config, Desktop (selected), Programming, and Attributes. The DHCP configuration section is active, showing the following settings:

- DHCP (selected) and Static
- IP Address: 10.10.14.2
- Subnet Mask: 255.255.255.0
- Default Gateway: 10.10.14.254
- DNS Server: 0.0.0.0

A message "DHCP request successful." is displayed in the top right corner. Below the DHCP section, the IPv6 Configuration section is visible, with DHCP, Auto Config, and Static selected. The IPv6 Address field is empty, and the Link Local Address is FE80::2E0:8FFF:FE41:B7CD. The 802.1X section is also visible, with Use 802.1X Security, Authentication set to MD5, and empty fields for Username and Password.

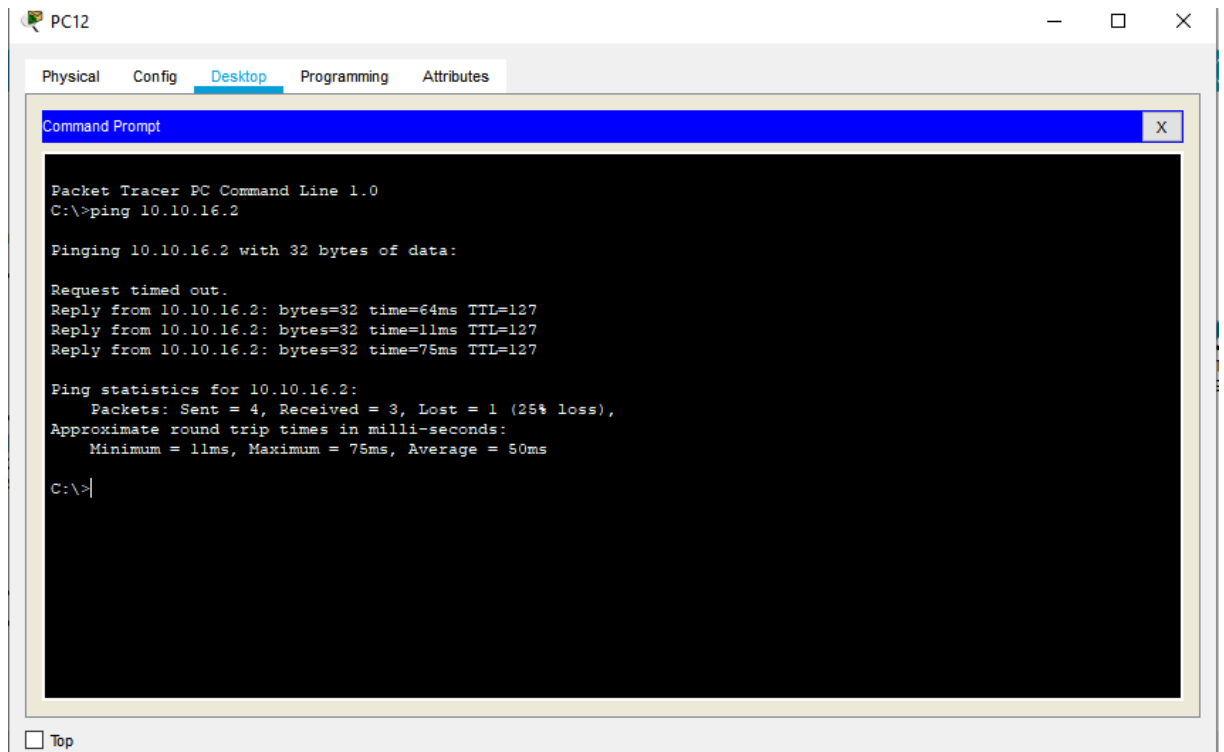
Figure 3.12 : Adressage IP attribué automatiquement.

3.4.4. Vérification de la connectivité

a. Test inter-VLANs

Ce test est d'envoyer des paquets qui appartiennent aux VLANs différent.

Pour tester la connectivité, nous pouvons envoyer un Ping entre le PC₁₂ d'adresse : 10.10.24.2 et le PC₆ avec l'adresse : 10.10.16.2.



```
PC12
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 10.10.16.2

Pinging 10.10.16.2 with 32 bytes of data:

Request timed out.
Reply from 10.10.16.2: bytes=32 time=64ms TTL=127
Reply from 10.10.16.2: bytes=32 time=11ms TTL=127
Reply from 10.10.16.2: bytes=32 time=75ms TTL=127

Ping statistics for 10.10.16.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 75ms, Average = 50ms

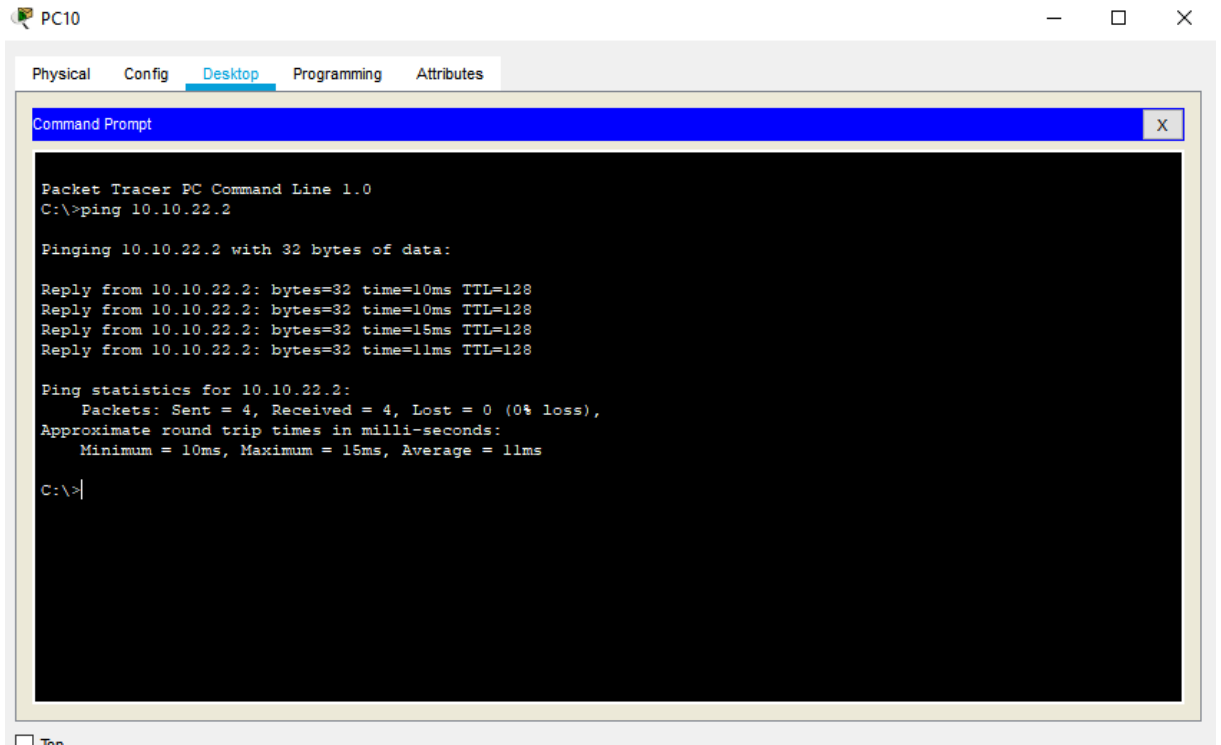
C:\>
```

Figure 3.13 : Test entre le PC₁₂ et le PC₆.

b. Test intra-VLANs

L'intérêt de ce test est d'envoyer des paquets qui appartiennent aux même VLAN.

Par exemple, nous effectuons un autre Ping entre l'adresse IP du PC₁₀ est : 10.10.22.3, avec l'adresse IP du PC₁₅ est : 10.10.22.2.



```
PC10
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 10.10.22.2

Pinging 10.10.22.2 with 32 bytes of data:

Reply from 10.10.22.2: bytes=32 time=10ms TTL=128
Reply from 10.10.22.2: bytes=32 time=10ms TTL=128
Reply from 10.10.22.2: bytes=32 time=15ms TTL=128
Reply from 10.10.22.2: bytes=32 time=11ms TTL=128

Ping statistics for 10.10.22.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 16ms, Average = 11ms

C:\>
```

Figure 3.14 : Test entre le PC₁₀ et le PC₁₅.

3.5. Partie 2 : Nouvelle architecture proposée au réseau CEVITAL

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

3.5.1. Architecture de mise en œuvre

La figure 3.15, illustre la nouvelle architecture mise en place.

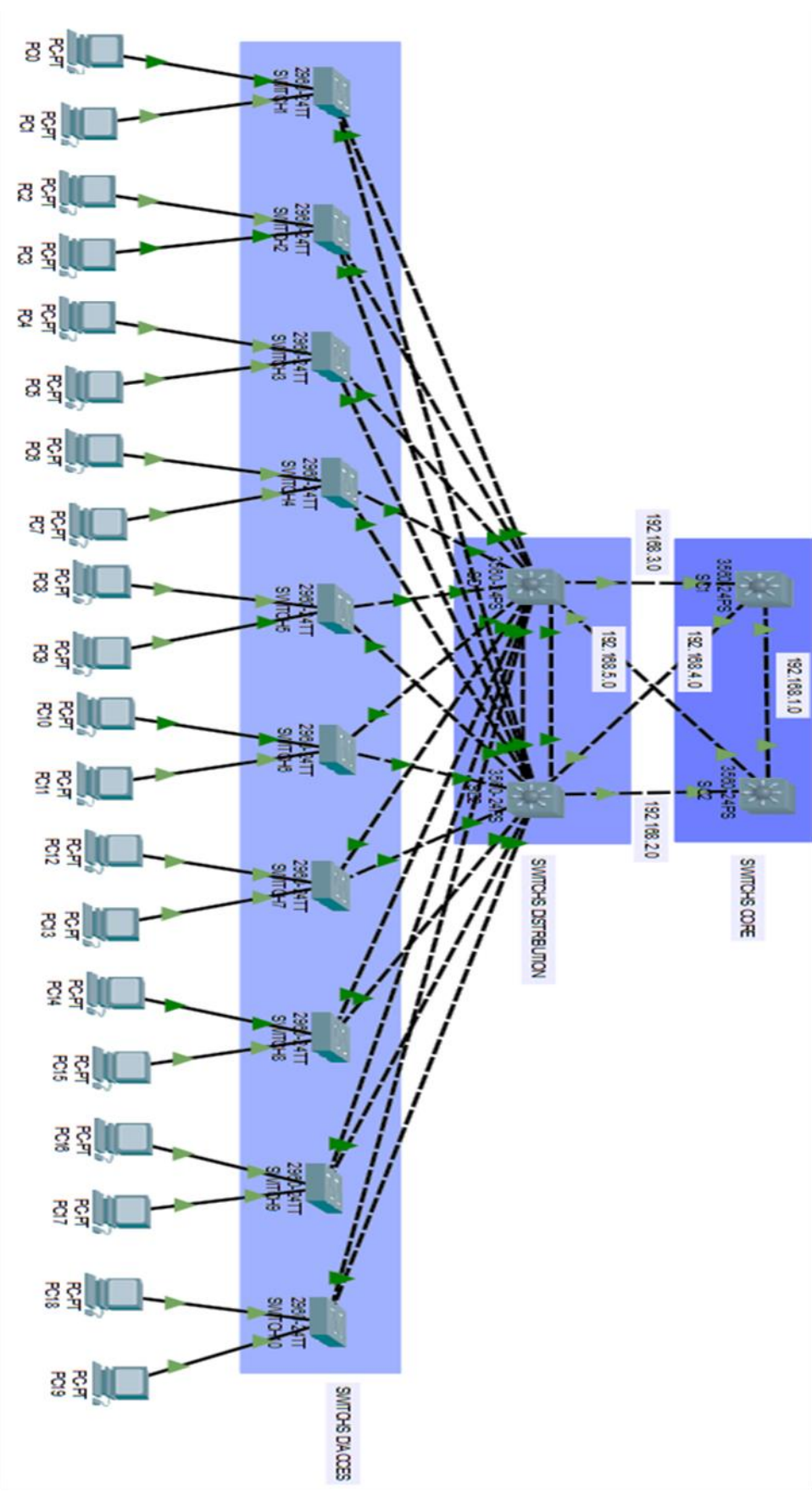


Figure 3.15 : Architecture proposée au réseau CEVITAL Bejaia

3.5.2. Configuration des équipements

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

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

a. Configuration des Hostname et Password

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#enable password CEVITAL
Switch(config)#service password-encryption
Switch(config)#hostname SD1
SD1(config)#exit
SD1#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 3.16 : Configuration du Hostname et Password.

b. Création des VLANs

La création des VLANs est faite au niveau des switchs de distribution comme le montre la figure 3.17.

```
SD1>EN
Password:
SD1#config t
Enter configuration commands, one per line. End with CNTL/Z.
SD1(config)# vlan 10
SD1(config-vlan)#name Direction
SD1(config-vlan)#exit
SD1(config)#
```

Figure 3.17 : Création des VLANs.

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

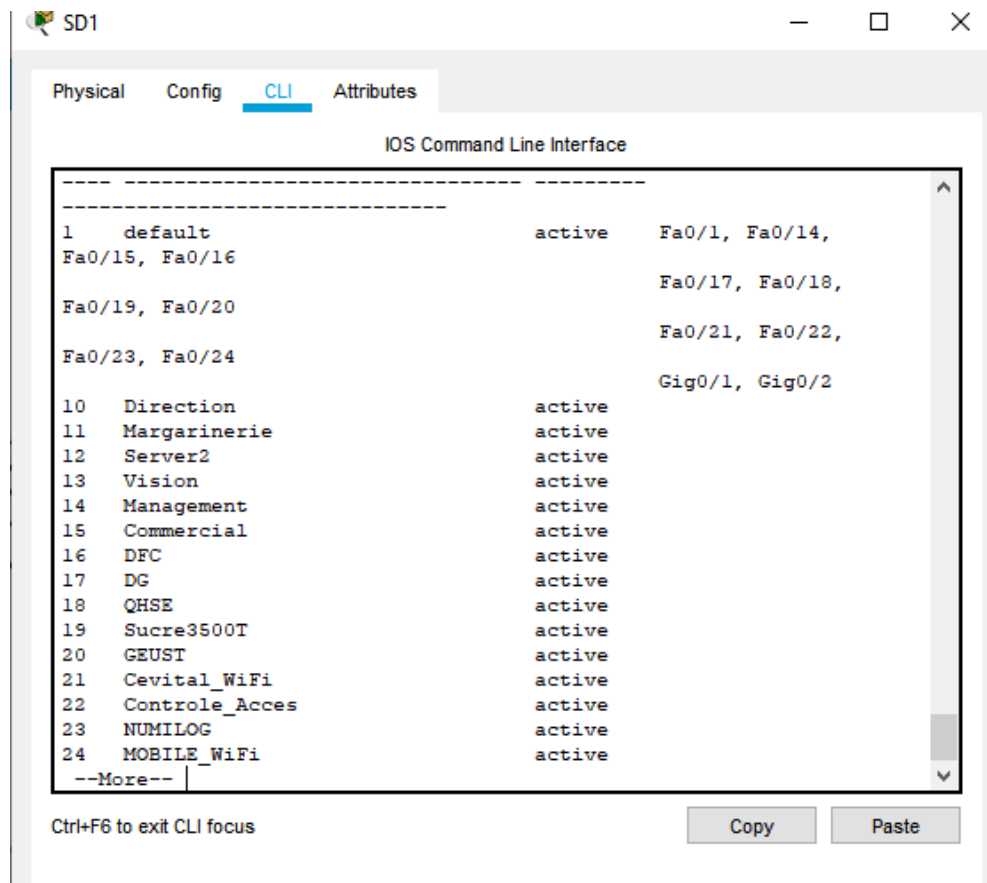


Figure 3.18 : Vérification des VLANs.

c. Configuration des interfaces VLAN

En outre, nous avons configuré les interfaces des switches de distribution de chaque VLAN, autrement dit, nous allons attribuer une adresse IP pour chaque VLAN sur les deux switches. Cela va nous permettre de faire un routage inter-VLAN, mais ce dernier ne sera pas fonctionnel avant son activation avec la commande **ip routing**.

Durant cette étape, nous allons attribuer les adresses aux interfaces virtuelles des switches de distribution, ou le **252** sera sur la partie machine de chaque VLAN de SD₁. Tandis que, sur le SD₂, nous allons attribuer le **253** sur la partie machine de chaque VLAN. La figure 3.19, est donnée pour bien illustrer cette étape.

```

SD1(config)#int vlan 10
SD1(config-if)#ip add 10.10.10.252 255.255.255.0
SD1(config-if)#
  
```

Figure 3.19 : Configuration des interfaces VLANs sur SD₁.

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

```

interface Vlan10
  mac-address 0009.7cde.7501
  ip address 10.10.10.252 255.255.255.0
!
interface Vlan11
  mac-address 0009.7cde.7502
  ip address 10.10.11.252 255.255.255.0
!
interface Vlan12
  mac-address 0009.7cde.7503
  ip address 10.10.12.252 255.255.255.0
!
interface Vlan13
  mac-address 0009.7cde.7504
  ip address 10.10.13.252 255.255.255.0
!
interface Vlan14
  mac-address 0009.7cde.7505
  ip address 10.10.14.252 255.255.255.0
!
interface Vlan15
  mac-address 0009.7cde.7506
  ip address 10.10.15.252 255.255.255.0
!
interface Vlan16
  mac-address 0009.7cde.7507
  ip address 10.10.16.252 255.255.255.0
!
interface Vlan17
  mac-address 0009.7cde.7508
  ip address 10.10.17.252 255.255.255.0
!
interface Vlan18
  mac-address 0009.7cde.7509
  ip address 10.10.18.252 255.255.255.0
!
interface Vlan19
  mac-address 0009.7cde.750a
  ip address 10.10.19.252 255.255.255.0
!
interface Vlan20
  mac-address 0009.7cde.750b
  ip address 10.10.20.252 255.255.255.0
!
interface Vlan21
  mac-address 0009.7cde.750c
  ip address 10.10.21.252 255.255.255.0
!
interface Vlan22
  mac-address 0009.7cde.750d
  ip address 10.10.22.252 255.255.255.0
!
interface Vlan23
  mac-address 0009.7cde.750e
  ip address 10.10.23.252 255.255.255.0
!
interface Vlan24
  mac-address 0009.7cde.750f
  ip address 10.10.24.252 255.255.255.0
!
interface Vlan25
  mac-address 0009.7cde.7510
  ip address 10.10.25.252 255.255.255.0
!

```

Figure 3.20 : Vérification des interfaces VLANs de SD₁.

```

SD2(config)#int vlan 10
SD2(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

SD2(config-if)#ip add 10.10.10.253 255.255.255.0
SD2(config-if)#exit
SD2(config)#

```

Figure 3.21 : Configuration des interfaces VLANs sur SD₂.

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


```

!
interface Vlan10
 mac-address 0030.f2cb.c901
 ip address 10.10.10.253 255.255.255.0
!
interface Vlan11
 mac-address 0030.f2cb.c902
 ip address 10.10.11.253 255.255.255.0
!
interface Vlan12
 mac-address 0030.f2cb.c903
 ip address 10.10.12.253 255.255.255.0
!
interface Vlan13
 mac-address 0030.f2cb.c904
 ip address 10.10.13.253 255.255.255.0
!
interface Vlan14
 mac-address 0030.f2cb.c905
 ip address 10.10.14.253 255.255.255.0
!
interface Vlan15
 mac-address 0030.f2cb.c906
 ip address 10.10.15.253 255.255.255.0
!
interface Vlan16
 mac-address 0030.f2cb.c907
 ip address 10.10.16.253 255.255.255.0
!
interface Vlan17
 mac-address 0030.f2cb.c908
 ip address 10.10.17.253 255.255.255.0
!
interface Vlan18
 mac-address 0030.f2cb.c909
 ip address 10.10.18.253 255.255.255.0
!
!
interface Vlan19
 mac-address 0030.f2cb.c90a
 ip address 10.10.19.253 255.255.255.0
!
interface Vlan20
 mac-address 0030.f2cb.c90b
 ip address 10.10.20.253 255.255.255.0
!
interface Vlan21
 mac-address 0030.f2cb.c90c
 ip address 10.10.21.253 255.255.255.0
!
interface Vlan22
 mac-address 0030.f2cb.c90d
 ip address 10.10.22.253 255.255.255.0
!
interface Vlan23
 mac-address 0030.f2cb.c90e
 ip address 10.10.23.253 255.255.255.0
!
interface Vlan24
 mac-address 0030.f2cb.c90f
 ip address 10.10.24.253 255.255.255.0
!
interface Vlan25
 mac-address 0030.f2cb.c910
 ip address 10.10.25.253 255.255.255.0
!
!

```

Figure 3.22 : Vérification des interfaces VLANs de SD₂.

d. Configuration du DHCP

La configuration se fera au niveau des switches de distribution, nous allons créer un pool d'adresse pour chaque VLAN, ensuite on définit la passerelle par défaut du sous réseau.

```

SD1(config)#ip dhcp pool VLAN_Direction
SD1(dhcp-config)#network 10.10.10.0 255.255.255.0
SD1(dhcp-config)#default-router 10.10.10.252
SD1(dhcp-config)#

```

Figure 3.23 : Configuration du DHCP sur SD₁.

```

SD2(config)# ip dhcp pool VLAN_Direction
SD2(dhcp-config)#network 10.10.10.0 255.255.255.0
SD2(dhcp-config)#default-router 10.10.10.253
SD2(dhcp-config)#

```

Figure 3.24 : Configuration du DHCP sur SD₂.

Ensuite, nous allons vérifier la création de nos pools DHCP avec la commande **show running-config**.

```
ip dhcp pool VLAN_Direction
network 10.10.10.0 255.255.255.0
default-router 10.10.10.252
ip dhcp pool VLAN_Margarinerie
network 10.10.11.0 255.255.255.0
default-router 10.10.11.252
ip dhcp pool VLAN_Server2
network 10.10.12.0 255.255.255.0
default-router 10.10.12.252
ip dhcp pool VLAN_Vision
network 10.10.13.0 255.255.255.0
default-router 10.10.13.252
ip dhcp pool VLAN_Management
network 10.10.14.0 255.255.255.0
default-router 10.10.14.252
ip dhcp pool VLAN_Commercial
network 10.10.15.0 255.255.255.0
default-router 10.10.15.252
ip dhcp pool VLAN_DFC
network 10.10.16.0 255.255.255.0
default-router 10.10.16.252
ip dhcp pool VLAN_DG
network 10.10.17.0 255.255.255.0
default-router 10.10.17.252
ip dhcp pool VLAN_QHSE
network 10.10.18.0 255.255.255.0
default-router 10.10.18.252
ip dhcp pool VLAN_Sucre3500T
network 10.10.19.0 255.255.255.0
default-router 10.10.19.252
ip dhcp pool VLAN_GEUST
network 10.10.20.0 255.255.255.0
default-router 10.10.20.252
ip dhcp pool VLAN_Cevital
ip dhcp pool VLAN_Cevital_WiFi
network 10.10.21.0 255.255.255.0
default-router 10.10.21.252
ip dhcp pool VLAN_NUMILOG
network 10.10.23.0 255.255.255.0
default-router 10.10.23.252
ip dhcp pool VLAN_MOBILE_WiFi
network 10.10.24.0 255.255.255.0
default-router 10.10.24.252
ip dhcp pool VLAN_Firewall_Datacenter
network 10.10.25.0 255.255.255.0
default-router 10.10.25.252
.
```

Figure 3.25 : Vérification de la création des pools DHCP sur SD₁.

```

ip dhcp pool VLAN_Direction
network 10.10.10.0 255.255.255.0
default-router 10.10.10.253
ip dhcp pool VLAN_Margarinerie
network 10.10.11.0 255.255.255.0
default-router 10.10.11.253
ip dhcp pool VLAN_Server2
network 10.10.12.0 255.255.255.0
default-router 10.10.12.253
ip dhcp pool VLAN_Vision
network 10.10.13.0 255.255.255.0
default-router 10.10.13.253
ip dhcp pool VLAN_Management
network 10.10.14.0 255.255.255.0
default-router 10.10.14.253
ip dhcp pool VLAN_Commercial
network 10.10.15.0 255.255.255.0
default-router 10.10.15.253
ip dhcp pool VLAN_DFC
network 10.10.16.0 255.255.255.0
default-router 10.10.16.253
ip dhcp pool VLAN_DG
network 10.10.17.0 255.255.255.0
default-router 10.10.17.253
ip dhcp pool VLAN_QHSE
network 10.10.18.0 255.255.255.0
default-router 10.10.18.253
ip dhcp pool VLAN_Sucre3500T
network 10.10.19.0 255.255.255.0
default-router 10.10.19.253
ip dhcp pool VLAN_GEUST
network 10.10.20.0 255.255.255.0
default-router 10.10.20.253
ip dhcp pool VLAN_Cevital_WiFi
network 10.10.21.0 255.255.255.0
default-router 10.10.21.253
ip dhcp pool VLAN_Controle_Acces
network 10.10.22.0 255.255.255.0
default-router 10.10.22.253
ip dhcp pool VLAN_NUMILOG
network 10.10.23.0 255.255.255.0
default-router 10.10.23.253
ip dhcp pool VLAN_MOBILE_WiFi
network 10.10.24.0 255.255.255.0
default-router 10.10.24.253
ip dhcp pool VLAN_Firewall_Datacenter
network 10.10.25.0 255.255.255.0
default-router 10.10.25.253

```

Figure 3.26 : Vérification de la création des pools DHCP sur SD₂.

Afin de réussir ce protocole et de permettre aux deux switches de distribution d'attribuer des adresses en même temps sans conflit. Nous allons exclure les adresses de 129 à 253 sur le SD₁ et exclure les adresses 1 à 128 du SD₂. C'est-à-dire le SD₁ va attribuer les adresses allant de 1 jusqu'à 128 et le SD₂, va attribuer les adresses allant de 129 à 253.

```

SD1(config)#ip dhcp excluded-address 10.10.10.1 10.10.10.128
SD1(config)#ip dhcp excluded-address 10.10.11.1 10.10.11.128
SD1(config)#ip dhcp excluded-address 10.10.12.1 10.10.12.128
SD1(config)#ip dhcp excluded-address 10.10.13.1 10.10.13.128
SD1(config)#ip dhcp excluded-address 10.10.14.1 10.10.14.128
SD1(config)#ip dhcp excluded-address 10.10.15.1 10.10.15.128
SD1(config)#ip dhcp excluded-address 10.10.16.1 10.10.16.128
SD1(config)#ip dhcp excluded-address 10.10.17.1 10.10.17.128
SD1(config)#ip dhcp excluded-address 10.10.18.1 10.10.17.128
SD1(config)#ip dhcp excluded-address 10.10.18.1 10.10.18.128
SD1(config)#ip dhcp excluded-address 10.10.19.1 10.10.19.128
SD1(config)#ip dhcp excluded-address 10.10.20.1 10.10.20.128
SD1(config)#ip dhcp excluded-address 10.10.21.1 10.10.21.128
SD1(config)#ip dhcp excluded-address 10.10.22.1 10.10.22.128
SD1(config)#ip dhcp excluded-address 10.10.23.1 10.10.23.128
SD1(config)#ip dhcp excluded-address 10.10.24.1 10.10.24.128
SD1(config)#ip dhcp excluded-address 10.10.25.1 10.10.25.128
SD1(config)#

```

Figure 3.27 : Adresses exclues sur SD₁.


```
SD2(config)#ip dhcp excluded-address 10.10.10.129 10.10.10.253
SD2(config)#ip dhcp excluded-address 10.10.11.129 10.10.11.253
SD2(config)#ip dhcp excluded-address 10.10.12.129 10.10.12.253
SD2(config)#ip dhcp excluded-address 10.10.13.129 10.10.13.253
SD2(config)#ip dhcp excluded-address 10.10.14.129 10.10.14.253
SD2(config)#ip dhcp excluded-address 10.10.15.129 10.15.14.253
SD2(config)#ip dhcp excluded-address 10.10.15.129 10.10.15.253
SD2(config)#ip dhcp excluded-address 10.10.16.129 10.10.16.253
SD2(config)#ip dhcp excluded-address 10.10.17.129 10.10.17.253
SD2(config)#ip dhcp excluded-address 10.10.18.129 10.10.18.253
SD2(config)#ip dhcp excluded-address 10.10.19.129 10.10.19.253
SD2(config)#ip dhcp excluded-address 10.10.20.129 10.10.20.253
SD2(config)#ip dhcp excluded-address 10.10.21.129 10.10.21.253
SD2(config)#ip dhcp excluded-address 10.10.22.129 10.10.22.253
SD2(config)#ip dhcp excluded-address 10.10.23.129 10.10.23.253
SD2(config)#ip dhcp excluded-address 10.10.24.129 10.10.24.253
SD2(config)#ip dhcp excluded-address 10.10.25.129 10.10.25.253
SD2(config)#
```

Figure 3.28 : Adresses exclues sur SD2.

e. Configuration des liens Trunks

Nous allons configurer les liaisons entre les switches de distribution et d'accès (Niveau 2) en mode Trunk, comme l'indique la figure. Afin que les switches communiquent et transmettent entre eux les VLANs configurés dans les switches de distribution.

```
SD1(config)#int fa 0/4
SD1(config-if)#switchport trunk encapsulation dot1q
SD1(config-if)#description TO_SWITCH1
SD1(config-if)#
```

Figure 3.29 : Configuration des liens Trunk.

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


```
description TO_SWITCH1
switchport trunk encapsulation dot1q
!
interface FastEthernet0/5
description TO_SWITCH2
switchport trunk encapsulation dot1q
!
interface FastEthernet0/6
description TO_SWITCH3
switchport trunk encapsulation dot1q
!
interface FastEthernet0/7
description TO_SWITCH4
switchport trunk encapsulation dot1q
!
interface FastEthernet0/8
description TO_SWITCH5
switchport trunk encapsulation dot1q
!
interface FastEthernet0/9
description TO_SWITCH6
switchport trunk encapsulation dot1q
!
interface FastEthernet0/10
description TO_SWITCH7
switchport trunk encapsulation dot1q
!
interface FastEthernet0/11
description TO_SWITCH8
switchport trunk encapsulation dot1q
!
interface FastEthernet0/12
description TO_SWITCH9
switchport trunk encapsulation dot1q
!
interface FastEthernet0/13
description TO_SWITCH10
switchport trunk encapsulation dot1q
.
```

Figure 3.30 : Vérification des liens Trunk.

f. Attribution des ports des commutateurs aux VLANs

```
SWITCH1(config)#int fa 0/3
SWITCH1(config-if)#switchport mode access
SWITCH1(config-if)#switchport access vlan 10
SWITCH1(config-if)#exit
SWITCH1(config)#int fa 0/4
SWITCH1(config-if)#switchport mode access
SWITCH1(config-if)#switchport access vlan 11
SWITCH1(config-if)#exit
SWITCH1(config)#|
```

Figure 3.31 : Configuration des interfaces du switch en mode Access.

g. Configuration du protocole VTP

Afin de profiter des services VTP, nous allons configurer le switch de distributions SD1 en mode serveur et le reste des switches en mode client afin que les VLANs se propagent de SD1 vers les autres switches.

Pour cela nous allons procéder comme suite :

h. Configurer le SD1 en VTP serveur :

```
SD1(config)#vtp mode server
Device mode already VTP SERVER.
SD1(config)#vtp domain CEVITAL.COM
Changing VTP domain name from NULL to CEVITAL.COM
SD1(config)#vtp password CEVITAL
Setting device VLAN database password to CEVITAL
```

Figure 3.32 : Configuration du VTP serveur.

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

```
Enter configuration commands, one per line. End with CNTL/Z.
SD1(config)# do show vtp status
VTP Version capable      : 1 to 2
VTP version running     : 2
VTP Domain Name         : CEVITAL.COM
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID               : 0050.0FAA.9B00
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 V110 (lowest numbered
VLAN interface found)

Feature VLAN :
-----|
VTP Operating Mode      : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 21
Configuration Revision  : 64
MDS digest              : 0xCC 0xE8 0x71 0x12 0x50 0x62
0xA4 0x56
                        0xCA 0x23 0x82 0xC6 0xC3 0xD6
0x76 0x0B
SD1(config)#
```

Figure 3.33 : Vérification de la configuration du VTP serveur.**i. Configuration du protocole VTP sur le switch d'accès :**

Le switch d'accès sera configuré comme VTP client.

```
SWITCH1(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWITCH1(config)#vtp domain CEVITAL.COM
Domain name already set to CEVITAL.COM.
SWITCH1(config)#vtp password CEVITAL
Setting device VLAN database password to CEVITAL
```

Figure 3.34 : Configuration du VTP client.

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

```
SWITCH1(config)#do show vtp status
VTP Version           : 2
Configuration Revision : 64
Maximum VLANs supported locally : 255
Number of existing VLANs : 21
VTP Operating Mode    : Client
VTP Domain Name      : CEVITAL.COM
VTP Pruning Mode     : Disabled
VTP V2 Mode          : Disabled
VTP Traps Generation : Disabled
MD5 digest           : 0xCC 0xE8 0x71 0x12 0x50 0x62 0xA4
0x56
-----
```

Figure 3.35 : Vérification de la configuration du VTP client.

3.5.3. Vérification des adresses IP attribuées par le DHCP

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

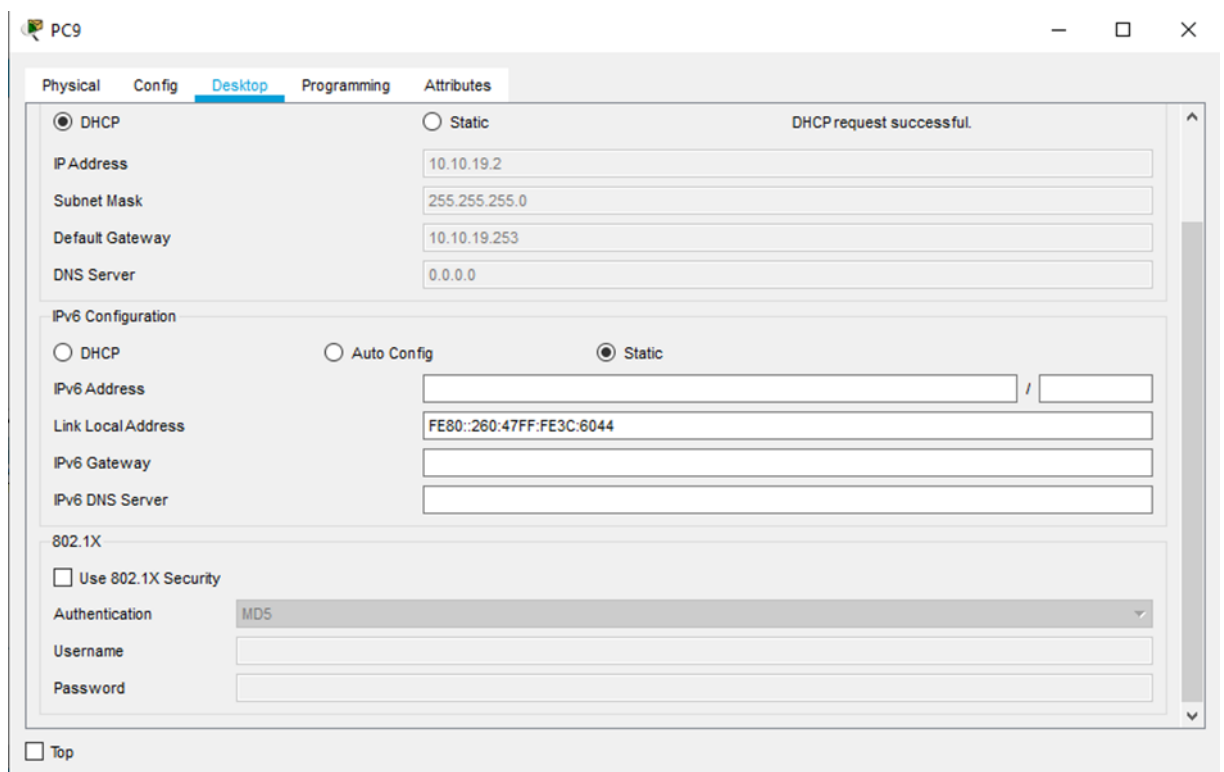


Figure 3.36 : Adresse IP attribuée automatiquement

3.5.4. EIGRP (Enhanced Interior Gateway Routing Protocol)

Pour l'EIGRP, nous allons configurer ce Protocol au niveau des switches distribution et ceux du Core. Nous allons attribuer un groupe 5 par exemple et nous allons saisir tous les

réseaux directement connectés dans chaque switch. Pour les VLANs, nous allons saisir le réseau 10.10.0.0 avec un masque inversé 0.0.255.255 qui englobera tous les VLANs.

```
SD1(config)#router eigrp 5
SD1(config-router)#network 192.168.3.0 0.0.0.3
SD1(config-router)#
%DUAL-S-NBRCHANGE: IP-EIGRP 5: Neighbor 192.168.3.1 (FastEthernet0/2) is up: new
adjacency

SD1(config-router)#network 192.168.5.0 0.0.0.3
SD1(config-router)#
%DUAL-S-NBRCHANGE: IP-EIGRP 5: Neighbor 192.168.5.1 (FastEthernet0/3) is up: new
adjacency

SD1(config-router)#network 10.10.0.0 0.0.255.255
SD1(config-router)#exit
```

Figure 3.37 : Configuration d'EIGRP sur SD₁

Nous allons procéder avec les autres switches Core et distribution.

```
SD2(config)#router eigrp 5
SD2(config-router)#network 192.168.2.0 0.0.0.3
SD2(config-router)#
%DUAL-S-NBRCHANGE: IP-EIGRP 5: Neighbor 192.168.2.1 (FastEthernet0/2) is up: new
adjacency

SD2(config-router)#network 192.168.4.0 0.0.0.3
SD2(config-router)#
%DUAL-S-NBRCHANGE: IP-EIGRP 5: Neighbor 192.168.4.1 (FastEthernet0/3) is up: new
adjacency

SD2(config-router)#network 10.10.0.0 0.0.255.255
SD2(config-router)#
```

Figure 3.38 : Configuration d'EIGRP sur SD₂

```
SC1(config)#router eigrp 5
SC1(config-router)#network 192.168.1.0 0.0.0.3
SC1(config-router)#network 192.168.4.0 0.0.0.3
SC1(config-router)#network 192.168.3.0 0.0.0.3
SC1(config-router)#exit
```

Figure 3.39 : Configuration d'EIGRP sur SC₁.

```
SC2(config)#router eigrp 5
SC2(config-router)#network 192.168.1.0 0.0.0.3
SC2(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 5: Neighbor 192.168.1.1 (FastEthernet0/1) is up: new
adjacency

SC2(config-router)#network 192.168.2.0 0.0.0.3
SC2(config-router)#network 192.168.5.0 0.0.0.3
SC2(config-router)#exit
```

Figure 3.40 : Configuration d'EIGRP sur SC₂.

3.5.5. Configuration du Spanning-Tree Protocol (STP)

Les figures 3.41 et 3.42 illustrent les commandes qui nous permettent de configurer le protocole STP, d'affecter un root primaire ou secondaire à un VLAN. Nous avons fait en sorte que :

SD₁ sera le root pour les VLANs 10-17 et bridge pour les VLANs 18-25, alors que le SD₂ sera le root pour les VLANs 18-25 et bridge pour les VLANs 10-17.

```
SD1(config)#spanning-tree mode pvst
SD1(config)#spanning-tree vlan 10-17 root primary
SD1(config)#spanning-tree vlan 18-25 root secondary
SD1(config)#exit
```

Figure 3.41 : Configuration de STP sur SD₁.

```
SD2(config)#spanning-tree mode pvst
SD2(config)#spanning-tree vlan 18-25 root primary
SD2(config)#spanning-tree vlan 10-17 root secondary
```

Figure 3.42 : Configuration de STP sur SD₂.

3.5.6. Configuration de Hot Standby Router Protocol (HSRP)

La configuration de la haute disponibilité s'effectue au niveau des Switchs de distribution. Pour cela, on utilise deux sortes de configurations HSRP : la première lorsqu'un VLAN est prioritaire, tant dit que le deuxième lorsqu'il est secondaire. La figure 3.43 ci-dessous montre les VLANs prioritaires par rapport aux VLANs secondaires.

La commande « Standby preempt » donne la priorité aux Switchs de distribution de protocole HSRP, pour que ce dernier devienne actif immédiatement. La priorité de base est de 100, avec une priorité de 105, SD₁ devient le routeur actif, on active l'option « preempt », qui permet au switch de distribution actif de prendre le rôle après une panne.


```
SD1(config)#int vlan 10
SD1(config-if)#standby 10 ip 10.10.10.254
SD1(config-if)#standby 10 priority 105
SD1(config-if)#standby 10 preempt
SD1(config-if)#
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Standby -> Active
```

Figure 3.43 : Configuration du HSRP sur SD₁ (VLAN 10-17).

Pour les VLANs 18 à 25 en mode « **Standby** » :

```
SD1(config-if)#int vlan 18
SD1(config-if)#standby 18 ip 10.10.18.254
SD1(config-if)#
```

Figure 3.44 : Configuration du HSRP sur SD₁ (VLAN 18-25).

Ensuite sur le SD₂ et pour les VLANs 18 à 25 en mode « **Active** » :

```
SD2(config-if)#standby 18 preempt
SD2(config-if)#int vlan 18
SD2(config-if)#standby 18 ip 10.10.18.254
SD2(config-if)#standby 18 priority 105
SD2(config-if)#standby 18 preempt
SD2(config-if)#
%HSRP-6-STATECHANGE: Vlan18 Grp 18 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan18 Grp 18 state Standby -> Active
```

Figure 3.45 : Configuration du HSRP sur SD₂ (VLAN 18-25).

Pour les VLANs de 10 à 17 en mode « **Standby** » :

```
SD2(config-if)#
SD2(config-if)#int vlan 10
SD2(config-if)#standby 10 ip 10.10.10.254
SD2(config-if)#
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
```

Figure 3.46 : Configuration du HSRP sur SD₂ (VLAN 10-17).

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

```

SD1(config-if)#do 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  105 P Active     local           10.10.15.253    10.10.15.254
Vl16           16  105 P Active     local           10.10.16.253    10.10.16.254
Vl17           17  105 P Active     local           10.10.17.253    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
Vl21           21  100 Standby     10.10.21.253    local           10.10.21.254
Vl22           22  100 Standby     10.10.22.253    local           10.10.22.254
Vl23           23  100 Standby     10.10.23.253    local           10.10.23.254
Vl24           24  100 Standby     10.10.24.253    local           10.10.24.254
Vl25           25  100 Standby     10.10.25.253    local           10.10.25.254
SD1(config-if)#

```

Figure 3.47 : Vérification du HSRP sur SD₁.

```

SD2(config-if)#do 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     10.10.13.252    local           10.10.13.254
Vl14           14  100 Standby     10.10.14.252    local           10.10.14.254
Vl15           15  100 Standby     10.10.15.252    local           10.10.15.254
Vl16           16  100 Standby     10.10.16.252    local           10.10.16.254
Vl17           17  100 Standby     10.10.17.252    local           10.10.17.254
Vl18           18  105 P Active     local           unknown         10.10.18.254
Vl19           19  105 P Active     local           unknown         10.10.19.254
Vl20           20  105 P Active     local           unknown         10.10.20.254
Vl21           21  105 P Active     local           unknown         10.10.21.254
Vl22           22  105 P Active     local           unknown         10.10.22.254
Vl23           23  105 P Active     local           unknown         10.10.23.254
Vl24           24  105 P Active     local           unknown         10.10.24.254
Vl25           25  105 P Active     local           unknown         10.10.25.254
SD2(config-if)#
SD2(config-if)#

```

Figure 3.48 : Vérification du HSRP sur SD₂

3.5.7. Agrégation des liens EtherChannel

Donc dans notre architecture, nous avons opté pour une agrégation des liens Fast Ethernet entre les deux switches de distribution SD₁ et SD₂ et nous allons la configurer comme l'indique la figure 3.49 ci-dessous,

```
SD1(config)#int rang fa0/14-15
SD1(config-if-range)#channel-group 1 mode on
SD1(config-if-range)#
Creating a port-channel interface Port-channel 1

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

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

SD1(config-if-range)#exit
SD1(config)#int port-channel 1
SD1(config-if)#switchport trunk encapsulation dot1q
SD1(config-if)#switchport mode trunk
```

Figure 3.49 : Configuration d'EtherChannel

3.5.8. Vérification de la communication

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

Premièrement, nous avons pris un PC du VLAN 11 et nous allons faire un Ping continue vers l'adresse **192.168.2.1** afin de vérifier non seulement le HSRP mais aussi l'EIGRP comme l'explique la figure 3.50.

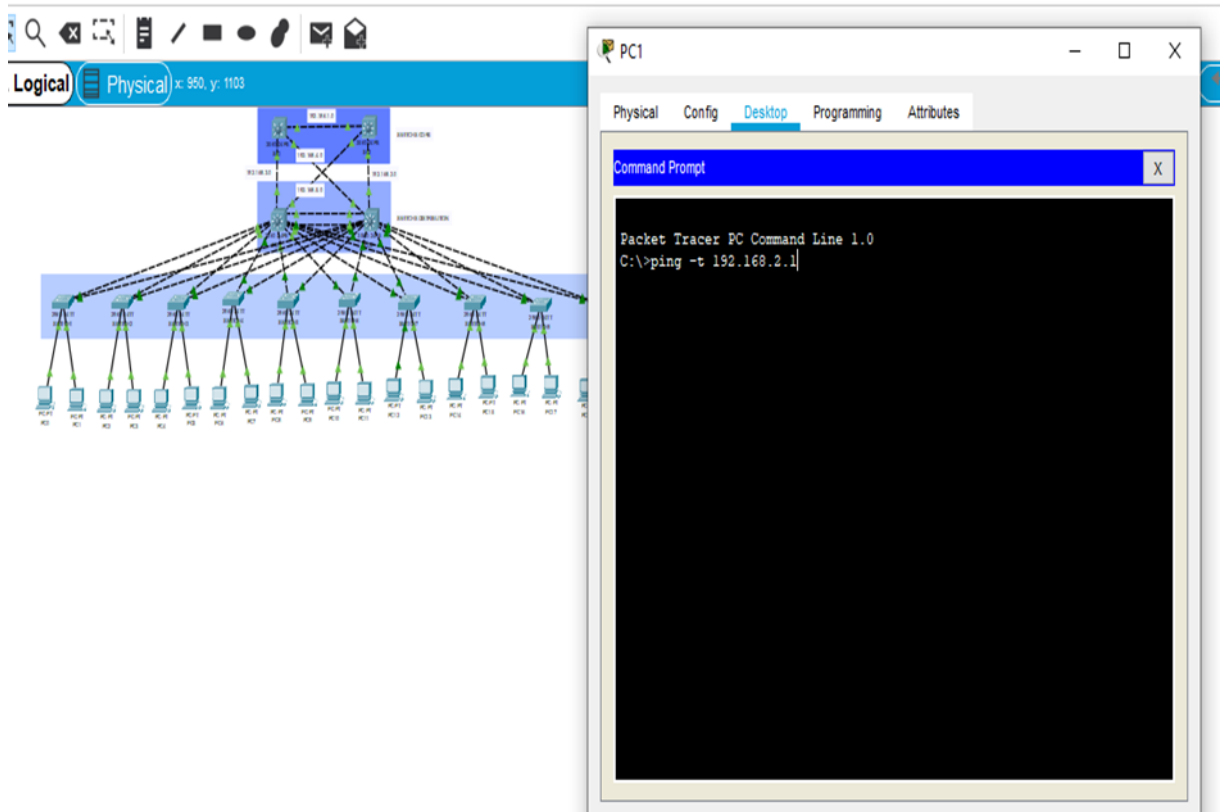


Figure 3.50 : Capture explicative du Ping

En premier lieu nous avons constaté que le Ping fonctionne parfaitement et sans problème, comme le montre la figure 3.51. Ensuite, nous allons simuler une panne, celle d'éteindre la route principale de ce VLAN, présenté par la ligne rouge sur la figure 3.51. En effet, nous allons constater directement que le Ping s'arrête et ne passe pas.

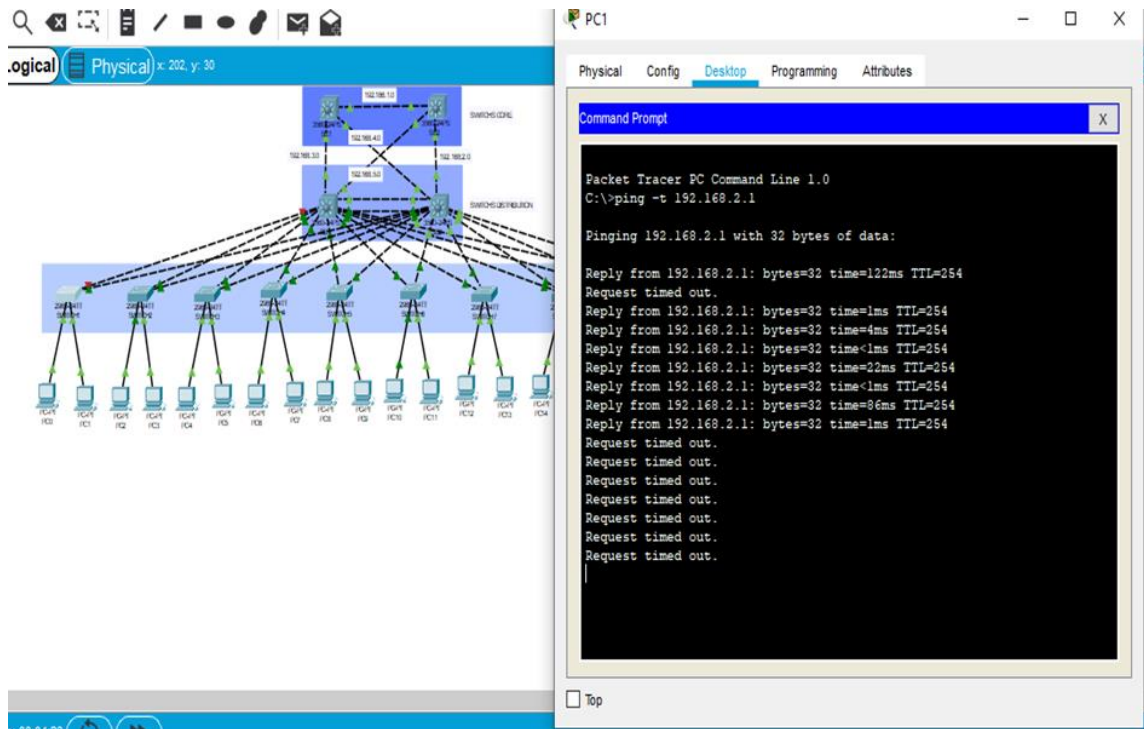


Figure 3.51 : Ping lors de désactivation du port vers SD1.

Après quelques arrêts le protocole HSRP communique avec le SD2 et active automatiquement la route qui standby en active, nous allons constater directement que le Ping reprend. Ce qui prouve que la route est converti vers SD2, comme est visible sur la figure 3.52 :

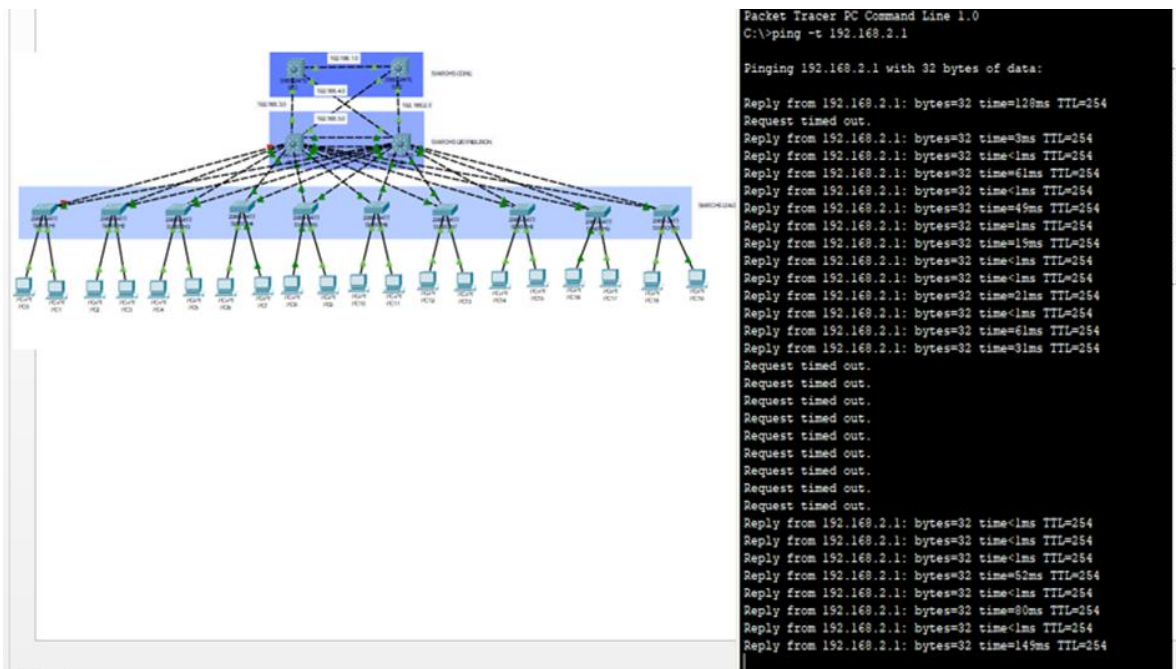


Figure 3.52 : Reprise du Ping après discussion avec SD2.

Maintenant, nous allons réactiver l'interface principale sur le SD₁, afin de s'assurer qu'il va reprendre sa route principale et vérifier que le **preempt** du HSRP fonctionne parfaitement.

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

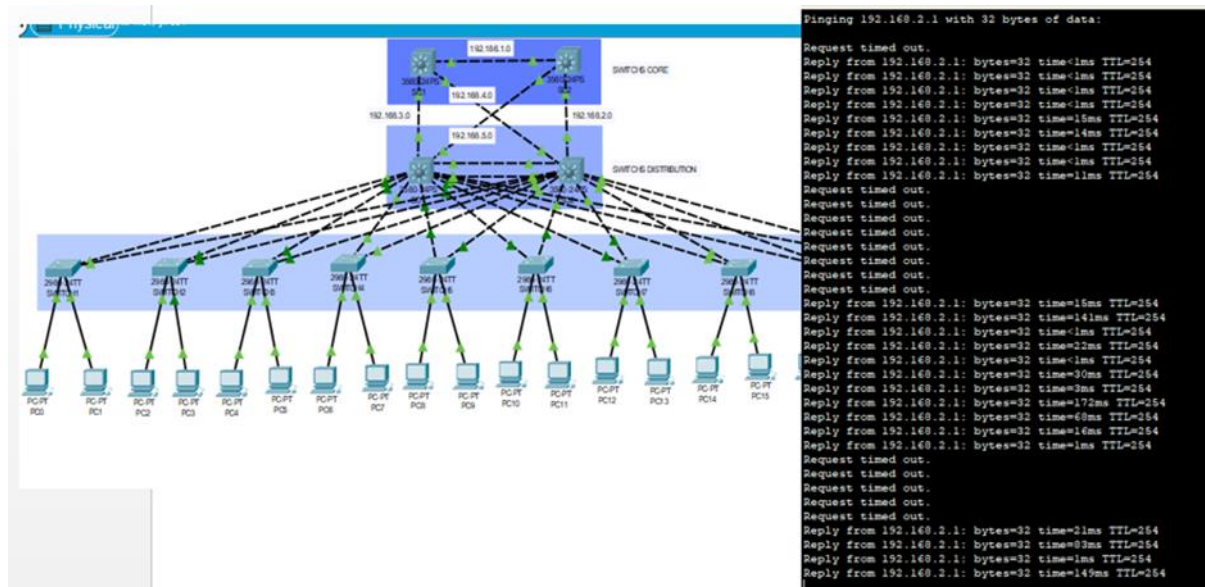


Figure 3.53 : Ping lors de la réactivation du port vers SD₁.

Remarque : désormais le protocole HSRP que nous avons configuré, ainsi que le protocole de routage EIGRP, fonctionnent parfaitement et signalent aucun problème.

3.6. Conclusion

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

Conclusion générale

Conclusion générale

Le secteur de la technologie de l'information ne cesse d'évoluer à l'échelle mondiale. Afin d'accomplir notre travail et d'aboutir au résultat escompté, nous avons choisi de travailler sur le simulateur Packet Tracer pour ces différents avantages en ce qui concerne la mise en évidence de l'architecture du système à réaliser en précisant les différents composants, ainsi que la simplicité et la clarté du matériel dont on a besoin, ce qui facilite leur configurations.

Grâce à notre projet, nous avons pu approfondir nos connaissances théoriques et les mettre en en pratique durant notre stage pour installer, configurer et administrer une architecture réseau locale pour l'entreprise CEVITAL Bejaia. Pour cela, il nous a fallu penser à une issue qui s'adapte avec l'architecture du réseau existant, tout en tenant compte de la durabilité, l'évolution et la fiabilité, tant que sur le plan technique que sur le plan économique.

Cependant, nous avons divisé notre travail en trois grands chapitres, dont le premier fournit des généralités sur les réseaux informatiques. Le second est porté sur l'organisme d'accueil CEVITAL et ces différentes infrastructure, ainsi que son architecture réseau dont nous avons constaté un problème, qui nous a poussé à proposer nos solutions. Et enfin, le troisième chapitre, que nous avons dédié principalement à la partie pratique de notre thème, avec une partie consacrée à l'étude du réseau existant de CEVITAL pour aboutir à une architecture meilleure d'un réseau local performant et évolutif.

Effectivement, l'échec dans le fonctionnement du réseau informatique de l'entreprise CEVITAL, s'est révélé en premier lieu, à travers son architecture. D'ailleurs, tout comme nous l'avons constaté et déclarer, de nombreuses insuffisances topologiques, faisant objet d'un grand risque de disfonctionnement. Par conséquent, afin d'arriver à un réseau plus performant et résistant aux pannes, nous avons proposé d'ajouter un second backbone interconnecté au seul backbone existant en redondance, et d'exploiter de nouveaux protocoles d'échange de bonne qualité avec un protocole de routage plus efficace.

Bibliographie

- [1] RAHOUAL, Malek et SIARRY, Patrick. Réseaux informatiques: conception et optimisation. Technip, 2006.
- [2] Philippe Atelin « Réseaux informatiques - Notions fondamentales », Eni éditions, 2009.
- [3] Guy Pujolle. Cours réseaux et télécoms. Edition Eyrolles, 2004.
- [4] FOROUZAN B., « Local Area Network, Mc GRAW Hill », éditions Eyrolles, 2002.
- [5] Bertrand PETIT ; architectures des réseaux ,2006.
- [6] Badéche A. classification selon l'architecture, Mémoire master Département Informatique, Université de Bejaia. 2012.
- [7] Christian Draux , Les réseaux.2006.
- [8] Soumia chelihi.les équipements d'interconnexion, Mémoire master Département Informatique,université de Guelma.2015.
- [9] Pujolle GUY., « Les Réseaux », Eyrolles éditions, 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] LI, T., COLE, B., MORTON, P., et al. RFC2281: Cisco Hot Standby Router Protocol (HSRP). 1998.
- [13] Khaled TRABELSI and Haythem AMARA. Mise en place des réseaux LAN interconnectés en redondance par 2 réseaux WAN. Thèse, Université Virtuelle de Tunis, 2011.
- [14] Richard Froom, Balaji Sivasubramanian, and Erum Frahim. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide : Foundation Learning for SWITCH 642-813. Cisco Press, 2010.
- [15] VETRISLVAN, 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.edrawsoft.com/fr/network-protocol.html>.

[W2] <https://www.astarox.com/blog/configuration-redondance-routeurs-cisco-vrrp-hsrp-b50.html#:~:text=La%20redondance%20de%20routeurs%20est,r%C3%A9seau%2C%20il%20existe%20deux%20protocoles>.

[W3] <https://www.supinfo.com/articles/single/596-introduction-au-protocole-hsrp>.

Résumé

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

Mots clés : VTP, VLAN, PACKET TRACER.

Abstract

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

Keywords: VTP, VLAN, PACKET TRACER