

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

Université A. Mira de Béjaïa
Faculté de la Technologie
Département d'Automatique, Télécommunication et d'Electronique



Mémoire de fin d'études

En vue de l'obtention du diplôme de Master Télécommunications.

Thème :

Equilibrage de charge du réseau LAN vers les applications et serveurs

Présenté par :
M^{lle} SLIM Ouezna.
M^{lle} ZATOUT Inas.

Encadré par :
Dr.TOUNSI Mohamed
Mr.BEKNADJ Dalil

Soutenu le 18 Juin 2023 devant le jury composé de :

Promotion : 2022/2023

** Remerciements **

Nous exprimons nos profondes gratitudes envers nos parents et familles bien-aimés pour leur soutien inconditionnel et leurs encouragements tout au long de notre parcours. Leur présence et leur confiance ont été des éléments essentiels qui nous ont permis d'atteindre cette étape importante de nos études.

Nous tenons à remercier chaleureusement nos encadrants universitaires, Monsieur TOUNSI mohamed et Monsieur BEKNADJ Dalil, pour leur confiance, leurs encouragements constants et leurs conseils précieux qui ont grandement contribué à la réalisation de notre travail.

Nous souhaitons également exprimer notre gratitude envers le personnel de l'entreprise CEVITAL Bejaia, en particulier Monsieur SLIMANI Mennad, notre encadrant de stage. Sa patience, son sérieux et sa disponibilité tout au long de notre stage ont été très appréciés. Nos sincères remerciements vont également à nos professeurs à l'université de Bejaia pour leur enseignement solide et leurs précieuses connaissances théoriques qui ont constitué les bases de notre mémoire.

Enfin, nous tenons à remercier toutes les personnes qui ont apporté leur aide, de près ou de loin, à l'élaboration de notre mémoire de fin d'études. Leur contribution a été inestimable et nous sommes reconnaissants pour leur soutien et leur implication. Nous sommes conscients que sans l'appui et la collaboration de toutes ces personnes, nous n'aurions pas pu accomplir ce travail. Nous leur adressons nos plus sincères remerciements et notre profonde reconnaissance pour leur précieuse contribution à notre parcours académique.

Cordialement, ZATOUT inas et SLIM ouezna

※ *Dédicaces* ※

Je dedie ce travail,

A ma très chère maman,

Qui a œuvré pour ma réussite, pour toute son assistance et sa présence dans ma vie.

A mon très cher papa,

Qui peut être fier et trouver ici le résultat de longues années de sacrifices pour m'aider à avancer dans la vie.

Que se travail traduise ma gratitude et mon affection à toi qui est le meilleur papa au monde.

A mon très cher mari,

Qui m'a toujours soutenu et qui m'a offert tous les moyens pour réussir.

A Mon frère et mes deux sœurs, en particulier MANEL qui sans elle ce travail n'aurait pas eu lieu.

Mes professeurs de l'université qui doivent voir dans ce travail la fierté d'un savoir bien acquis.

A Mon binôme, pour sa sympathie et son sérieux.

Merci!

Inas

✧ Dédicaces ✧

Tout d'abord, je tiens à remercier DIEU De m'avoir donné la force et le courage de mener à bien ce modeste travail.

Je tiens à dédier cet humble travail à :

A ma tendre mère et mon très cher père .

A mes sœurs et à mon frère.

A tous les professeurs que ce soit du primaire, du moyen, du secondaire ou de l'enseignement supérieur.

A mon binôme Inas pour sa patience et son sérieux.

*A tous ceux qui ont eu et qui ont confiance en nous .
Merci !*

Ouezna

Table des matières

Table des matières	i
Table des figures	iv
Notations et symboles	vii
Introduction générale	1
1 <i>Rappels sur les réseaux informatiques</i>	3
1.1 Introduction	3
1.2 Définitions et Notions de base	3
1.2.1 Un réseau informatique	3
1.2.2 Fonctionnalités d'un réseau informatique	3
1.3 Architecture d'un réseau informatique	4
1.3.1 Architecture client-serveur	4
1.3.2 Architecture pair à pair (P2P)	5
1.4 Topologie d'un réseau informatique	5
1.5 Types de réseau informatique d'entreprise	7
1.6 Caractéristiques des réseaux	8
1.6.1 Support de transmission	8
1.6.2 Modes de transmission	8
1.6.3 Les équipements réseau	10
1.7 Technologie VLAN (Virtual Local Area Network)	12
1.8 Modèles de références OSI (Open Systems Interconnection)	14
1.9 Les protocoles réseaux	15
1.9.1 Protocole Spanning Tree (STP) :	15
1.9.1.1 états STP :	15
1.9.1.2 Configuration du protocole Spanning Tree (STP) :	16
1.9.2 DHCP (Dynamic Host Control Protocol)	16

1.9.3	Technologie Etherchannel	17
1.9.4	Serveur DNS	17
1.9.5	HSRP(Hot Standby Routing Protocol)	17
1.9.6	Le VTP (VLAN Trunking protocol)	18
1.10	Conclusion	18
2	<i>Problème d'équilibrage de charge sur le réseau informatique de CEVITAL</i>	19
2.1	Introduction	19
2.2	Partie 1 : Historique de cevital	19
2.2.1	Présentation de l'entreprise	19
2.2.2	Historique de Cevital agro-industrie	20
2.2.3	Infrastructure de l'entreprise	20
2.2.4	Architecture du réseau CEVITAL	21
2.2.5	Equipements utilisés dans l'architecture CEVITAL	23
2.3	Partie 2 : Architecture du réseau local existant de CEVITAL	25
2.4	Partie 3 : Définition de Cisco paquet tracer et les configurations du réseau existant	26
2.4.1	Cisco packet tracer	26
2.4.2	Configuration des équipements du réseau existant	26
2.5	Partie 4 : problématique de CEVITAL et la solution qu'on propose	34
2.5.1	Critique du réseau existant	34
2.5.2	Problématique :	34
2.5.3	Solution proposée :	35
2.6	Conclusion :	35
3	<i>Proposition et configuration d'une nouvelle architecture réseau</i>	36
3.1	Introduction	36
3.2	Architecture proposée	36
3.3	Configuration des équipements	38
3.3.1	Configuration des hostname et sécurité	38
3.3.2	Création des VLANs	40
3.3.3	Configuration des interfaces VLANs	41
3.3.4	Configuration du DHCP	43
3.3.5	Configuration des liens Trunk	46
3.3.6	Activation du VTP	47
3.3.7	Configuration STP	47
3.3.8	Configuration du HSRP	48
3.4	Vérification de la communication	49

3.5 Conclusion 50

Conclusion et perspective **51**

Bibliographie **52**

Table des figures

1.1	Architecture client-serveur	4
1.2	Architecture entre pairs	5
1.3	Topologie de bus	5
1.4	Topologie en anneau	6
1.5	Topologie en étoile	6
1.6	Topologie de maillage	7
1.7	Types de réseau informatique [21]	8
1.8	La liaison simplex	9
1.9	La liaison half-duplex	9
1.10	La liaison full duplex	10
1.11	La carte réseau.[19]	10
1.12	Les répéteurs.	11
1.13	Le pont.	11
1.14	Le commutateur	12
1.15	La passerelle.	12
1.16	Le routeur.	12
1.17	Vlan	13
1.18	Model OSI	14
2.1	Architecture du réseau CEVITAL [20].	22
2.2	Le Cisco Catalyst 9200 [19].	24
2.3	Architecture du réseau local existant de CEVITAL [20].	25
2.4	Cisco packet tracer.	26
2.5	Configuration des Hostname	27
2.6	Creation des VLANs.	27
2.7	Vérification des VLANs.	28
2.8	Configuration des interfaces VLANs.	28
2.9	Vérification des interfaces VLANs.	29
2.10	Configuration du DHCP.	29

2.11	Vérification de l'activation du DHCP.	30
2.12	Configuration des trunk.	30
2.13	Verification des trunk.	31
2.14	Configuration en mode server.	31
2.15	Configuration en mode client.	32
2.16	Verification des configurations VTP en mode server.	32
2.17	Verification des configurations VTP en mode client.	32
2.18	Verification adresse Ip par DHCP	33
2.19	Test intra VLAN	33
2.20	Test inter VLAN	34
3.1	Nouvelle architecture.	37
3.2	Configuration des hostname	38
3.3	Sécurité du mode enable et creation des session.	38
3.4	Verification des sécurités.	39
3.5	Sécurité des ports.	39
3.6	Le Bpduguard.	40
3.7	Création des VLANs dans le score1.	40
3.8	Création dans VLANs dans le score2.	41
3.9	Vérification des VLANs.	41
3.10	Configuration des interfaces VLANs dans le score1	42
3.11	Configuration des interfaces VLANs dans le score2	42
3.12	Configuration des interfaces dans le reste des VLANs	42
3.13	Verification de la configuration des VLANs	43
3.14	Configuration du DHCP	43
3.15	Verification de la configuration DHCP.	44
3.16	Exclure les adresses du score1.	44
3.17	Exclure les adresses du score2.	45
3.18	Verification des adresses exclues dans le score1	45
3.19	Verification des adresses exclues dans le score2.	45
3.20	Configuration des switchs en mode trunk	46
3.21	Vérification de la configuration trunk dans le score1.	46
3.22	Vérification de la configuration trunk dans le score2.	47
3.23	Activation VTP dans le score1.	47
3.24	Verification du VTP	48
3.25	Configuration STP dans le score1	48
3.26	Configuration STP dans le score2.	48

3.27 Configuration HSRP dans le score1	49
3.28 Configuration HSRP dans le score2.	49
3.29 Ping entre PC5 et PC12.	50
3.30 Désactivation d'un port et ping.	50

Notations et symboles

LAN : Local Area Network.

MAN : Metropolitan Area Network.

WAN : Wide Area Network.

PAN : Personal Area Network.

OSI : Open System Interconnexion.

DHCP : Dynamique Host Configuration Protocol.

DSI : Direction du Système Informatique.

HSRP : Hot Standby Router Protocol.

IEEE : Institute of Electric and Electronique Engineer.

STP : Spanning Tree Protocol.

TCP : Transmission Control Protocol.

IP : Internet Protocol.

VLAN : Virtual Local Area Network.

VTP : Virtual Trunking Protocol.

WIFI : Wireless Fidelity.

WLAN : Wireless Local Area Network.

ETTD : Equipement Terminal de Traitement de Données.

ETCD : Equipement Terminal de Circuit de Données.

ID : Identifiant.

ADSL : Ligne d'Abonné Numérique Asymétrique.

VIP : Adresse IP Virtuelle.

DNA : Digital Network Architecture.

QoS : Quality Of Service (Qualité de service).

MAC : Media Access Control (Contrôle d'accès au support).

BPDU : Bridge Protocol Data Unit (Unité de données de protocole de pont).

FHRP : First Hop Redundancy Protocol (Protocole de redondance de premier saut).

PPP : Point-to-Point Protocol (Protocole point à point).

LLC : Logical Link Control (Contrôle de liaison logique).

VPN : Virtual Private Network (Réseau privé virtuel).

Introduction générale

L'arrivée des ordinateurs a rapidement mis en évidence la nécessité de partager les ressources entre les utilisateurs. Afin de répondre à ce besoin, l'idée de connecter plusieurs ordinateurs a émergé, donnant ainsi naissance aux premiers réseaux informatiques. La création d'un réseau informatique est devenue essentielle pour les entreprises, offrant divers avantages tels que le partage des données et des ressources, une flexibilité d'utilisation, une sécurité renforcée et une gestion efficace du réseau.

Le groupe algérien CEVITAL est une entreprise privée de grande envergure qui joue un rôle majeur dans l'économie du pays. Compte tenu de l'importance des informations échangées entre ses divers services, l'entreprise a décidé de moderniser l'infrastructure de son réseau informatique. Cependant, ce processus de modernisation a été confronté à plusieurs difficultés liées à une architecture mal distribuée et à un mauvais partage de ressources. En effet, divers problèmes tels que les collisions et les congestions dans le trafic de données ont été identifiés.

Durant un notre stage pratique au sein du complexe Cevital de Béjaia, nous avons pu vérifier une inadéquation de l'architecture existante vu la charge du réseau. Notre projet a ainsi consisté à proposer une nouvelle architecture sécurisée pour un meilleur équilibrage de la charge.

Nos investigations sont synthétisées dans le présent mémoire qui a été structuré comme suit :

- **Chapitre 1** est une revue de diverses notions de base des réseaux informatiques pour faciliter la suite de notre travail ;
- Dans le **chapitre 2** historique de cevital et la problématique que rencontre l'entreprise, nous allons présenter l'entreprise Cevital Bejaia, son historique et son infrastructure, nous allons configurer le réseau déjà existant de Cevital puis nous allons parler de la problématique de ce reseau et nous allons finir par proposer une solution pour ce problème ;
- Dans **chapitre 3** nous proposons une nouvelle configuration avec différents tests montrant l'amélioration et la correction des faiblesses de l'architecture existante avec des nouveaux protocoles tels que le STP et le HSRP ;
- Nous terminons par une conclusion générale où nous résumons notre apport à un problème

concret dans le secteur professionnel et nous présentons une synthèse des compétences que nous avons acquises tout au long de notre stage et de notre projet de fin d'études.

Rappels sur les réseaux informatiques

1.1 Introduction

Dans ce premier chapitre, nous rappelons quelques notions de base sur l'infrastructure des réseaux informatiques, notamment les différentes topologies et les architectures existantes.

1.2 Définitions et Notions de base

1.2.1 Un réseau informatique

Le réseau informatique fait référence à des appareils informatiques interconnectés qui peuvent échanger des données et partager des ressources entre eux. Ces appareils mis en réseau, utilisent des protocoles de communication pour transmettre des informations sur des technologies physiques ou sans fil.

1.2.2 Fonctionnalités d'un réseau informatique

Avec l'émergence des technologies Internet, les réseaux informatiques modernes sont devenus indispensables pour les entreprises. Les nouvelles solutions réseau offrent bien plus que la simple connectivité, une transformation numérique certaine et une meilleure réussite des entreprises contemporaines. Les capacités sous-jacentes des réseaux sont devenues plus programmables, automatisées et sécurisées. Les réseaux modernes peuvent remplir les fonctions suivantes :

★ **Fonctionner de façon virtuelle**

Il est possible de partitionner logiquement l'infrastructure physique sous-jacente d'un réseau pour créer plusieurs réseaux « superposés ». Dans un réseau informatique superposé, les nœuds sont connectés de manière virtuelle et les données peuvent être transmises entre

eux par différents chemins physiques. Par exemple, de nombreux réseaux d'entreprise sont superposés sur Internet.

★ S'intégrer à grande échelle

De nombreux réseaux informatiques sont définis par des logiciels. Le trafic peut être acheminé et contrôlé de manière centralisée à l'aide d'une interface numérique. Ces réseaux informatiques prennent en charge la gestion du trafic virtuel.

★ Garantir la sécurité des données

Les solutions de réseaux intègrent des fonctions de sécurité, telles que le chiffrement et le contrôle d'accès. Des solutions tierces, telles que des logiciels antivirus, des pare-feu et des logiciels anti-logiciels malveillants, peuvent être intégrées pour renforcer la sécurité du réseau.

1.3 Architecture d'un réseau informatique

La conception des réseaux informatiques relève de deux grandes catégories :

1.3.1 Architecture client-serveur

Dans ce type de réseau informatique, les nœuds peuvent être des serveurs ou des clients. Les nœuds serveur fournissent aux nœuds clients, des ressources telles que la mémoire, la puissance de traitement ou les données. Les nœuds serveur peuvent également gérer le comportement des nœuds clients. Les clients peuvent communiquer entre eux, mais ils ne partagent pas de ressources. Par exemple, dans les réseaux d'entreprise, certains appareils informatiques stockent des données et des paramètres de configuration et jouent le rôle de serveurs. Les clients peuvent accéder à ces données en adressant une requête à la machine serveur.[1]

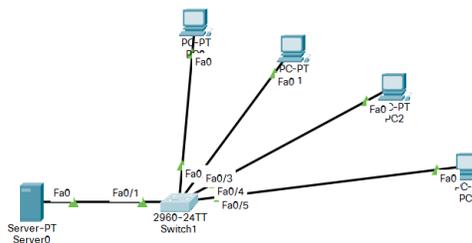


FIGURE 1.1 – Architecture client-serveur

1.3.2 Architecture pair à pair (P2P)

Dans l'architecture P2P, les ordinateurs connectés ont les mêmes pouvoirs et privilèges. Il n'existe aucun serveur central pour la coordination. Chaque appareil du réseau informatique peut agir en tant que client ou serveur. Chaque pair peut partager certaines de ses ressources, comme la mémoire et la puissance de traitement, avec l'ensemble du réseau informatique. Par exemple, certaines entreprises utilisent l'architecture P2P pour héberger des applications gourmandes en mémoire, comme le rendu graphique en 3D, sur plusieurs appareils numériques.[1]

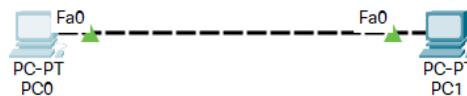


FIGURE 1.2 – Architecture entre pairs

1.4 Topologie d'un réseau informatique

Topologie de bus

Dans ce type de réseau informatique, chaque noeud est connecté à un autre noeud unique et la transmission des données se fait dans un seul sens sur les connexions du réseau.[2]

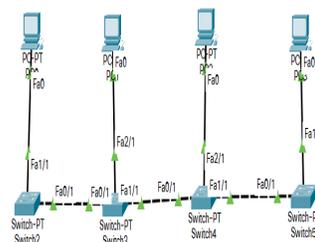


FIGURE 1.3 – Topologie de bus .

Topologie en anneau

Le réseau est constitué d'un anneau où chaque noeud est relié à deux autres noeuds, permettant la circulation des données dans les deux sens. Cependant, si un seul noeud tombe en panne, cela peut entraîner la défaillance de l'ensemble du réseau.[2]

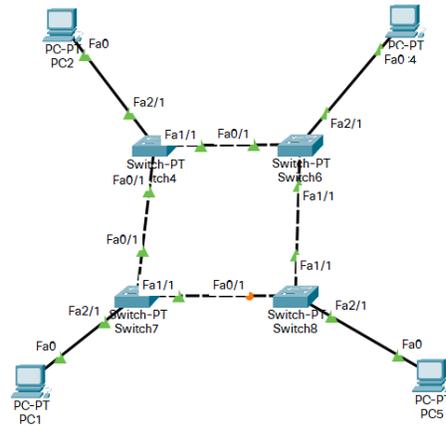


FIGURE 1.4 – Topologie en anneau

Topologie en étoile

Un noeud de serveur central est relié à plusieurs appareils du réseau client. Cette topologie est plus performante, car les données n'ont pas à passer par chaque noeud. Elle est aussi plus fiable. [2]

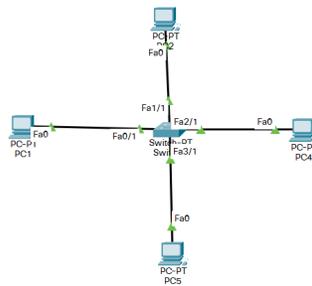


FIGURE 1.5 – Topologie en étoile .

Topologie de maillage

Dans une topologie de maillage complet, chaque noeud du réseau est connecté à plusieurs autres noeuds, créant ainsi un réseau dense et interconnecté. Chaque noeud peut communiquer directement avec tous les autres noeuds sans avoir à passer par des noeuds intermédiaires. [2]

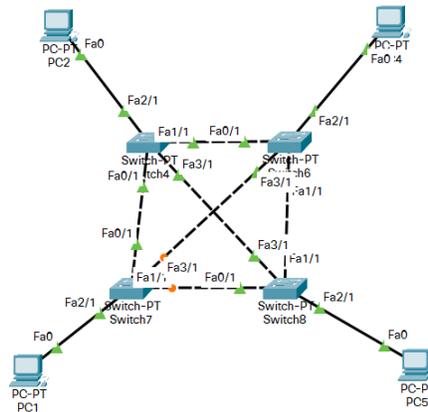


FIGURE 1.6 – Topologie de maillage

1.5 Types de réseau informatique d'entreprise

✓ Réseau local (LAN)

Un réseau local est un système qui relie des ordinateurs et des appareils dans une zone limitée en termes de taille et de portée géographique. Il est couramment utilisé pour relier les dispositifs situés dans un même bureau ou bâtiment, et est souvent utilisé par les petites entreprises ou pour des projets de prototypage à petite échelle.[3]

✓ Réseaux étendus (WAN)

Un réseau d'entreprise qui couvre plusieurs bâtiments, villes ou même pays est appelé réseau étendu (WAN). Contrairement aux réseaux locaux qui sont conçus pour des transmissions de données à grande vitesse à courte portée, les réseaux étendus sont conçus pour des communications à longue distance fiables et sécurisées. Le SD-WAN, également connu sous le nom de WAN défini par logiciel, est une architecture WAN virtuelle contrôlée par des technologies logicielles. Le SD-WAN offre des services de connectivité plus flexibles et fiables qui peuvent être contrôlés au niveau de l'application, sans compromettre la sécurité et la qualité du service.[3]

✓ Réseaux métropolitains (MAN)

Les MAN (Métropolitain Area Network) représentent une interconnexion de plusieurs réseaux locaux répartis sur différents sites dans une zone urbaine dont l'étendue géographique n'excède pas 200 km. Autrement dit, ils couvrent une métropole (ville) à des débits supérieurs à 1000 Mb/s. [4]

✓ Personal Area Network (PAN)

Il fait référence à un réseau restreint d'appareils informatiques, généralement à usage

personnel. Les bus les plus courants sont l'USB, le Bluetooth ou les technologies sans fil comme l'IR (infrarouge).

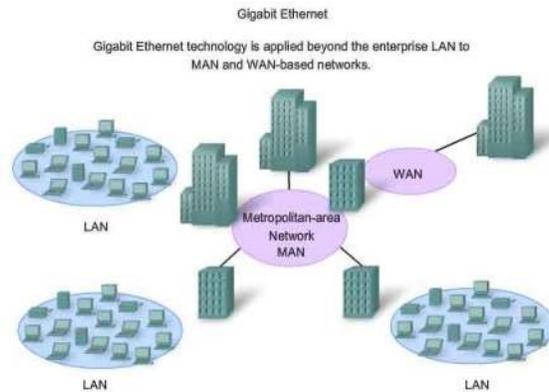


FIGURE 1.7 – Types de réseau informatique [21]

1.6 Caractéristiques des réseaux

Un réseau est caractérisé par ses éléments principaux : une topologie (physique et logique) ainsi que le support de transmission utilisé, le matériel d'interconnexion et enfin les méthodes de transmission.

1.6.1 Support de transmission

Il existe plusieurs supports de transmission tels que le câble coaxial, la paire de fils torsadés, la fibre optique, les liaisons infrarouges et les ondes hertziennes (pour des réseaux WLAN : LAN sans fils).

1.6.2 Modes de transmission

Pour une transmission donnée sur une voie de communication entre deux machines la communication peut s'effectuer de différentes manières. La transmission est caractérisée par le sens des échanges, le mode de transmission et la synchronisation (entre émetteur et récepteur). Selon le sens des échanges, on distingue 3 modes de transmission :

◆ **La liaison simplex** est un type de liaison dans laquelle les données sont transmises dans un seul sens, de l'émetteur vers le récepteur. Elle est utilisée lorsque les données n'ont pas

besoin de circuler dans les deux sens, comme dans le cas de la communication entre un ordinateur et une imprimante ou entre une souris et un ordinateur.

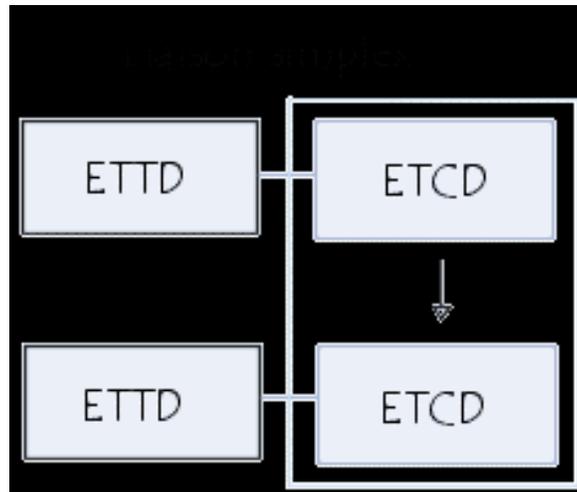


FIGURE 1.8 – La liaison simplex

- ◆ **La liaison half-duplex** (parfois appelée liaison à l'alternat ou semi-duplex) caractérise une liaison dans laquelle les données circulent dans un sens ou l'autre, mais pas les deux simultanément. Ainsi, avec ce genre de liaison chaque extrémité de la liaison émet à son tour. Ce type de liaison permet d'avoir une liaison bidirectionnelle utilisant la capacité totale de la ligne.

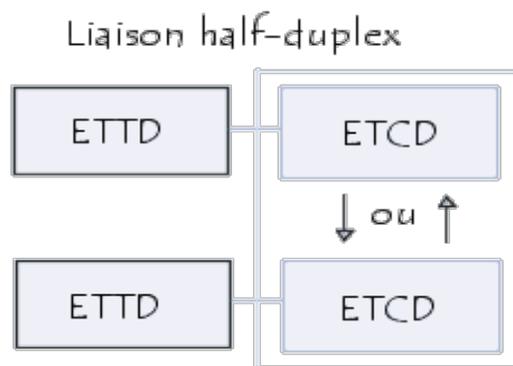


FIGURE 1.9 – La liaison half-duplex .

- ◆ **La liaison full-duplex** (appelée aussi duplex intégral) est utilisée dans des situations où les données doivent être transmises dans les deux sens, mais pas en même temps. Cela permet d'utiliser pleinement la capacité de la ligne de communication, mais peut entraîner des retards si les extrémités doivent attendre leur tour pour transmettre. Par exemple, la plupart des communications par radio utilisent des liaisons half-duplex

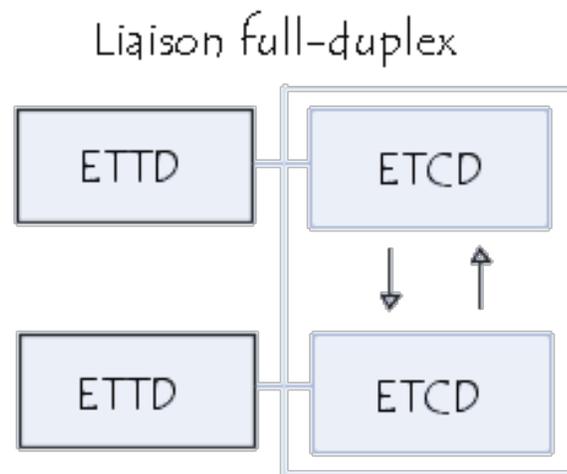


FIGURE 1.10 – La liaison full duplex

1.6.3 Les équipements réseau

On appelle ainsi les matériels connectés au réseau, mais qui ne sont pas des hôtes. Ils portent une appellation différente selon leur niveau d'intelligence ou le rôle qu'ils jouent, qui sont : [9]

- **La carte réseau**

C'est l'interface physique entre l'ordinateur et le support de communication. Pour qu'un ordinateur soit mis en réseau, il doit être muni d'une carte réseau.

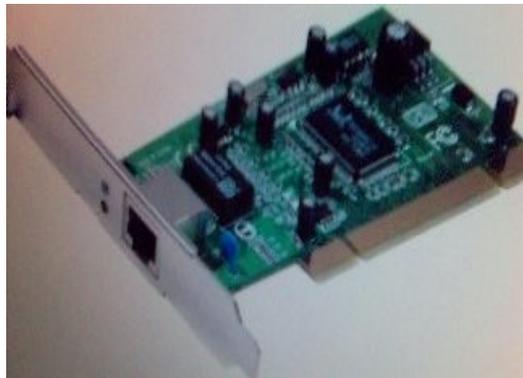


FIGURE 1.11 – La carte réseau.[19]

- **Le concentrateur (hub en anglais)**

Équipement physique à plusieurs ports, servant à relier plusieurs ordinateurs entre eux. Son rôle est de relayer les données reçues sur un port vers l'ensemble des ports.

- **Les répéteurs**(repeater en anglais) :

Équipement servant à régénérer le signal entre deux nœuds pour le but d'étendre la distance du réseau. Il est à noter qu'on peut utiliser un répéteur pour relier deux supports de transmission de types différents.



FIGURE 1.12 – Les répéteurs.
[19]

- **Pont (Bridge en anglais)**

Équipement servant à relier deux réseaux utilisant le même protocole. Quand il reçoit la trame, il est en mesure d'identifier l'émetteur et le récepteur ; comme ça il dirige la trame directement vers la machine destinataire.



FIGURE 1.13 – Le pont.
[19]

- **le commutateur**(switch en anglais)

C'est un équipement multiport comme le concentrateur. Il sert à relier plusieurs équipements informatiques entre eux. Sa seule différence avec le hub, c'est sa capacité 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.

- **Passerelle (Gateway en anglais)**

Système matériel et logiciel servant à relier deux réseaux utilisant deux protocoles et/ou architectures différents ; comme par exemple un réseau local et internet. Lorsqu'un utilisateur distant contact un tel dispositif, celui-ci examine sa requête, et si celle-ci correspond aux règles que l'administrateur réseau a défini, la passerelle crée un pont entre les deux réseaux. Les informations ne sont pas directement transmises, elles sont plutôt traduites pour assurer la transmission tout en respectant les deux protocoles.



FIGURE 1.14 – Le commutateur
[19]

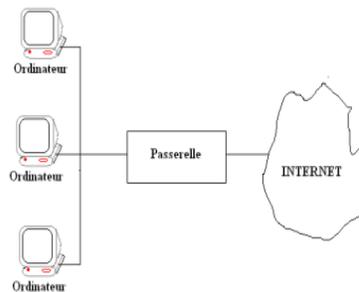


FIGURE 1.15 – La passerelle.
[22]

- **Routeur (Router en anglais)**

Matériel de communication de réseau informatique qui a pour rôle d'assurer l'acheminement des paquets, le filtrage et le control du trafic. Le routage est la fonction qui consiste à trouver le chemin optimal que va emprunter le message depuis l'émetteur vers le récepteur.



FIGURE 1.16 – Le routeur.
[19]

1.7 Technologie VLAN (Virtual Local Area Network)

La technologie VLAN "virtualise" un LAN, un réseau local. La virtualisation d'un LAN consiste en la séparation entre, d'une part, l'infrastructure physique et, d'autre part, les services de couche 2 "liaison de données" fournis par les commutateurs. Soit une seule infrastructure physique supporte plusieurs LAN distincts (VLANs). [10]

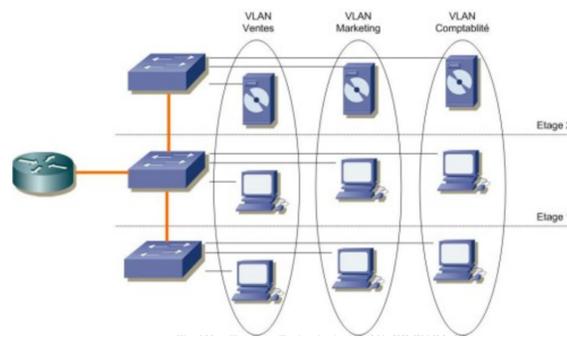


FIGURE 1.17 – Vlan

La technologie VLAN (LAN virtuel) permet de gérer et de maintenir plusieurs réseaux locaux (LANs), soit séparés par du routage, sur une seule et même infrastructure physique commutée.

Par analogie, on peut considérer qu'un VLAN est un commutateur virtuel sur plusieurs commutateurs physiques. On peut aussi considérer qu'un VLAN correspond à un domaine de diffusion (Broadcast) dans lequel on déploie un adressage IP cohérent comme un LAN.[10]

On citera brièvement les avantages acquis de la technologie VLAN [10] :

- Indépendance de la couche physique
- Contribue à la séparation des flux et la sécurité de l'infrastructure.
- Flexibilité : allocation dynamique des utilisateurs dans un réseau indépendamment de l'emplacement.
- Facilité de gestion : QoS, classification, routage, filtrage.
- Performances : diminution de la taille des domaines de Broadcast.
- Coût abordable.

A titre d'inconvénients, on peut citer :

- Architecture adaptées
- Investissements dans l'infrastructure
- Montées en compétences du personnel

1.8 Modèles de références OSI (Open Systems Interconnection)

Le modèle de référence OSI est une représentation abstraite en couches servant de guide à la conception des protocoles réseau. Il divise le processus de réseau en sept couches logiques, chacune comportant des fonctionnalités uniques et se voyant attribuer des services et des protocoles spécifiques[11].

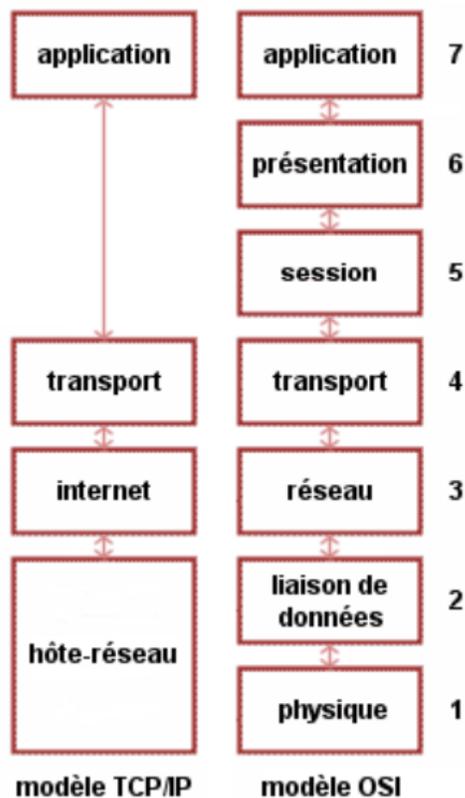


FIGURE 1.18 – Model OSI

- Couche physique : c'est des signaux : modulation, puissance, support de transmission (câble, fibre optique).
- Couche liaison de donnée : établissement, maintien et libération des connexions entre les éléments du réseau, détection et correction des erreurs.
- Couche réseau : responsable de l'adressage et le routage.

- Couche transport : transfert entre utilisateurs (transparence).
- Couche session : optimisation et réglage des sessions (reprise de transfert).
- Couche présentation : compression et représentation (poids fort à gauche ou adroite).
- Couche application : offrir aux logiciels des standards d'accès aux réseaux (fichier virtuel).

1.9 Les protocoles réseaux

1.9.1 Protocole Spanning Tree (STP) :

Le protocole Spanning Tree (STP) est un protocole de couche 2 qui s'exécute sur des ponts et des commutateurs. La spécification pour STP est IEEE 802.1D. L'objectif principal de STP est de s'assurer que l'on ne crée pas de boucles lorsque des chemins redondants existent dans le réseau. [12]

1.9.1.1 états STP :

- **Blocage** : après l'initialisation, STP démarre l'état de blocage pour empêcher la formation de boucles de pontage. Le port reçoit les trames BPDU (Bridge Protocol Data Unit) pour déterminer l'emplacement et l'ID racine du commutateur de pont racine et quels rôles de port chaque port de commutateur doit assumer dans la topologie STP active finale.
- **Ecoute** : le port passe à l'état d'écoute s'il peut être sélectionné comme port racine. Le port du switch reçoit les trames BPDU, transmet ses propres trames BPDU et informe les commutateurs adjacents que le port du commutateur se prépare à participer au topologie active.
- **Apprentissage** : après la période de délai de transfert, le port passe à l'état d'apprentissage sous forme d'état d'écoute. L'interrupteur apprend les adresses MAC et l'ajoute à la table d'adresses. Le port continue d'envoyer la trame BPDU comme avant. Le port se prépare à participer au transfert de trame et commence à remplir la table d'adresses MAC
- **Transfert** : après une autre période de délai de transfert, le port passe à l'état de transfert et il est considéré comme partie du réseau actif. Il transmet les trames de données et envoie et reçoit des trames BPDU.
- **Désactivé** : dans cet état, le port est désactivé par l'administration ou a échoué en raison d'une condition critique du réseau. Cela fait qu'il ne participe pas à la transmission des trames.

1.9.1.2 Configuration du protocole Spanning Tree (STP) :

Tout d'abord, le pont racine principal doit être configuré. Le commutateur avec une valeur de priorité numérique inférieure doit être le pont racine principal. Ensuite, le pont racine secondaire doit être configuré dans le commutateur avec une valeur de priorité numérique plus élevée. Les priorités peuvent être définies manuellement ou la priorité par défaut peut être utilisée, mais il est important de faire attention aux priorités lors de la configuration. Le spanning tree classique IEEE 802.1D consomme 15 secondes pour l'écoute, 15 secondes pour l'apprentissage, délai d'attente maximal de 20 secondes, ce qui est très lent. Pour surmonter cette longue convergence un meilleur protocole est développé nommé Rapid Spanning Tree Protocol (RSTP) qui est IEEE 802.1w. [12]

1.9.2 DHCP (Dynamic Host Control Protocol)

Ce protocole permet aux administrateurs de réseaux TCP/IP de configurer les postes clients de façon automatique. Il a été utilisé par les fournisseurs d'accès à l'Internet par le câble, mais a été abandonné au profit d'une connexion point à point type PPP, comme pour l'ADSL. DHCP reste cependant un protocole de configuration de clients extrêmement pratique sur un réseau local Ethernet.

DHCP offre les avantages suivants.[13]

- **Configuration d'adresse IP fiable**

DHCP réduit les erreurs de configuration causées par la configuration manuelle des adresses IP, telles que les erreurs typographiques ou les conflits d'adresses provoqués par l'affectation d'une adresse IP à plusieurs ordinateurs en même temps.

- **Administration réseau réduite**

DHCP inclut les fonctionnalités suivantes pour réduire l'administration réseau :

- ◇ Configuration TCP/IP centralisée et automatisée.
- ◇ Possibilité de définir des configurations TCP/IP à partir d'un emplacement central.
- ◇ Possibilité d'affecter une plage complète de valeurs de configuration TCP/IP supplémentaires au moyen d'options DHCP.
- ◇ Gestion efficace des modifications d'adresses IP pour les clients qui doivent être mis à jour fréquemment, comme ceux des appareils portables qui se déplacent vers différents emplacements sur un réseau sans fil.
- ◇ Le transfert des messages DHCP initiaux à l'aide d'un agent de relais DHCP, ce qui élimine la nécessité d'un serveur DHCP sur chaque sous-réseau

1.9.3 Technologie Etherchannel

EtherChannel est une technologie d'agrégation de liens qui permet d'assembler plusieurs liens physiques Ethernet identiques en un seul lien logique. On l'appelle aussi bonding, LAG, etherchannel, ou encore portchannel. Le but est d'augmenter la vitesse et la tolérance aux pannes entre les commutateurs, les routeurs et les serveurs. Elle permet de simplifier une topologie Spanning-Tree en diminuant le nombre de liens. Un lien EtherChannel groupe de 2 à 8 liens actifs de 100 Mbit/s, 1 Gbit/s et 10 Gbit/s, plus éventuellement de 1 à 8 liens inactifs en réserve qui deviennent actifs quand des liens actifs sont coupés. EtherChannel est principalement utilisé sur la dorsale du réseau local, dans le "Switch Block" entre la couche Access et Distributions, mais on peut aussi l'utiliser pour connecter des postes d'utilisateurs, des serveurs. La technologie EtherChannel a été inventée par la société Kalpana au début des années 1990. Cette société a ensuite été acquise par Cisco Systems en 1994. En 2000, l'IEEE a publié le standard 802.3ad, qui est une version ouverte d'EtherChannel.[14]

1.9.4 Serveur DNS

Un serveur DNS (Domain Name System, système de nom de domaine) est un serveur informatique qui permet de traduire les noms de domaine en adresses IP. Lorsque vous entrez une adresse Web dans votre navigateur, le serveur DNS est chargé de trouver l'adresse IP correspondante pour que votre navigateur puisse charger le site Web demandé. Les serveurs DNS sont répartis à travers le monde et travaillent en réseau pour fournir un accès rapide et fiable aux sites Web. En résumé, le serveur DNS est un élément essentiel de l'infrastructure d'Internet.[15]

1.9.5 HSRP(Hot Standby Routing Protocol)

C'est un protocole de routage de premier hop redondant (FHRP) développé par Cisco. Il permet à un groupe de routeurs de partager une adresse IP virtuelle (Virtual IP ou VIP) afin de fournir une redondance de passerelle par défaut pour les hôtes du réseau.

Un seul routeur du groupe est actif et traite le trafic entrant et sortant pour la VIP, tandis que les autres routeurs restent en attente (standby) et surveillent l'état de l'actif. Si le routeur actif tombe en panne, un des routeurs standby prendra en charge la VIP pour assurer la continuité de service.

HSRP est largement utilisé dans les réseaux d'entreprise pour fournir une haute disponibilité des passerelles par défaut et une redondance de routage pour les réseaux locaux (LAN).[16]

1.9.6 Le VTP (VLAN Trunking protocol)

Ce protocole permet en effet aux switches de diffuser les informations relatives aux VLANs pour les ports trunk à l'ensemble du réseau. Il permet ainsi de simplifier l'administration des VLANs en assurant une configuration centralisée des VLANs à travers le réseau. Il fonctionne avec une architecture client-serveur.[17]

- Mode de fonctionnement :

Le protocole VTP (VLAN Trunking Protocol) est utilisé pour administrer les VLANs sur un réseau en permettant leur diffusion sur l'ensemble des ports trunk des switches. Il est propriétaire de la marque CISCO et suit une architecture client-serveur. Le serveur maintient une table des VLANs déclarés, qui est diffusée aux clients appartenant au même domaine VTP. Toute modification apportée à la table est répercutée sur l'ensemble des clients, ce qui permet à tous les VLANs définis sur le serveur de circuler sur les ports trunk des switches clients (sauf si des configurations spécifiques ont été appliquées sur les interfaces).

Les matériels peuvent être en mode :

- ▶ **Server** : Il est associé à un domaine VTP. La déclaration des VLANs s'effectue sur le serveur. Il tient à jour la liste des VLANs déclarés et la diffuse à l'ensemble des clients.
- ▶ **Client** : Il est associé à un domaine VTP. Il reçoit la liste des VLANs, il la propage aux autres clients auxquels il est connecté et met à jour sa propre liste.
- ▶ **Transparent** : Il est associé à aucun domaine VTP. Sa liste de VLAN est locale et n'est pas mis à jour lorsqu'il reçoit une trame VTP. Cependant il propage les listes de VLAN qu'il reçoit.

1.10 Conclusion

Dans ce chapitre nous avons présenté des rappels sur les réseaux informatiques, à savoir leurs objectifs, leur classification et leurs équipements. Nous avons également exposé les topologies, les architectures ainsi que les caractéristiques de ces réseaux.

Problème d'équilibrage de charge sur le réseau informatique de CEVITAL

2.1 Introduction

Dans ce chapitre, en premier lieu nous allons présenter l'entreprise cevital ainsi que son historique et les équipements utilisés dans son architecture. En second lieu nous allons exposer l'architecture actuelle de leur réseau. En troisième lieu nous allons définir le logiciel utilisé pour la création de cette architecture, puis nous allons monter les configurations établies sur celle-ci. En dernier nous allons donner des critiques sur ce réseau et la problématique qu'il rencontre.

2.2 Partie 1 : Historique de cevital

2.2.1 Présentation de l'entreprise

Cevital est un conglomérat algérien qui opère dans différents secteurs économiques, notamment l'agroalimentaire, la grande distribution, la sidérurgie, l'industrie automobile, la logistique et l'immobilier. Fondée en 1998 par l'homme d'affaires Issad Rebrab.

L'entreprise a connu une croissance rapide au fil des années et est aujourd'hui considérée comme l'un des plus grands conglomérats industriels d'Afrique. Elle emploie plus de 18 000 personnes à travers le monde et est présente dans plus de 25 pays, notamment en Europe, en Afrique et en Amérique du Nord.

Cevital Agro-Industrie dispose d'une usine à Béjaïa, une ville située sur la côte nord-est de l'Algérie. Cette usine est spécialisée dans la production d'huiles alimentaires et de sucre.

L'usine de Béjaïa dispose de capacités de production importantes. Elle peut produire jusqu'à 2 000 tonnes d'huile de tournesol par jour et 3 000 tonnes de sucre par jour. Elle emploie également plus de 1 000 personnes. Cevital Agro-Industrie a investi dans l'usine de Béjaïa afin de

moderniser ses installations et d'améliorer sa productivité. L'entreprise a notamment installé des équipements de pointe pour le raffinage de l'huile et le traitement du sucre.[18]

2.2.2 Historique de Cevital agro-industrie

Cevital Agro-Industrie a été créée en 2008 en tant que filiale de Cevital, le conglomérat industriel algérien fondé par Issad Rebrab. Depuis sa création, l'entreprise s'est développée rapidement pour devenir l'un des principaux acteurs du secteur agroalimentaire en Algérie.

En 2009, Cevital Agro-Industrie a acquis une usine de production d'huile de soja à Béjaïa, dans le nord-est de l'Algérie. Cette acquisition a permis à l'entreprise de se lancer dans la production d'huiles alimentaires.

En 2011, Cevital Agro-Industrie a lancé sa propre marque d'huiles alimentaires, appelée "Moulins Mahjoub". Cette marque est devenue très populaire en Algérie et est aujourd'hui largement distribuée dans le pays.

En 2013, l'entreprise a inauguré une nouvelle usine de production de sucre à Béjaïa. Cette usine a été construite avec des équipements de pointe pour garantir une qualité de production élevée.

Depuis sa création, Cevital Agro-Industrie s'est engagée dans des projets de développement de l'agriculture locale en Algérie, notamment en travaillant avec des agriculteurs locaux pour les aider à cultiver des matières premières destinées à ses productions. Elle a également investi dans la modernisation de ses installations pour améliorer sa productivité et sa compétitivité sur le marché.[18]

2.2.3 Infrastructure de l'entreprise

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

- raffineries de sucre.
- unité de sucre liquide.
- 1 raffinerie d'huile.
- 1 margarinerie.
- 1 unité de conditionnement d'eau minérale (se situe à Tizi Ouzou).

- 1 unité de fabrication et de conditionnement de boissons rafraichissantes.
- 1 conserverie.

Cevital est aujourd'hui le premier terminal de déchargement portuaire en Méditerranée. Ceci est dû à la possession de plusieurs silos portuaires ainsi que celle d'un terminal de déchargement d'une capacité de 2000 tonnes/heure.[18]

2.2.4 Architecture du réseau CEVITAL

Cevital a créé un vaste réseau interne pour connecter les différents bâtiments, unités de production et la direction du complexe. Ce réseau est composé de plusieurs éléments, notamment un backbone, un pare-feu et une zone démilitarisée (DMZ), une couverture Wi-Fi, un routeur et un centre de données qui héberge les serveurs de l'entreprise.

Le réseau de Cevital est constitué de plusieurs équipements, la plupart étant de marque Cisco, tels que des switches, des Catalysts et des routeurs. Ces équipements sont interconnectés entre eux à l'aide de fibre optiques ou de cables en cuivre.[18]

FOOD Bejaia High Level Design Overview

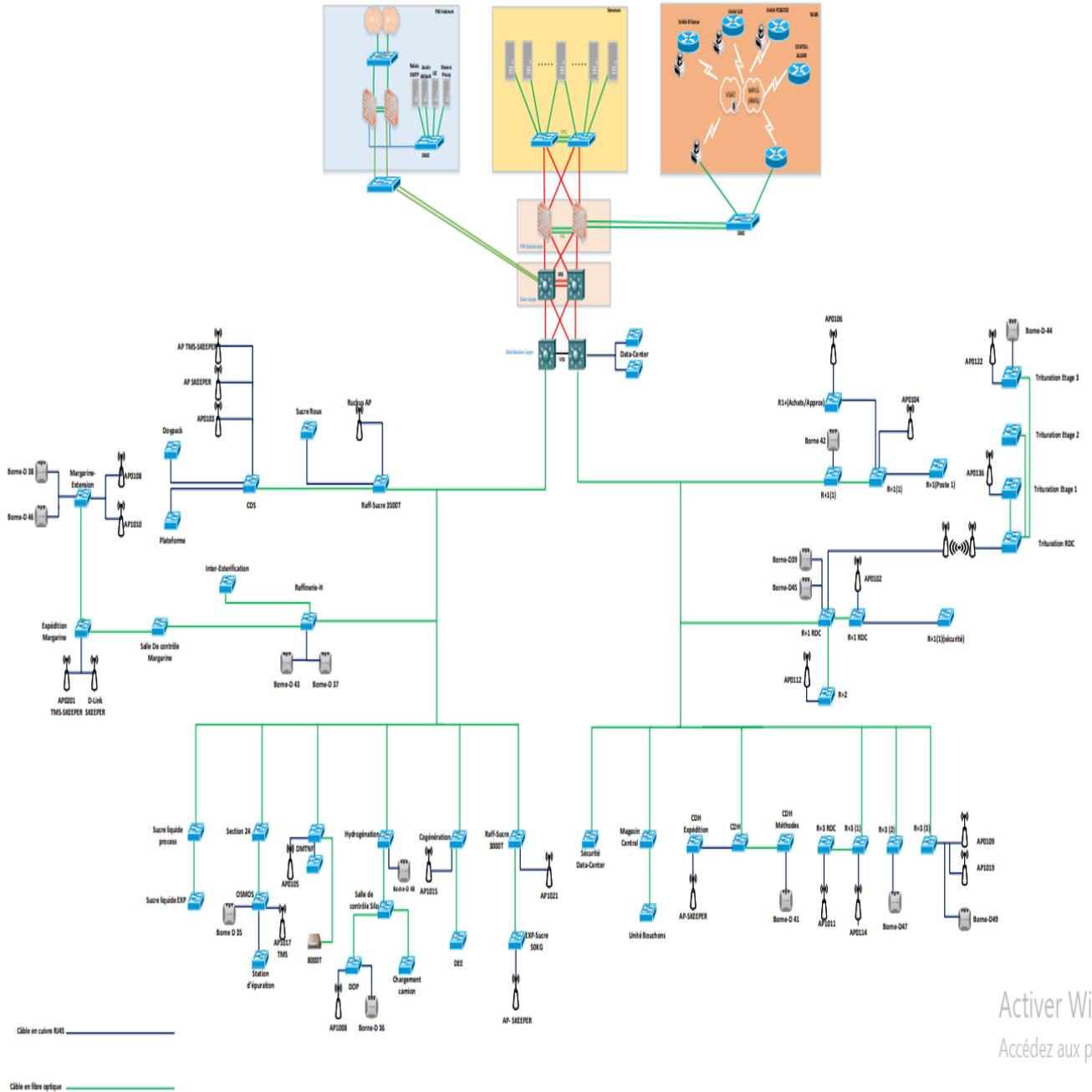


FIGURE 2.1 – Architecture du réseau CEVITAL [20].

2.2.5 Equipements utilisés dans l'architecture CEVITAL

- **Point d'accès WIFI :**

Pour assurer une couverture réseau sans fil dans certaines zones du complexe, l'entreprise a mis en place plusieurs points d'accès WIFI. Ce réseau sans fil peut atteindre une portée de 3000 mètres avec une vitesse de transfert allant jusqu'à 867 Mbits/s, utilisant une plage de fréquences qui varie de 2,5 GHz à 5 GHz.

- **Pare feu :**

Le pare-feu Palo Alto PA-3020 est un pare-feu de nouvelle génération conçu pour protéger les réseaux d'entreprise de taille moyenne à grande. Il utilise une approche de sécurité basée sur les applications pour identifier et contrôler le trafic réseau en fonction des applications qu'il utilise, plutôt que sur les ports et les adresses IP. Il est doté de fonctionnalités de prévention des intrusions, de détection de logiciels malveillants, de contrôle d'accès, de VPN et de gestion unifiée des menaces.

- **Data center :**

Le data center est une salle hautement sécurisée avec un accès restreint aux responsables et aux techniciens de la DSI. La température y est régulée grâce à un système de climatisation, la puissance est doublée et le bon fonctionnement des équipements est garanti. Chez Cevital, le data center est considéré comme le noyau central du réseau de l'entreprise et abrite plusieurs équipements tels que :

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

- **Le Cisco Catalyst 9200 :**

Est une gamme de commutateurs de réseau d'entreprise offrant une mise en réseau basé sur l'intention et une innovation matérielle et logicielle pour un ensemble plus large de déploiements. Ils simplifient la complexité, optimisent l'informatique et réduisent les coûts opérationnels grâce à l'intelligence, l'automatisation et l'expertise humaine de Cisco.

Les commutateurs Catalyst 9200 sont dotés de fonctionnalités de sécurité avancées, d'une résilience permettant à l'entreprise de fonctionner sans interruption, d'une capacité PoE+ complète, d'une redondance d'alimentation et de ventilateurs, et d'une bande passante d'empilage allant jusqu'à 160 Gbit/s. Ils sont la solution inégale pour un accès économique aux succursales. Les clients peuvent choisir entre Cisco DNA Center et la

surveillance cloud pour la gestion du réseau. Les commutateurs Catalyst 9200 sont une solution fiable et performante pour la mise en réseau d'entreprise offrant une sécurité de niveau entreprise, une disponibilité permanente, une résilience et une informatique simplifiée.



FIGURE 2.2 – Le Cisco Catalyst 9200 [19].

2.3 Partie 2 : Architecture du réseau local existant de CEVITAL

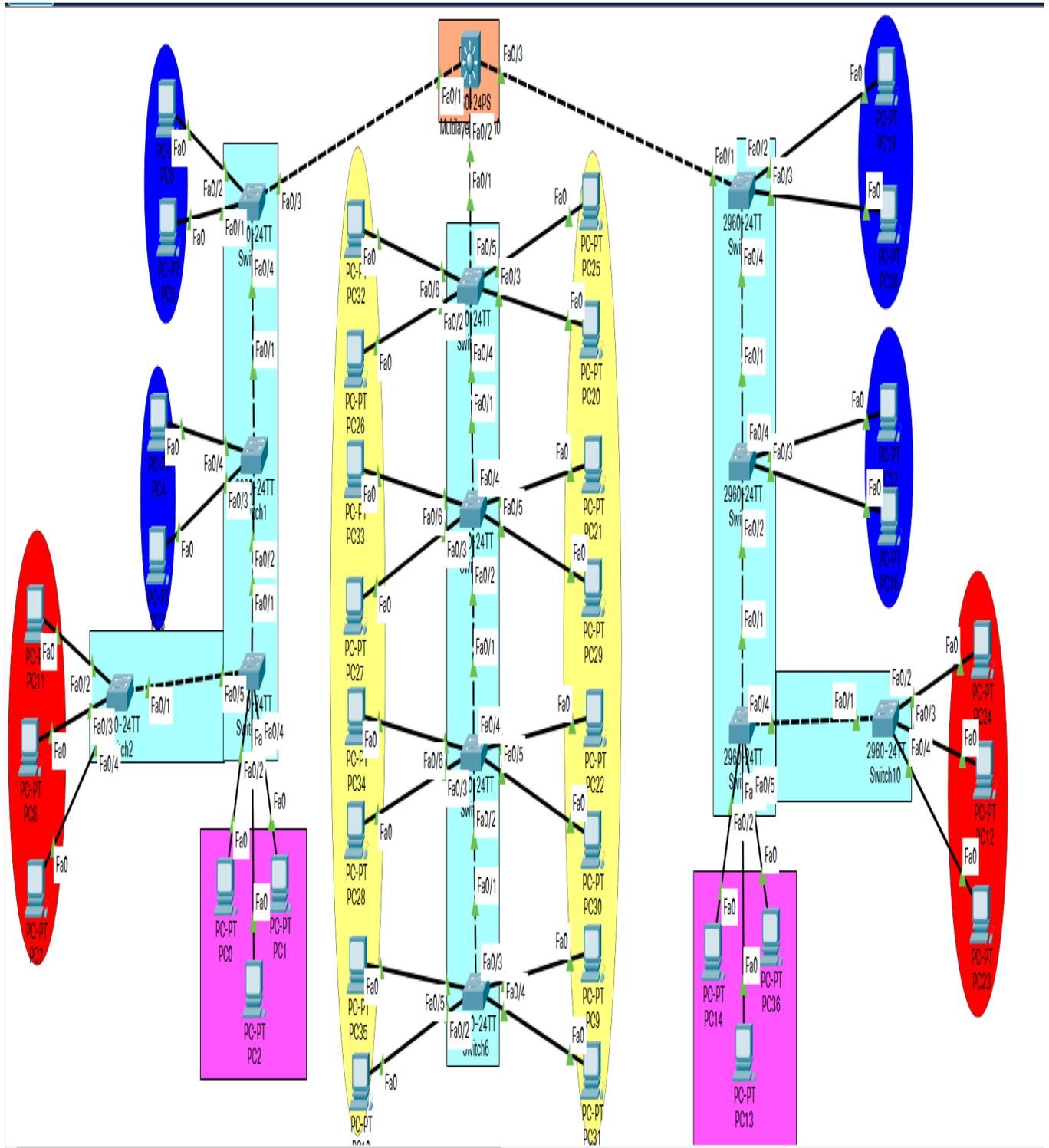


FIGURE 2.3 – Architecture du réseau local existant de CEVITAL [20].

2.4 Partie 3 : Définition de Cisco paquet tracer et les configurations du réseau existant

2.4.1 Cisco packet tracer

Cisco Packet Tracer est un logiciel qui permet de créer des réseaux virtuels, développé par une entreprise américaine nommée Cisco. Ce logiciel est compatible avec les systèmes d'exploitation Microsoft Windows, Linux et MacOS.

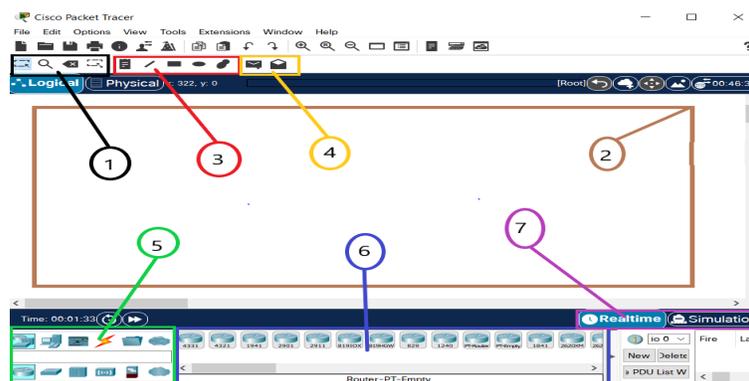


FIGURE 2.4 – Cisco packet tracer.

✓ Définition de emplacement :

- ◇ **Emplacement 1** : l'ensemble d'outils (sélection, inspection, suppression et redimensionner la forme).
- ◇ **Emplacement 2** : Partie où l'on crée l'architecture que l'on souhaite.
- ◇ **Emplacement 3** : annotation du schéma et palettes de dialogue.
- ◇ **Emplacement 4** : effectuer le ping entre les équipements.
- ◇ **Emplacement 5** : type des équipements.
- ◇ **Emplacement 6** : différents équipements existants.
- ◇ **Emplacement 7** : passage du mode réel au mode simulation.

2.4.2 Configuration des équipements du réseau existant

Nous allons utiliser une topologie de réseau qui implique un switch de niveau 3. Nous présenterons également un exemple de configuration pour chaque équipement de cette topologie.

- **Configuration des Hostname et sécurité**

Cette configuration a deux avantages principaux. Tout d'abord, elle permet de renommer les équipements avec des noms significatifs pour faciliter leur identification. Ensuite, elle permet de limiter l'accès aux personnes non autorisées en protégeant l'accès au mode privilégié avec un mot de passe robuste, renforçant ainsi la sécurité de l'équipement. Dans cette figure, nous avons pris l'exemple du switch Core de niveau 3 que nous avons renommé "Scoeur" et sécurisé avec un mot de passe "**slimzatout**".

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

FIGURE 2.5 – Configuration des Hostname

- **Création des VLANs**

Nous avons créé 10 VLAN au niveau du switch core, commençant du vlan 2 jusqu'au vlan 11 tout en leur attribuant les noms qui leur correspondent. Cette figure montre la manière de créer les vlans.

```
Scoeur(config)#vlan 2
Scoeur(config-vlan)#name GRH
Scoeur(config-vlan)#ex
Scoeur(config)#vlan 3
Scoeur(config-vlan)#name commercial
Scoeur(config-vlan)#ex
Scoeur(config)#vlan 4
Scoeur(config-vlan)#name administratif
Scoeur(config-vlan)#ex
Scoeur(config)#vlan 5
Scoeur(config-vlan)#name ingenierie
Scoeur(config-vlan)#ex
Scoeur(config)#vlan 6
Scoeur(config-vlan)#name telephonie
Scoeur(config-vlan)#ex
Scoeur(config)#vlan 7
Scoeur(config-vlan)#name reseau
Scoeur(config-vlan)#ex
Scoeur(config)#vlan 8
Scoeur(config-vlan)#name visio-conference
Scoeur(config-vlan)#ex
Scoeur(config)#vlan 9
Scoeur(config-vlan)#name finance
Scoeur(config-vlan)#ex
Scoeur(config)#vlan 10
Scoeur(config-vlan)#name voix
Scoeur(config-vlan)#ex
Scoeur(config)#vlan 11
Scoeur(config-vlan)#name management
Scoeur(config-vlan)#
```

FIGURE 2.6 – Creation des VLANs.

▷ A fin de monter tous les VLANs qui ont été créés nous avons utilisé la commande **show vlan brief**

```
2 GRH active
3 commercial active
4 administratif active
5 ingenierie active
6 telephonie active
7 reseau active
8 visio-conference active
9 finance active
10 voix active
11 management active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
Scoeux#
```

FIGURE 2.7 – Vérification des VLANs.

- Configuration des interfaces VLANs

La configuration des interfaces virtuelles des VLANs implique l'attribution d'une adresse IP à chaque interface, une opération qui se fait au niveau du switch Core. Nous avons configuré les interfaces des VLANs que nous avons crs auparavant.

La figure suivante illustre cette méthode en présentant la configuration des interfaces

```
Scoeux(config)#int Vlan 4
Scoeux(config-if)#
%LINK-5-CHANGED: Interface Vlan4, changed state to up
Scoeux(config-if)#ip add 10.50.4.254 255.255.255.0
Scoeux(config-if)#ex
Scoeux(config)#int Vlan 5
Scoeux(config-if)#
%LINK-5-CHANGED: Interface Vlan5, changed state to up
Scoeux(config-if)#ip add 10.50.5.254 255.255.255.0
Scoeux(config-if)#ex
Scoeux(config)#int Vlan 6
Scoeux(config-if)#
%LINK-5-CHANGED: Interface Vlan6, changed state to up
Scoeux(config-if)#ip add 10.50.6.254 255.255.255.0
Scoeux(config-if)#ex
Scoeux(config)#int Vlan 7
Scoeux(config-if)#
%LINK-5-CHANGED: Interface Vlan7, changed state to up
Scoeux(config-if)#ip add 10.50.7.254 255.255.255.0
Scoeux(config-if)#ex
Scoeux(config)#int Vlan 8
Scoeux(config-if)#
%LINK-5-CHANGED: Interface Vlan8, changed state to up
Scoeux(config-if)#ip add 10.50.8.254 255.255.255.0
Scoeux(config-if)#ex
Scoeux(config)#int Vlan 9
Scoeux(config-if)#
%LINK-5-CHANGED: Interface Vlan9, changed state to up
Scoeux(config-if)#ip add 10.50.9.254 255.255.255.0
Scoeux(config-if)#ex
Scoeux(config)#
Scoeux(config)#int Vlan 10
Scoeux(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
Scoeux(config-if)#ip add 10.50.10.254 255.255.255.0
Scoeux(config-if)#ex
Scoeux(config)#int Vlan 11
Scoeux(config-if)#
%LINK-5-CHANGED: Interface Vlan11, changed state to up
Scoeux(config-if)#ip add 10.50.11.254 255.255.255.0
Scoeux(config-if)#ex
```

FIGURE 2.8 – Configuration des interfaces VLANs.

Une fois toutes les interfaces des VLAN configurées, nous avons utilisé la commande "**show running-config**" pour vérifier toutes les interfaces, dont les résultats sont présentés dans la figure

```
interface Vlan2
  mac-address 0060.3ecc.ab01
  ip address 10.50.2.254 255.255.255.0
!
interface Vlan3
  mac-address 0060.3ecc.ab02
  ip address 10.50.3.254 255.255.255.0
!
interface Vlan4
  mac-address 0060.3ecc.ab03
  ip address 10.50.4.254 255.255.255.0
!
interface Vlan5
  mac-address 0060.3ecc.ab04
  ip address 10.50.5.254 255.255.255.0
!
interface Vlan6
  mac-address 0060.3ecc.ab05
  ip address 10.50.6.254 255.255.255.0
!
interface Vlan7
  mac-address 0060.3ecc.ab06
  ip address 10.50.7.254 255.255.255.0
!
interface Vlan8
  mac-address 0060.3ecc.ab07
  ip address 10.50.8.254 255.255.255.0
!
interface Vlan9
--More-- |
```

FIGURE 2.9 – Vérification des interfaces VLANs.

- **Configuration du DHCP**

Plutôt que de définir manuellement l'adresse IP pour chaque hôte connecté, le DHCP nous permet de les attribuer automatiquement à travers une configuration effectuée sur le switch core. Nous avons activé le DHCP pour tous les VLANs en utilisant la méthode illustrée ci-dessous.

```
>Scoeur(config)#ip dhcp pool vlan5
Scoeur(dhcp-config)#network 10.50.5.0 255.255.255.0
Scoeur(dhcp-config)#default-router 10.50.5.254
Scoeur(dhcp-config)#ex
Scoeur(config)#ip dhcp pool vlan6
Scoeur(dhcp-config)#network 10.50.6.0 255.255.255.0
Scoeur(dhcp-config)#default-router 10.50.6.254
Scoeur(dhcp-config)#ex
Scoeur(config)#ip dhcp pool vlan7
Scoeur(dhcp-config)#network 10.50.7.0 255.255.255.0
Scoeur(dhcp-config)#default-router 10.50.7.254
Scoeur(dhcp-config)#ex
Scoeur(config)#ip dhcp pool vlan8
Scoeur(dhcp-config)#network 10.50.8.0 255.255.255.0
Scoeur(dhcp-config)#default-router 10.50.8.254
Scoeur(dhcp-config)#ex
Scoeur(config)#ip dhcp pool vlan9
Scoeur(dhcp-config)#network 10.50.9.0 255.255.255.0
Scoeur(dhcp-config)#default-router 10.50.9.254
Scoeur(dhcp-config)#ex
Scoeur(config)#ip dhcp pool vlan10
Scoeur(dhcp-config)#network 10.50.10.0 255.255.255.0
Scoeur(dhcp-config)#default-router 10.50.10.254
Scoeur(dhcp-config)#ex
Scoeur(config)#ip dhcp pool vlan11
Scoeur(dhcp-config)#network 10.50.11.0 255.255.255.0
Scoeur(dhcp-config)#default-router 10.50.11.254
Scoeur(dhcp-config)#ex
Scoeur(dhcp-config)#ex
```

FIGURE 2.10 – Configuration du DHCP.

▷ Après avoir appliqué cette méthode pour chaque VLAN, nous avons vérifié leur activation en utilisant la commande "**Vérification du DHCP**".

```
ip dhcp pool vlan2
network 10.50.2.0 255.255.255.0
default-router 10.50.2.254
ip dhcp pool vlan3
network 10.50.3.0 255.255.255.0
default-router 10.50.3.254
ip dhcp pool vlan4
network 10.50.4.0 255.255.255.0
default-router 10.50.4.254
ip dhcp pool vlan5
network 10.50.5.0 255.255.255.0
default-router 10.50.5.254
ip dhcp pool vlan6
network 10.50.6.0 255.255.255.0
default-router 10.50.6.254
ip dhcp pool vlan7
network 10.50.7.0 255.255.255.0
default-router 10.50.7.254
ip dhcp pool vlan8
network 10.50.8.0 255.255.255.0
default-router 10.50.8.254
ip dhcp pool vlan9
network 10.50.9.0 255.255.255.0
default-router 10.50.9.254
ip dhcp pool vlan10
network 10.50.10.0 255.255.255.0
default-router 10.50.10.254
ip dhcp pool vlan11
network 10.50.11.0 255.255.255.0
--More-- |
```

FIGURE 2.11 – Vérification de l'activation du DHCP.

- Configuration des Trunk

En configurant les liens Trunk, il est possible de faire passer plusieurs flux de différents VLANs sur un seul lien physique. Dans ce cas, nous avons configuré tous les liens vers les switchs d'accès en mode Trunk à partir du switch Core, comme décrit ci-dessous.

```
Scorel#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Scorel(config)#int f0/1
Scorel(config-if)#switchport trunk encapsulation dot1q
Scorel(config-if)#ex
Scorel(config)#int f0/2
Scorel(config-if)#switchport trunk encapsulation dot1q
Scorel(config-if)#ex
Scorel(config)#int f0/3
Scorel(config-if)#switchport trunk encapsulation dot1q
Scorel(config-if)#ex
Scorel(config)#int f0/4
Scorel(config-if)#switchport trunk encapsulation dot1q
Scorel(config-if)#ex
Scorel(config)#int f0/5
Scorel(config-if)#switchport trunk encapsulation dot1q
Scorel(config-if)#ex
Scorel(config)#int f0/6
Scorel(config-if)#switchport trunk encapsulation dot1q
Scorel(config-if)#ex
```

FIGURE 2.12 – Configuration des trunk.

▷ Nous avons ensuite vérifié la configuration à l'aide de la commande "**show interface trunk**".

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

Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa0/2     1-1005
Fa0/3     1-1005
Fa0/4     1-1005
Fa0/5     1-1005
Fa0/6     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1,2,3,4,5,6
Fa0/2     1,2,3,4,5,6
Fa0/3     1,2,3,4,5,6
Fa0/4     1,2,3,4,5,6
Fa0/5     1,2,3,4,5,6
Fa0/6     1,2,3,4,5,6
--More--
```

FIGURE 2.13 – Verification des trunk.

- **Attribution des ports des commutateurs aux VLANs**

Cette opération consiste à associer un VLAN à chaque liaison physique connectée à un switch d'accès. Pour cela, nous avons configuré toutes les interfaces des switches d'accès, en suivant la méthode décrite dans la figure suivante, qui représente la configuration des interfaces du Switch 1

- **Configuration du protocole VTP**

La configuration du protocole VTP permet de distribuer tous les VLANs à partir des commutateurs configurés en mode serveur vers les commutateurs configurés en mode client appartenant au même domaine VTP. Dans notre cas, nous avons configuré le switch Core en mode serveur et les switches d'accès en mode client.

▷ **Configuration du switch core en mode server**

```
Swcoeur(config)#vtp mode server
Device mode already VTP SERVER.
Swcoeur(config)#vtp domain cevital.com
Changing VTP domain name from NULL to cevital.com
Swcoeur(config)#vtp password slimzatout
Setting device VLAN database password to slimzatout
Swcoeur(config)#ex
Swcoeur#
%SYS-5-CONFIG_I: Configured from console by console
```

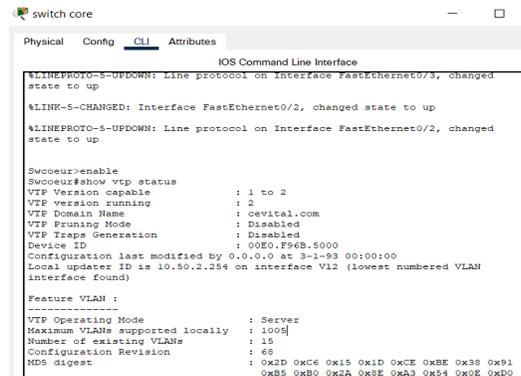
FIGURE 2.14 – Configuration en mode server.

▷ **Configuration des switches d'accès en mode client**

```
Swcoeur#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Swcoeur(config)#vtp mode client
Setting device to VTP CLIENT mode.
Swcoeur(config)#vtp domain cevital.com
Domain name already set to cevital.com.
Swcoeur(config)#vtp password slimzatout
Password already set to slimzatout
```

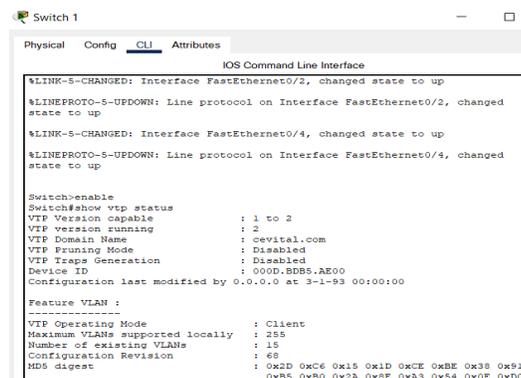
FIGURE 2.15 – Configuration en mode client.

▷ Pour vérifier que ces configurations ont bien été mises en place, nous avons utilisé la commande "show vtp status" dans le switch core ainsi que dans le switch 1.



```
switch core
Physical Config CLI Attributes
IOS Command Line Interface
%LINK-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINK-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed
state to up
Swcoeur#enable
Swcoeur#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                : 00E0.F96B.5000
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 10.50.2.254 on interface V12 (lowest numbered VLAN
interface found)
Feature VLAN :
-----
VTP Operating Mode      : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 15
Configuration Revision  : 68
MDS digest              : 0x2D 0xC6 0x15 0x1D 0xCE 0xBE 0x38 0x91
                       : 0xB5 0xB0 0x2A 0x8E 0xA3 0x54 0x0E 0xD0
```

FIGURE 2.16 – Verification des configurations VTP en mode server.



```
Switch 1
Physical Config CLI Attributes
IOS Command Line Interface
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINK-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed
state to up
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up
%LINK-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed
state to up
Switch#enable
Switch#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                : 000D.BDB5.AE00
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Feature VLAN :
-----
VTP Operating Mode      : Client
Maximum VLANs supported locally : 255
Number of existing VLANs : 15
Configuration Revision  : 68
MDS digest              : 0x2D 0xC6 0x15 0x1D 0xCE 0xBE 0x38 0x91
                       : 0xB5 0xB0 0x2A 0x8E 0xA3 0x54 0x0E 0xD0
```

FIGURE 2.17 – Verification des configurations VTP en mode client.

- **Vérification des adresses IP attribués par le DHCP** Cette figure montre l'adresse IP attribuée par le DHCP au PC 6. La vérification se fera pour tous les PC.

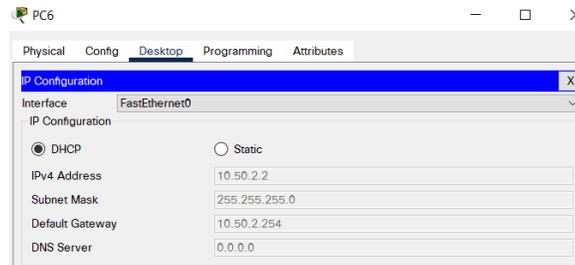


FIGURE 2.18 – Verification adresse Ip par DHCP

- **Vérification de la connectivité**

▷ **Test intra-VLANs**

Nous avons procédé à une vérification de la connectivité entre les ordinateurs appartenant aux mêmes VLANs en effectuant des Pings entre les adresses IP correspondantes. Un exemple de cette vérification est illustré dans la Figure ci-dessous, qui représente les résultats du Ping entre l'adresse IP du PC 2 (10.50.6.3) et celle du PC 10 (10.50.6.4).

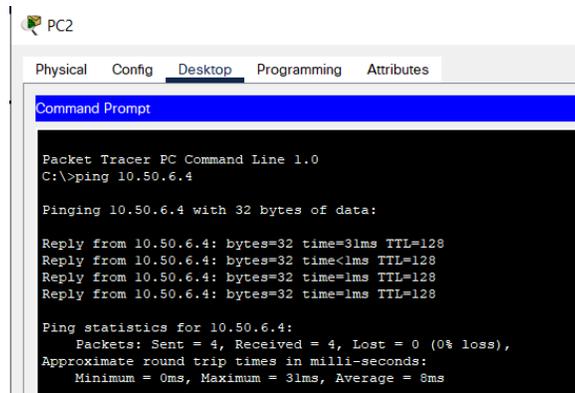
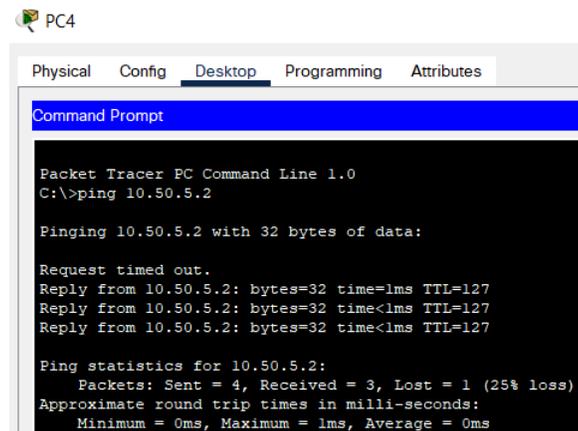


FIGURE 2.19 – Test intra VLAN

▷ **Test inter-VLANs**

Nous avons test la connectivité entre des PC appartenant à des VLANs distincts en effectuant un Ping entre leurs adresses IP. La figure ci-dessous illustre le résultat du Ping entre l'adresse IP du PC 4 (10.50.4.2) et celle du PC 0 (10.50.5.2).



```
PC4
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 10.50.5.2

Pinging 10.50.5.2 with 32 bytes of data:

Request timed out.
Reply from 10.50.5.2: bytes=32 time<1ms TTL=127
Reply from 10.50.5.2: bytes=32 time<1ms TTL=127
Reply from 10.50.5.2: bytes=32 time<1ms TTL=127

Ping statistics for 10.50.5.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

FIGURE 2.20 – Test inter VLAN

2.5 Partie 4 : problématique de CEVITAL et la solution qu'on propose

2.5.1 Critique du réseau existant

A partir de toutes les recherches qu'on a effectuées précédemment, nous avons remarqué plusieurs lacunes qui diminuent les performances du réseau existant.

Les lacunes les plus importante qu'on a remarqué sont :

- ✓ Absence de liaison avec les sites distants ce qui implique que chaque site a son propre data center, non seulement c'est couteux mais en plus le partage de ressources et de la communication sont inexistants.
- ✓ Il n'existe qu'un seul backbone qui se charge de centraliser le réseau. Ce qui entraine la surcharge de ce dernier.

2.5.2 Problématique :

Après avoir mené une étude, il est apparu que l'infrastructure du réseau d'une entreprise est l'un des piliers les plus importants pour assurer son bon fonctionnement. Cevital, étant l'une des plus grandes entreprises agro-alimentaires en Algérie, nécessite une gestion très rigoureuse afin de garantir la collecte, le stockage, le traitement et la communication des informations entre ses nombreux salariés dispersés sur plusieurs sites. Cette situation peut entraîner une surcharge du réseau, pouvant occasionner des ralentissements ou, dans les cas les plus graves, une panne du réseau.

2.5.3 Solution proposée :

Après avoir identifié les problèmes du réseau existant de Cevital, nous avons travaillé à trouver une solution appropriée. Nous avons conclu que la meilleure solution consiste à utiliser une architecture à deux switches de niveau 3, tout en assurant un équilibrage de charge entre les connexions pour permettre le partage des ressources et une communication fluide. Ensuite, nous ajouterions un protocole de haute disponibilité au niveau de la distribution. Dans ce cas, nous avons opté pour le HSRP.

2.6 Conclusion :

Ce chapitre nous a permis d'avoir une vue d'ensemble du réseau informatique de Cevital. Il a également mis en évidence des problèmes importants qui ont conduit à proposer une solution. Cette dernière repose principalement sur une nouvelle architecture réseau, avec l'utilisation de deux switches core de niveau 3, au lieu d'un seul, afin d'assurer un équilibrage de charge optimal.

Proposition et configuration d'une nouvelle architecture réseau

3.1 Introduction

La configuration actuelle repose sur un unique Switch Core, ce qui la rend très vulnérable aux pannes, cela peut entraîner un ralentissement ou même une interruption complète de l'activité, ce qui affecte la productivité de l'équipe et nuit au bon fonctionnement de l'entreprise. C'est la raison pour laquelle dans ce chapitre, nous proposerons une nouvelle configuration réseau pour Cevital, qui répondra à tous les problèmes du réseau actuel.

3.2 Architecture proposée

Nous avons réalisé une architecture sur Cisco packet tracer qui favorise l'équilibrage de charge dans notre réseau.

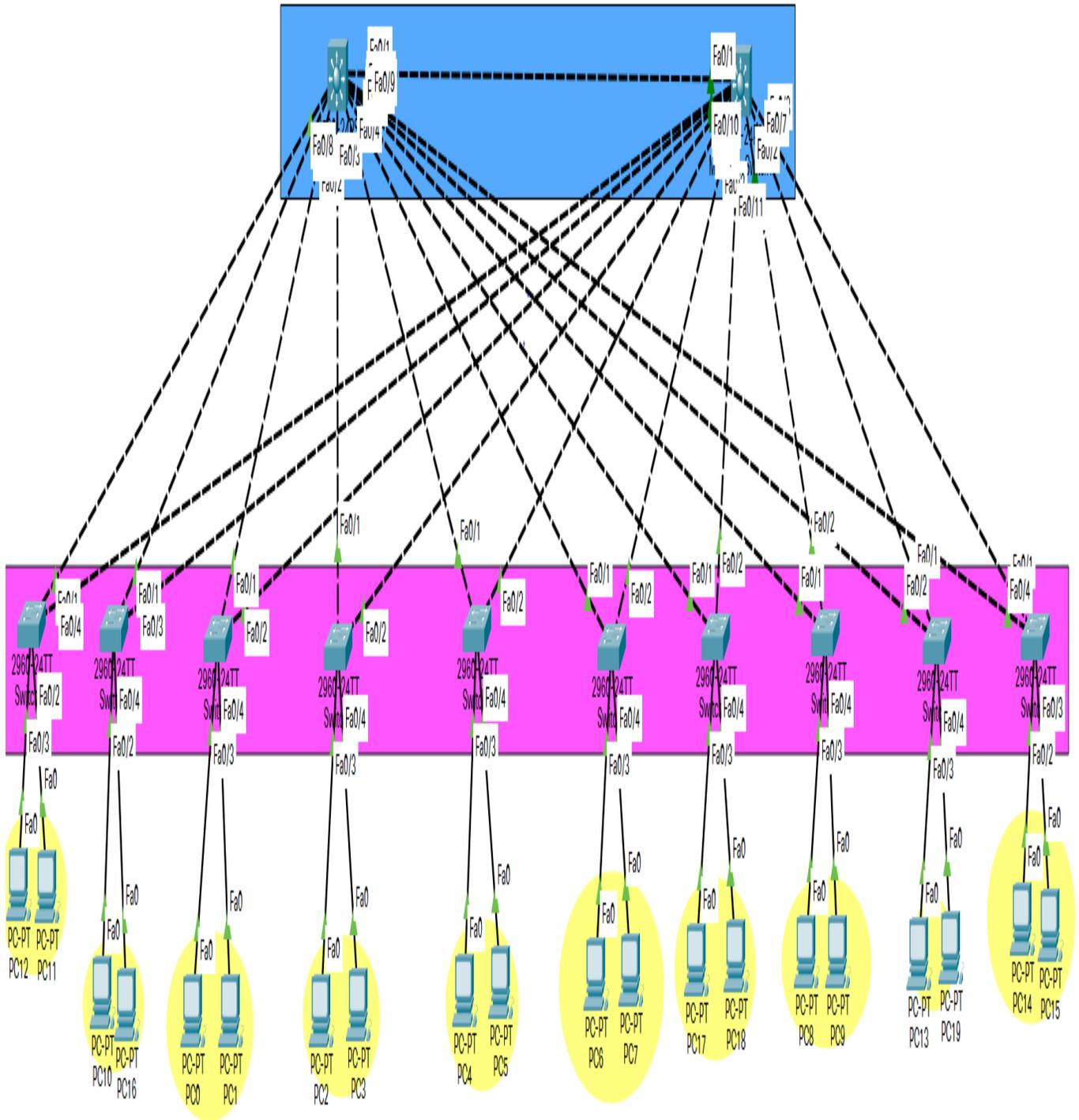


FIGURE 3.1 – Nouvelle architecture.

3.3 Configuration des équipements

Dans la nouvelle topologie présentée, nous avons utilisé 2 switches de niveau 3 interconnectés entre eux qui ont le rôle de switches Core. Nous avons rajouté cinq switches d'accès de niveau 2, ainsi que dix pcs .

3.3.1 Configuration des hostname et sécurité

Comme dans la première partie nous avons sécurisé les switches de niveau 3. cette figure représente la configuration du premier switch Core, que nous avons renommé Score1 et 2 successivement. Puis nous avons sécurisé le mode enable ; ensuite crée les sessions et on les

```
switch1#  
switch1#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
switch1(config)#hostname Score1  
Score1(config)#
```

FIGURE 3.2 – Configuration des hostname

a sécurisés (ligne console et ligne vty) en leurs attribuant des mots de passes sans oublier de chiffrer tous ces derniers. La figure ci-dessous montre ceci :

```
Score2#enable  
Score2#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Score2(config)#enable secret cisco1  
Score2(config)#line vty 0 4  
Score2(config-line)#password cisco1  
Score2(config-line)#login  
Score2(config-line)#exit  
Score2(config)#line vty 5 15  
Score2(config-line)#password cisco1  
Score2(config-line)#login  
Score2(config-line)#exit  
Score2(config)#line con 0  
Score2(config-line)#password cisco 1  
Score2(config-line)#login  
Score2(config-line)#exit  
Score2(config)#service password-encryption  
Score2(config)#
```

FIGURE 3.3 – Sécurité du mode enable et creation des session.

A l'aide de la commande «Show Run» nous pouvons voir que tous est bien sécurisé et chiffré ; cette figure illustre le résultat :

```
line con 0
  password 7 0822455D0A1654
  login
!
line aux 0
!
line vty 0 4
  password 7 0822455D0A1654
  login
line vty 5 15
  password 7 0822455D0A1654
  login
!
```

FIGURE 3.4 – Verification des sécurités.

✓ Sécurité des ports et Bpduguard

Pour sécuriser tous les ports reliés aux switches niveau 2, on a utilisé les commandes dont cette figure montre :

```
Switch>enable
Switch#
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switch
Switch(config-if)#switchport p
Switch(config-if)#switchport po
Switch(config-if)#switchport port-security max
Switch(config-if)#switchport port-security maximum 2
Switch(config-if)#switchport port-security viol
Switch(config-if)#switchport port-security violation r
Switch(config-if)#switchport port-security violation restrict
Switch(config-if)#switchport port-security mac
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#ex
Switch(config)#int f0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security maximum 2
Switch(config-if)#switchport port-security violation restrict
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#ex
```

FIGURE 3.5 – Sécurité des ports.

Le Bpduguard permet une sécurité de haut niveau c'est-à-dire si un autre utilisateur essaiera de se connecter à l'un des switches de l'entreprise il va être directement bloqué grâce à cette commande ; pour mieux comprendre nous avons cette figure qui explique ceci :

```
Enter configuration commands, one per line. End with CNTL/Z
Switch(config)#int range f0/3-24
Switch(config-if-range)#sp
Switch(config-if-range)#spa
Switch(config-if-range)#spanning-tree bpduguard ?
  disable  Disable BPDU guard for this interface
  enable   Enable BPDU guard for this interface
Switch(config-if-range)#spanning-tree bpduguard en
Switch(config-if-range)#spanning-tree bpduguard enable
Switch(config-if-range)#ex
Switch(config)#end
Switch#
```

FIGURE 3.6 – Le Bpduguard.

3.3.2 Création des VLANs

La création des VLANs se fait au niveau des switches Core (score1) et (score2), cette figure illustre la manière de configurer les vlans.

```
Score1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Score1(config)#vlan 2
Score1(config-vlan)#name DRH
Score1(config-vlan)#ex
Score1(config)#vlan 3
Score1(config-vlan)#name Finance
Score1(config-vlan)#ex
Score1(config)#vlan 4
Score1(config-vlan)#name gestion
Score1(config-vlan)#ex
Score1(config)#vlan 5
Score1(config-vlan)#name voix
Score1(config-vlan)#ex
```

FIGURE 3.7 – Création des VLANs dans le score1.

```
Score2(config)#vlan 2
Score2(config-vlan)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

Score2(config-vlan)#name telephonie
Score2(config-vlan)#ex
Score2(config)#vlan 3
Score2(config-vlan)#name administration
Score2(config-vlan)#ex
Score2(config)#vlan 4
Score2(config-vlan)#name management
Score2(config-vlan)#vlan 5
Score2(config-vlan)#name visio
Score2(config-vlan)#vlan 6
Score2(config-vlan)#name ingnierie
Score2(config-vlan)#ex
Score2(config)#
```

FIGURE 3.8 – Création dans VLANs dans le score2.

✓ Après avoir crée tous les VLANs, nous avons vérifié leur création avec la commande **show vlan brief**.

Voici le résultat qu'on a obtenue :

```
2    GRH                active
3    commercial         active
4    administratif      active
5    ingenierie         active
6    telephonie         active
7    reseau             active
8    visio-conference   active
9    finance            active
10   voix               active
11   management         active
1002 fddi-default       active
1003 token-ring-default active
1004 fddinet-default   active
1005 trnet-default     active
score2#
```

FIGURE 3.9 – Vérification des VLANs.

3.3.3 Configuration des interfaces VLANs

Comme dans la première partie, nous avons mis en place la configuration des interfaces des VLANs que nous avons créés auparavant. Cette étape permettra d'assurer le routage inter-VLAN. Nous avons attribuer l' IP (10.50.2.252) pour le score1 , et l'IP (10.50.2.253) pour le score 2 . Ensuite, nous avons activé ce routage en exécutant la commande "IP routing". Voici la figure qui montre les étapes à suivre pour crée le VLAN 2 dans les deux score 1 et 2

```

Score2(config)#int vlan 2
Score2(config-if)#ip add 10.50.2.253 255.255.255.0
Score2(config-if)#no shutdown
Score2(config-if)#ex
Score2(config)#
Score2(config)#
Score2(config)#ex
Score2#
%SYS-5-CONFIG_I: Configured from console by console

Score2#
Score2#wr
Building configuration...
[OK]
Score2#

```

FIGURE 3.10 – Configuration des interfaces VLANs dans le score1

```

Score1(config)#int vlan 2
Score1(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

Score1(config-if)#ip add 10.50.2.252 255.255.255.0
Score1(config-if)#no shutdown
Score1(config-if)#ex
Score1(config)#ex
Score1#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]

```

FIGURE 3.11 – Configuration des interfaces VLANs dans le score2

On fait la même chose pour le reste des VLAN :

```

Score1(config)#int vlan 3
Score1(config-if)#
%LINK-5-CHANGED: Interface Vlan3, changed state to up

Score1(config-if)#ip add 10.50.3.252 255.255.255.0
Score1(config-if)#ex
Score1(config)#int vlan 4
Score1(config-if)#
%LINK-5-CHANGED: Interface Vlan4, changed state to up

Score1(config-if)#ip add 10.50.4.252 255.255.255.0
Score1(config-if)#ex
Score1(config)#int vlan 5
Score1(config-if)#
%LINK-5-CHANGED: Interface Vlan5, changed state to up

Score1(config-if)#ip add 10.50.5.252 255.255.255.0
Score1(config-if)#ex
Score1(config)#
Score1(config)#
Score1(config)#int vlan 6
Score1(config-if)#
%LINK-5-CHANGED: Interface Vlan6, changed state to up

```

FIGURE 3.12 – Configuration des interfaces dans le reste des VLANs

✓ Vérification de la configuration des VLANs

Pour vérifier que les VLANs ont été configuré on utilise la commande `show vlan brief`.

```

interface Vlan2
  mac-address 0060.3ecc.ab01
  ip address 10.50.2.254 255.255.255.0
!
interface Vlan3
  mac-address 0060.3ecc.ab02
  ip address 10.50.3.254 255.255.255.0
!
interface Vlan4
  mac-address 0060.3ecc.ab03
  ip address 10.50.4.254 255.255.255.0
!
interface Vlan5
  mac-address 0060.3ecc.ab04
  ip address 10.50.5.254 255.255.255.0
!
interface Vlan6
  mac-address 0060.3ecc.ab05
  ip address 10.50.6.254 255.255.255.0
!
interface Vlan7
  mac-address 0060.3ecc.ab06
  ip address 10.50.7.254 255.255.255.0
!
interface Vlan8
  mac-address 0060.3ecc.ab07
  ip address 10.50.8.254 255.255.255.0
!
interface Vlan9
  --More-- |

```

FIGURE 3.13 – Verification de la configuration des VLANs

3.3.4 Configuration du DHCP

Nous avons établi un pool d'adresses pour chaque VLAN en effectuant cette opération au niveau des commutateurs centraux (Core switches). Ensuite, nous avons défini la passerelle par défaut pour chaque sous-réseau.

```

scoeur(config)#ip dhcp pool vlan5
Scoeur(dhcp-config)#network 10.50.5.0 255.255.255.0
Scoeur(dhcp-config)#default-router 10.50.5.254
Scoeur(dhcp-config)#ex
Scoeur(config)#ip dhcp pool vlan6
Scoeur(dhcp-config)#network 10.50.6.0 255.255.255.0
Scoeur(dhcp-config)#default-router 10.50.6.254
Scoeur(dhcp-config)#ex
Scoeur(config)#ip dhcp pool vlan7
Scoeur(dhcp-config)#network 10.50.7.0 255.255.255.0
Scoeur(dhcp-config)#default-router 10.50.7.254
Scoeur(dhcp-config)#ex
Scoeur(config)#ip dhcp pool vlan8
Scoeur(dhcp-config)#network 10.50.8.0 255.255.255.0
Scoeur(dhcp-config)#default-router 10.50.8.254
Scoeur(dhcp-config)#ex
Scoeur(config)#ip dhcp pool vlan9
Scoeur(dhcp-config)#network 10.50.9.0 255.255.255.0
Scoeur(dhcp-config)#default-router 10.50.9.254
Scoeur(dhcp-config)#ex
Scoeur(config)#ip dhcp pool vlan10
Scoeur(dhcp-config)#network 10.50.10.0 255.255.255.0
Scoeur(dhcp-config)#default-router 10.50.10.254
Scoeur(dhcp-config)#ex
Scoeur(config)#ip dhcp pool vlan11
Scoeur(dhcp-config)#network 10.50.11.0 255.255.255.0
Scoeur(dhcp-config)#default-router 10.50.11.254
Scoeur(dhcp-config)#ex
scoeur(config)#

```

FIGURE 3.14 – Configuration du DHCP

La commande «Show run» montre le résultat de la configuration précédente :

```
ip dhcp pool vlan2
network 10.50.2.0 255.255.255.0
default-router 10.50.2.254
ip dhcp pool vlan3
network 10.50.3.0 255.255.255.0
default-router 10.50.3.254
ip dhcp pool vlan4
network 10.50.4.0 255.255.255.0
default-router 10.50.4.254
ip dhcp pool vlan5
network 10.50.5.0 255.255.255.0
default-router 10.50.5.254
ip dhcp pool vlan6
network 10.50.6.0 255.255.255.0
default-router 10.50.6.254
!
!
```

FIGURE 3.15 – Verification de la configuration DHCP.

Nous avons exclu les adresses de 125 à 251 sur Score1, ce qui voudra dire que le Score1 va attribuer les adresses de 1 à 124. Les adresses de 1 à 124 sont quant à elles exclues sur Score2, ce qui voudra dire que le Score2 va attribuer les adresses de 125 à 251. Cette opération a pour but d'éviter les conflits au moment de l'attribution des adresses.

```
*****
Score1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Score1(config)#ip dhcp excluded-address 10.50.2.125 10.50.2.251
Score1(config)#ip dhcp excluded-address 10.50.3.125 10.50.3.251
Score1(config)#ip dhcp excluded-address 10.50.4.125 10.50.4.251
Score1(config)#ip dhcp excluded-address 10.50.5.125 10.50.5.251
Score1(config)#ip dhcp excluded-address 10.50.6.125 10.50.6.251
Score1(config)#
```

FIGURE 3.16 – Exclure les adresses du score1.

```

Score2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Score2(config)#ip dhcp excluded-address 10.50.2.1 10.50.2.124
Score2(config)#ip dhcp excluded-address 10.50.3.1 10.50.3.124
Score2(config)#ip dhcp excluded-address 10.50.4.1 10.50.4.124
Score2(config)#ip dhcp excluded-address 10.50.5.1 10.50.5.124
Score2(config)#ip dhcp excluded-address 10.50.6.1 10.50.6.124
Score2(config)#ex
Score2#
%SYS-5-CONFIG I: Configured from console by console

```

FIGURE 3.17 – Exclure les adresses du score2.

✓ Vérification que les adresses sont bien exclues dans les deux scores «**show run**»

```

.
ip dhcp excluded-address 10.50.2.125 10.50.2.251
ip dhcp excluded-address 10.50.3.125 10.50.3.251
ip dhcp excluded-address 10.50.4.125 10.50.4.251
ip dhcp excluded-address 10.50.5.125 10.50.5.251
ip dhcp excluded-address 10.50.6.125 10.50.6.251
!

```

FIGURE 3.18 – Verification des adresses exclues dans le score1 .

```

ip dhcp excluded-address 10.50.2.1 10.50.2.124
ip dhcp excluded-address 10.50.3.1 10.50.3.124
ip dhcp excluded-address 10.50.4.1 10.50.4.124
ip dhcp excluded-address 10.50.5.1 10.50.5.124
ip dhcp excluded-address 10.50.6.1 10.50.6.124
!
. . . . .

```

FIGURE 3.19 – Verification des adresses exclues dans le score2.

3.3.5 Configuration des liens Trunk

Nous avons configuré tous les liens vers les switches d'accès en mode Trunk à partir des switches Core ✓ Vérification que la configuration trunk a bien été établie

```
Score1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Score1(config)#int f0/1
Score1(config-if)#switchport trunk encapsulation dot1q
Score1(config-if)#ex
Score1(config)#int f0/2
Score1(config-if)#switchport trunk encapsulation dot1q
Score1(config-if)#ex
Score1(config)#int f0/3
Score1(config-if)#switchport trunk encapsulation dot1q
Score1(config-if)#ex
Score1(config)#int f0/4
Score1(config-if)#switchport trunk encapsulation dot1q
Score1(config-if)#ex
Score1(config)#int f0/5
Score1(config-if)#switchport trunk encapsulation dot1q
Score1(config-if)#ex
Score1(config)#int f0/6
Score1(config-if)#switchport trunk encapsulation dot1q
Score1(config-if)#ex
```

FIGURE 3.20 – Configuration des switches en mode trunk

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

Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa0/2     1-1005
Fa0/3     1-1005
Fa0/4     1-1005
Fa0/5     1-1005
Fa0/6     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1,2,3,4,5,6
Fa0/2     1,2,3,4,5,6
Fa0/3     1,2,3,4,5,6
Fa0/4     1,2,3,4,5,6
Fa0/5     1,2,3,4,5,6
--More--
```

FIGURE 3.21 – Vérification de la configuration trunk dans le score1.

```

Score2#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     on        802.1q         trunking    1
Fa0/2     on        802.1q         trunking    1
Fa0/3     on        802.1q         trunking    1
Fa0/4     on        802.1q         trunking    1
Fa0/5     on        802.1q         trunking    1
Fa0/6     on        802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa0/2     1-1005
Fa0/3     1-1005
Fa0/4     1-1005
Fa0/5     1-1005
Fa0/6     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1,2,3,4,5,6
Fa0/2     1,2,3,4,5,6
Fa0/3     1,2,3,4,5,6
Fa0/4     1,2,3,4,5,6
Fa0/5     1,2,3,4,5,6
Fa0/6     1,2,3,4,5,6
V....

```

FIGURE 3.22 – Vérification de la configuration trunk dans le score2.

3.3.6 Activation du VTP

Nous avons activé le VTP en mode server dans le score 1

```

Score1>
Score1#enable
Score1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Score1(config)#vtp mode server
Device mode already VTP SERVER.
Score1(config)#vtp domain cev.com
Changing VTP domain name from NULL to cev.com
Score1(config)#vtp password cisco
Setting device VLAN database password to cisco
Score1(config)#

```

FIGURE 3.23 – Activation VTP dans le score1.

✓ Vérification que le mode server a bien été activé, en utilisant la commande `show vtp status`

3.3.7 Configuration STP

◇ Dans ces figures nous vous montrons les commandes nécessaires pour la configuration du STP dans le score 1 et dans le score 2, nous avons donner la priorité 4096 du vlan 2 au vlan 6 et la priorité 8196 pour les vlan de 7 jusqu'au 11.

```

Score1>enable
Score1#show vtp status
VTP Version capable      : 1 to 2
VTP version running     : 2
VTP Domain Name         : cev.com
VTP Pruning Mode        : Disabled
VTP Traps Generation     : Disabled
Device ID                : 0001.4349.2E00
Configuration last modified by 0.0.0.0 at 3-1-93 00:03:21
Local updater ID is 10.50.2.252 on interface V12 (lowest numbered VLAN
interface found)

Feature VLAN :
-----
VTP Operating Mode      : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 10
Configuration Revision  : 31
MDS digest              : 0x73 0xC2 0x84 0xE8 0x48 0x7F 0xF7 0x2F
                        : 0x3C 0xCF 0xAF 0x79 0x05 0xE9 0x65 0x3B

```

FIGURE 3.24 – Verification du VTP

```

Score1(config)#spanning-tree mode p
Score1(config)#spanning-tree mode pvst
Score1(config)#sp
Score1(config)#spanning-tree v
Score1(config)#spanning-tree vlan 2-6 p
Score1(config)#spanning-tree vlan 2-6 priority 4096
Score1(config)#spanning-tree vlan 7-11 priority 8192
Score1(config)#ex
Score1#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]

```

FIGURE 3.25 – Configuration STP dans le score1

```

Score2(config)#spanning-tree mode pvst
Score2(config)#s
Score2(config)#sp
Score2(config)#spanning-tree v
Score2(config)#spanning-tree vlan 7-11 p
Score2(config)#spanning-tree vlan 7-11 priority 4096
Score2(config)#spanning-tree vlan 2-6 priority 8192
Score2(config)#

```

FIGURE 3.26 – Configuration STP dans le score2.

3.3.8 Configuration du HSRP

Nous avons configuré l'HSRP sur Score1 en mode « actif » pour les VLANs 2-6, et en mode « Standby » pour les VLANs 7-11.

Nous avons configuré l'HSRP sur Score2 en mode « actif » pour les VLANs 7-11, et en mode « Standby » pour les VLANs 2-6.

```

Score1(config)#int vlan 2
Score1(config-if)#standby 2 ip 10.50.2.254
Score1(config-if)#standby 2 priority 110
Score1(config-if)#standby
%HSRP-6-STATECHANGE: Vlan2 Grp 2 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan2 Grp 2 state Standby -> Active

% Incomplete command.
Score1(config-if)#standby 2 preempt
Score1(config-if)#ex
Score1(config)#int vlan 3
Score1(config-if)#standby 2 ip 10.50.3.254
Score1(config-if)#standby 3 priority 110
Score1(config-if)#standby 3 preempt
Score1(config-if)#ex
Score1(config)#int vlan 4
Score1(config-if)#standby 2 ip 10.50.3.254
%HSRP-6-STATECHANGE: Vlan3 Grp 2 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan3 Grp 2 int vlan 3
Score1(config-if)#int vlan 4

```

FIGURE 3.27 – Configuration HSRP dans le score1

```

Score1(config)#int vlan 7
Score1(config-if)#standby 7 ip 10.50.7.254
Score1(config-if)#ex
Score1(config)#int vlan 8
Score1(config-if)#standby 8 ip 10.50.7.254
% Address 10.50.7.254 in group 7
Score1(config-if)#standby 8 ip 10.50.8.254
Score1(config-if)#ex
Score1(config)#int vlan 9
Score1(config-if)#standby 9 ip 10.50.9.254
Score1(config-if)#ex
Score1(config)#int vlan 9
%HSRP-6-STATECHANGE: Vlan7 Grp 7 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan7 Grp 7 state Standby -> Active

```

FIGURE 3.28 – Configuration HSRP dans le score2.

3.4 Vérification de la communication

Nous avons testé la connectivité entre des PC appartenant à des VLANs distincts en effectuant un Ping entre leurs adresses IP. La figure ci-dessous illustre le résultat du Ping entre l'adresse IP du PC 5(10.50.6.2) et celle du PC 12 (10.50.7.252).

Lorsque on désactive l'un des ports du switch 5, on remarque que l'envoi de paquets s'arrêtent immédiatement, après quelques secondes l'envoi reprend place. La figure ci-dessous montre ce dernier.

```
Packet Tracer PC Command Line 1.0
C:\>ping -t 10.50.6.2

Pinging 10.50.6.2 with 32 bytes of data:

Request timed out.
Reply from 10.50.6.2: bytes=32 time=28ms TTL=127
Reply from 10.50.6.2: bytes=32 time<1ms TTL=127
Reply from 10.50.6.2: bytes=32 time=1ms TTL=127
Reply from 10.50.6.2: bytes=32 time=15ms TTL=127
Reply from 10.50.6.2: bytes=32 time=13ms TTL=127
Reply from 10.50.6.2: bytes=32 time=11ms TTL=127
```

FIGURE 3.29 – Ping entre PC5 et PC12.

```
Reply from 10.50.6.2: bytes=32 time=43ms TTL=127
Request timed out.
Reply from 10.50.6.2: bytes=32 time=20ms TTL=127
Reply from 10.50.6.2: bytes=32 time=43ms TTL=127
```

FIGURE 3.30 – Désactivation d'un port et ping.

3.5 Conclusion

Le chapitre précédent celui-ci a révélé que la fonctionnalité du réseau est limitée car l'architecture contient un seul switch core de niveau 3 ce qui est insuffisant ; par conséquent peut présenter des défaillances. C'est pourquoi, nous avons proposé et configuré un nouveau réseau visant à améliorer le réseau existant en utilisant des protocoles tels que le STP, HSRP

Conclusion et perspectives

Notre objectif était de proposer une architecture plus avancée et de mettre en place des solutions fiables pour garantir un fonctionnement optimal et un partage efficace des ressources. Ce projet nous a permis de mettre en pratique les connaissances acquises lors de notre stage pratique au sein de l'entreprise Cevital de Béjaïa.

Pour mener à bien notre projet et atteindre les objectifs fixés, nous avons opté pour l'utilisation du simulateur Packet Tracer pour plusieurs raisons avantageuses. Ce logiciel nous a permis de modéliser avec précision l'architecture du système à mettre en place en identifiant les différents composants et en rendant la configuration plus simple et claire.

En travaillant sur ce projet, nous avons acquis les connaissances nécessaires pour concevoir un réseau d'entreprise efficace et évolutif. Nous avons approfondi notre compréhension des fonctionnalités des commutateurs de niveau 2 et multi-niveaux tels que les VLANs, les trunks, le routage inter-VLAN, l'agrégation des ports, le STP, ainsi que des protocoles tels que HSRP. Les résultats obtenus et présentés dans ce mémoire, avec la configuration détaillée du nouveau réseau proposé, démontrent que cette solution répond de manière appropriée à la problématique identifiée.

Bibliographie

- [1] Christian Draux , « Les réseaux »,2006.
- [2] Bertrand PETIT ; architectures des réseaux ,2006.
- [3] GUY Pujolle. Cours réseaux et télécoms. Edition Eyrolles, 2004
- [4] FOROUZAN B., « Local Area Network, Mc GRAW Hill » éditions, 2009
- [5] COUR CISCO CCNA1,chapitre 3 MédiAs réseau. netacad, 2016.
- [6] [https ://www.futura-sciences.com/tech/definitions/informatique-fibre-optique-18133](https://www.futura-sciences.com/tech/definitions/informatique-fibre-optique-18133)
- [7] Gerardo Rubino, Laurent Toutain, Réseaux locaux sans fil, Edition 8mai 1998.
- [8] [https ://www.techno-science.net/definition/1363.html](https://www.techno-science.net/definition/1363.html).
- [9] Dean .T (2001). Réseaux Informatique. Edition RYNALD GOULET.
- [10] [https ://cisco.goffinet.org/ccna/vlans/concepts-vlan-cisco/](https://cisco.goffinet.org/ccna/vlans/concepts-vlan-cisco/)
- [11] Chabane.T ; mémoire, installation et configuration d'un réseau informatique, Bejaia, session 2006.
- [12] [https ://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-5.html](https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-5.html).
- [13] B. Kercheval. « DHCP : Aguide to dynamic TCO/IP Network configuration ». Edition 1999.
- [14] [https ://cisco.goffinet.org/ccna/redondance-de-liens/cisco-etherchannel-configuration-verification-depannage/](https://cisco.goffinet.org/ccna/redondance-de-liens/cisco-etherchannel-configuration-verification-depannage/)
- [15] William.R. S, Guide de l'administrateur Windows server 2012, Edition Dunod, 2007.
- [16] LI, T., COLE, B., MORTON, P., et al.RFC2281 : Cisco Hot standby Routeur Protocol (HSRP).
- [17] Richard TRABELSI Froom, Balaji Sivasubramanian, and Erum Frahim. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide : Foundation Learning for SWITCH 642-813. Cisco Press, 2010.
- [18] Source interne de CEVITAL.
- [19] [https ://www.cisco.com](https://www.cisco.com)
- [20] Document Cevital.

[21] <https://math.univ-lyon1.fr>.

[22] <https://www.samomoi.com/reseauxinformatiques>

RÉSUMÉ

Ce mémoire représente notre stage de fin d'étude dans l'entreprise agroalimentaire cevital .Tout d'abord nous avons commencé par décrire les généralisées sur les réseaux , puis nous avons présenté l'entreprise en citant ses point fort et ses lacunes ensuite nous avons proposé la solution adéquate pour résoudre les problèmes que rencontre cette établissement, enfin nous avons mis en pratique toute nos connaissance durant notre cursus universitaire a fin de crée une nouvelle architecture plus développer ou nous avons utiliser deux switch core afin de permettre l'équilibrage de charge au sein de notre réseau local .

ABSTRACT

This dissertation represents our end-of-study internship in the agri-food company cevital. First of all, we started by describing the generalized ones on the networks. Then, we presented the company by citing its strong points and its shortcomings then we proposed the appropriate solution to solve the problems encountered by this establishment. Finally, we put into practice all our knowledge during our university course in order to create a new more developed architecture where we used two switch cores in order to allow load balancing within our local network.