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

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

ATE Department

Département d'Automatique, Télécommunication et d'Electronique

Projet de Fin d'Etudes

Pour l'obtention du diplôme de Master

Filière : Télécommunications.

Spécialité :Réseaux et Télécommunications.

Thème

Mise en place d'une infrastructure d'équilibrage de charge pour garantir la performance, la disponibilité et la continuité des services applicatifs sur les serveurs de l'entreprise. Cas pratique Cevital

Préparé par :

Herbi Massinissa

Meridja Khaled

Dirigé par :

Mme GHERBI Meriem

M. SLIMANI Mennad

Examiné par :

Mme MAMMErI Karima

M. Diboune A.Hani

Année universitaire : **2024/2025**

Remerciements

Avant tout, je tiens à remercier mon Dieu tout-puissant de nous avoir donné la force et le courage

Nous souhaitons adresser nos remerciements les plus sincères à notre encadrante, Meriem Gherbi, pour sa disponibilité, sa patience et son précieux suivi tout au long de la réalisation de ce travail

Nous tenons à exprimer notre profonde reconnaissance au groupe CEVITAL, en particulier à M. Slimani, pour l'accueil chaleureux qui nous a été réservé ainsi que pour le soutien constant dont nous avons bénéficié tout au long de notre stage

Nous adressons nos remerciements les plus sincères aux membres du jury pour avoir accepté de faire partie de la commission d'évaluation et pour le temps qu'ils nous ont consacré

Enfin, Je tien à remercier également ma famille et mes amis pour leurs aides considérables.

Dedicace

Avant de commencer je remercie dieu qui m'a aidée et m'a donné de la force d'arriver à ce point là et de terminer ce modiste travail.

Premièrement, je dédie ce travail à ma chère famille, mes parents qui m'ont accompagné dans tous mon cursus scolaire et universitaire, pour leurs encouragements et sacrifices, je le dédie aussi à mon frère mon cher jumeau Missipssa et ma petite belle sœur Léticia.

Je dédie ce travail à mon cher ami et camarade,frère Adel et à toute l'équipe de G204 (Fares, Yanis, Zaki, ...).

Je le dédie aussi à ma chère amie Amel pour toute les moments inoubliables sans oublier les amis .

Je le dédie à mon cher binôme pour sa patience.

Massinissa

Je dédie ce travail

A mes chers parents et ma grand-mère, pour leur amour, leurs prières et leur soutien inestimable.

A mon frère Lounis et ma sœur Sabrina, pour leur présence précieuse.

A tous mes amis, pour les moments partagés et leur encouragement.

À mon cher binôme pour sa patience.

Khaled

Table des matières

Table des figures

Liste des tableaux

Liste des acronymes

ARP	*Address Resolution Protocol*
AVG	*Active Virtual Gateway*
AVF	*Active Virtual Forwarders*
BPDU	*Bridge Protocol Data Unit*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
FAI	*Fournisseur d'Accès à Internet*
FTP	*File Transfer Protocol*
GLBP	*Gateway Load Balancing Protocol*
GZIP	*GNU zip*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
HSRP	*Hot Standby Routing Protocol*
ICMP	*Internet Control Message Protocol*
IP	*Internet Protocol*
IPv4	*Internet Protocol version 4*
LAN	*Local Area Network*
MAC	*Media Access Control*
MAN	*Metropolitan Area Network*
OSI	*Open Systems Interconnection*
SMTP	*Simple Mail Transfer Protocol*
SSH	*Secure Socket Shell*
STP	*Spanning Tree Protocol*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
VLAN	*Virtual Local Area Network*
VTP	*VLAN Trunking Protocol*
VRRP	*Virtual Router Redundancy Protocol*
WAN	*Wide Area Network*

Introduction Générale

L'équilibrage de charge est un défi important pour la gestion des réseaux dans les entre- prises, surtout aujourd'hui ou les données et le nombre d'utilisateurs augmentent constamment. Pour faire face à ces défis, il est essentiel que les entreprises améliorent leurs infrastructures afin de garantir une performance stable et fiable

Notre projet de fin d'étude s'articule autour de la mise en place d'une infrastructure d'équilibrage de charge pour garantir la performance, la disponibilité et la continuité des ser- vices applicatifs sur les serveurs de l'entreprise. Cette étude résout la problématique majeur des réseaux des entreprises qui est l'équilibrage de charge ce qui garant la continuité des services d'une entreprise donc la continuité de la majorité des tâches essentielles dans l'entreprise.

Notre mémiore est composé de quatre chapiters :

- Le premier chapitre présent les généralités sur les réseaux informatiques, nous allons étu- dier les différentes classifications des réseaux et les protocoles utilisés par les réseaux et quelques équipements essentiels

- Le deuxième chapitre est consacré pour l'étude de l'existant, c'est une présentation de l'entreprise de Cevital et les modèles des équipements qui utilise au sein d'entreprise, puis enfin nous allons proposer une problématique et quelques propositions et solutions.

- Le troisième chapiter est l'equilibrage de charge dans un réseau , nous présentons une définition de Load Balancing et les objectifs de ce dernier, son fonctionnement (Ses com- posants et la processus), puis nous exposons les différents types d'équilibrage de charge, ensuit nous terminons avec quelque algorithmes et protocoles d'équilibrage de charge

- Dans le dernier chapitre Conception et réalisation, c'est la partie pratique dans laquelle nous simulons une architecture réseau de Cevital sur le logiciel Cisco Packet Tracer, Dans cette architecture, nous allons appliquer des configurations (VLANs, VIP) et des proto- coles nécessaires pour résoudre le problem d'un équilibrage de charge (SSH, STP HSRP, Line console, bpdu guard et port fast), Nous clôturons avec des tests de validation de la configuration globale utilisée dans le souci de verifier les objectifs ont été atteints

Enfin, nous terminerons avec une conclusion générale et quelques perspectives .

Chapitre I

Généralités sur les réseaux informatiques

I.1 Introduction

Dans ce chapitre nous allons présenter les réseaux informatiques, leurs types, topologies, architectures et équipements. Ensuite, nous introduirons les protocoles utilises, les modèles de réseaux existents. Enfin, nous parlons sur les VLANs et quelques notions sur l'adressage IP.

I.2 Définition d'un réseau informatique

Un réseau informatique est un ensemble d'appareils interconnecté (des ordinateurs, des ser- veurs, des routeurs, des commutateurs, des imprimantes et des périphériques), qui sont conçus pour partager des ressources, communiquer entre eux et échanger des données, ils peuvent être reliés par des câbles physiques ou des connexions sans fil.

Actuellement , les réseaux informatiques font partie intégrante des entreprises et autres entités et ont totalement changé notre manière de travailler et de communiquer, devenant ainsi indispensables à notre quotidien.[1]

I.3 Classification des réseaux informatiques

Les réseaux informatiques dont classés selon plusieurs critères :

I.3.1 Classification selon leur étendue géographique (leur taille)

On peut distingues différents types de réseaux selon leurs étendue géographique, on peut classer en 3 types de réseaux :

I.3.1.1 Réseau local (LAN : Local Area Network)

Un réseau LAN est un réseau informatique déployé sur une zone géographique limité, on l'utilise généralement dans les entreprises et les établissements car il permet d'interconnecté l'ensemble des équipements de l'organisation.[2]

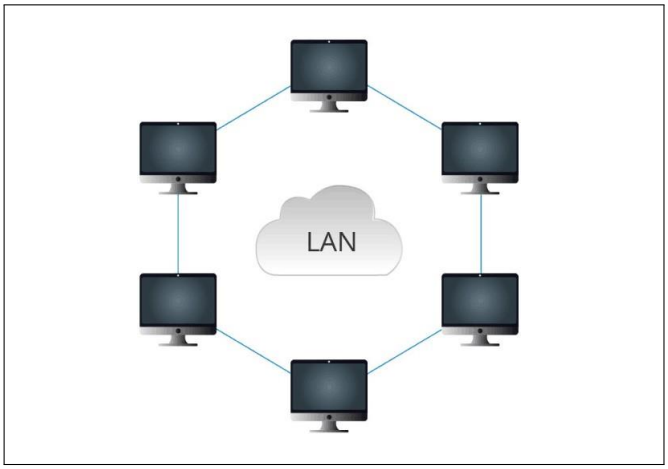


FIGURE I.1 – Un réseau local (LAN) [F1]

I.3.1.2 Réseau métropolitain (MAN : Metropolitan Aria Network)

Un réseau MAN est un réseau informatique haut débit conçu pour interconnecter plusieurs réseaux locaux. Généralement, il est établi par la fibre optique pour augmenter la vitesse du transfert des données [3]

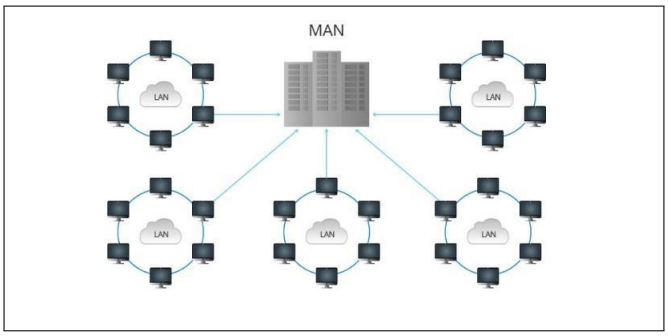


FIGURE I.2 – Un réseau métropolitain (MAN) [F2]

I.3.1.3 Réseau étendu (WAN : Wide Area Network)

Un réseau WAN est un réseau informatique déployé pour les grandes zones géographiques, on l'utilise pour inclure des zones nationales et mondiales pour permettre une communication entre les différentes empalements sur cette zone.[2]

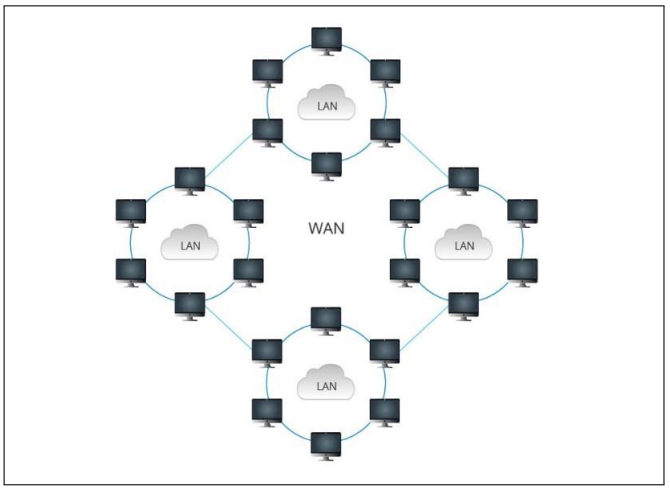


FIGURE I.3 – Un réseau étendu (WAN) [F3]

I.3.2 Classification selon leur architecture des réseaux

On peut distinguer 2 types d'architectures :

I.3.2.1 Réseau Poste à Poste (Peer to Peer)

Pour ce modèle Poste à Poste, les machines opèrent en égaux c'est-à-dire toute machine peut se comporter comme un serveur par rapport aux autre machines ou comme une station des travail [4]

Avantages :

- Un coût réduit.
- Une simplicité à toute épreuve

Inconvénients

- Ce système n'est pas du tout centralisé, ce qui le rend très difficile à administrer.
- La sécurité est très peu présente

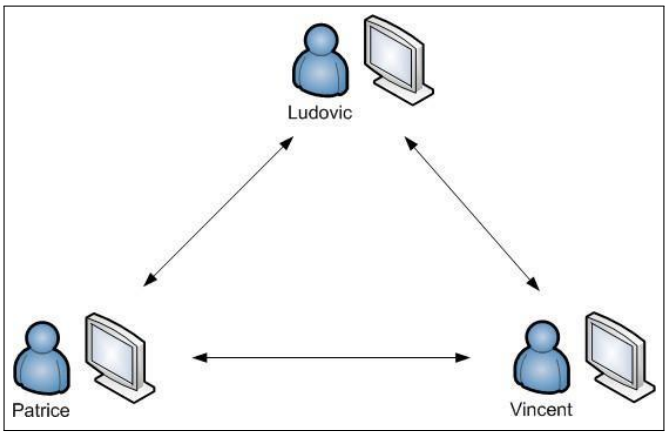


FIGURE I.4 – Architecture poste à poste [F4]

I.3.2.2 Réseau Client /Serveur

Pour le modèle Client / Serveur, les machines du réseau sont répartis en deux catégories ; la première catégorie contient des serveurs qui ont pour unique fonction de rendre des services aux autres ordinateurs du réseau, la deuxième catégorie ce sont des clients ou stations de travail qui pour une tâche donnée émettent des requêtes de services vers un serveur, qui répond à leurs requêtes [4]

Avantages :

- Administrer au niveau serveur (moins besoin d'être administrés).
- Une meilleure sécurité.

Inconvénients :

- Un coût élevé dû à la technicité du serveur et à sa mise place.
- Pas d'interconnexion des machines au cas des pannes

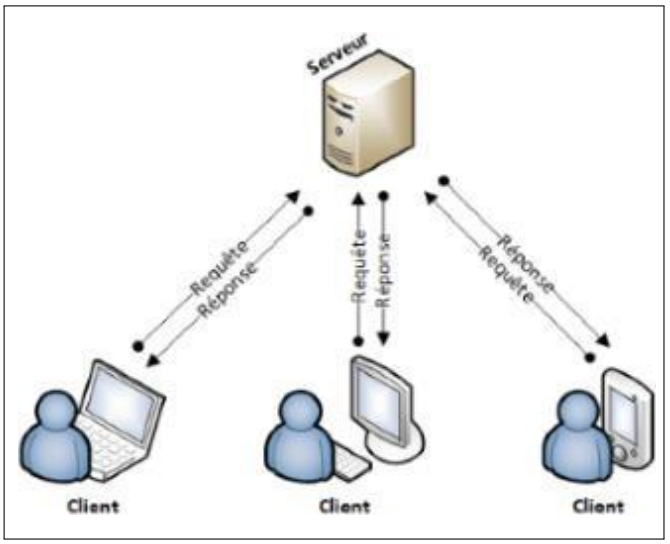


FIGURE I.5 – Architecture client/serveur [F5]

I.3.3 Classification selon leur topologie

On peut distingue 3 types de topologies :

I.3.3.1 Topologie en Bus

C'est la topologie la plus simple d'un réseau, car toutes les machine sont relieés à une même ligne de transmission (Bus) par l'intermédiaire de câble, on utilise un câble coaxial généralement, la connexion post-câble constitue un nœud et un message est émis à partir de n'importe quel poste et dans les deux sens. [4]

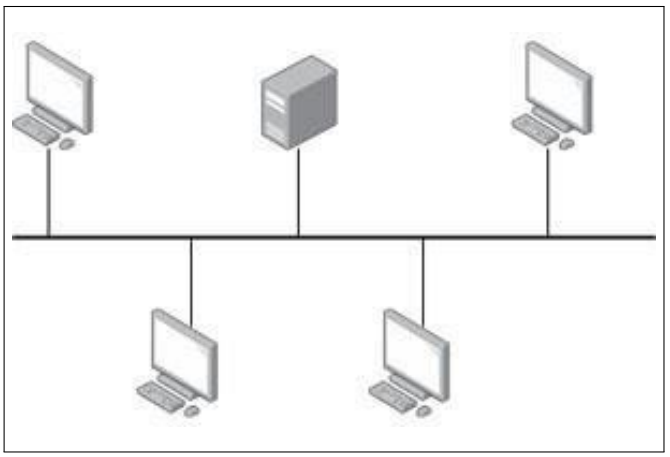


FIGURE I.6 – Topologie Bus [F6]

I.3.3.2 Topologie en Anneau

Cette topologie équivaut fonctionnellement à un Bus dont le câble se referme sur lui même, les machines du réseau communiquent chacun à leur tour, on aura donc une boucle de machines sur laquelle chacun va avoir la parole successivement. Cette topologie a des inconvénients ; si le câble présente un défaut, le réseau ne fonctionne plus. Elle est moins utilisée car elle est très couteuse.[4]

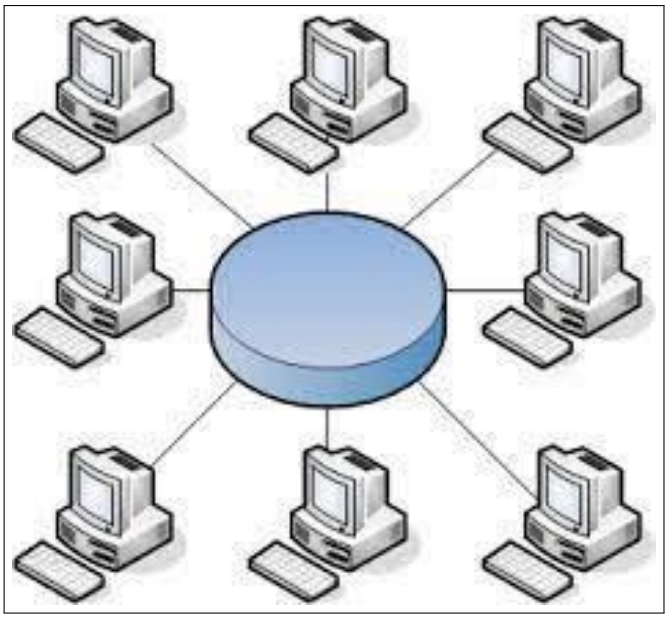


FIGURE I.7 – Topologie Anneau [F7]

I.3.3.3 Topologie en Étoile

Pour cette topologie, toutes les machines sont reliées par des câbles différents à des nœuds centraux appelé « Hub » (en français Concentrateur). Le Hub contient un certain nombre de

ports sur lesquels sont branchées les machines du réseau. Il propage les signaux émis par chaque machine atteignent tous les autres machines.

Cette architecture présente une meilleure tolérance aux panne , car une coupure dans un câble n'affecte que la machine directement connectée.[4]

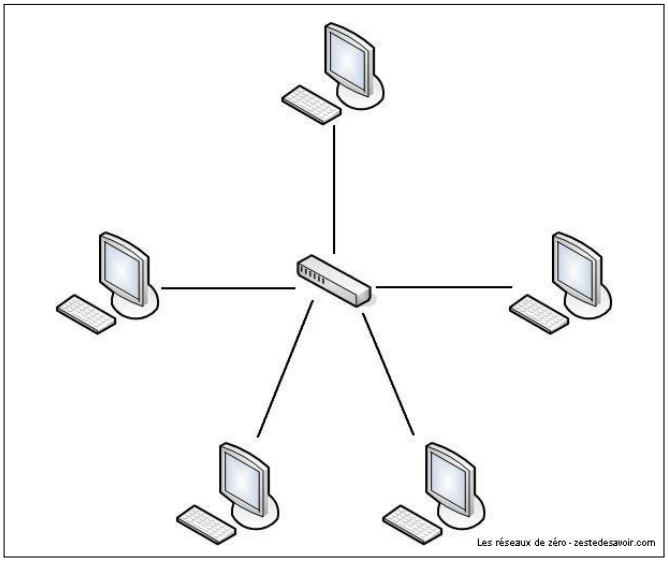


FIGURE I.8 – Topologie Étoile [F8]

I.4 Les équipements d'interconnexion

Pour établir un réseau, il est nécessaire d'utiliser plusieurs équipements, en grande partie dédiés à l'interconnexion, chacun ayant un rôle bien défini.

I.4.1 Carte réseau

La carte réseau joue un rôle essentiel dans la communication entre un ordinateur et un réseau. Elle sert d'interface physique permettant l'échange de données via un support de trans- mission. Ainsi, pour qu'un ordinateur puisse se connecter à un réseau, il est indispensable qu'il en soit équipé.

I.4.2 Routeur

Le routeur est un dispositif clé dans un réseau informatique. Il sert à interconnecter plusieurs réseaux ou sous-réseaux et à réguler le flux des données qui circulent entre eux. Son rôle principal est d'assurer le routage des paquets afin d'optimiser la transmission des informations. Il opère au niveau de la couche réseau (couche 3) du modèle OSI.

I.4.3 Modem

Un modem est un appareil qui permet à votre ordinateur ou autre appareil de se connecter à Internet. Il agit comme un traducteur, convertissant les signaux numériques de votre appareil en signaux analogiques qui peuvent être transmis via des lignes téléphoniques ou des câbles, et vice versa, Le mot "modem" est un mot-valise formé à partir de "modulateur" et "démodulateur". Il fait référence à sa fonction principale [5]

I.4.4 Concentrateur

Un concentrateur est un dispositif matériel équipé de plusieurs ports, conçu pour intercon- necter plusieurs ordinateurs. Il agit également comme un répéteur de signal en recevant des données sur l'un de ses ports, puis en les diffusant à l'ensemble des autres ports.

I.4.5 Commutateur

Le commutateur, ou switch, est un élément essentiel des réseaux fonctionnant au niveau 2 du modèle OSI, il assure la connexion entre plusieurs dispositifs informatiques de manière efficace. Contrairement au hub, il est capable d'identifier l'adresse physique des équipements qui lui sont reliés et d'analyser les trames reçues afin de les acheminer directement vers la bonne destination.

I.5 Modèles de communication

Aujourd'hui, dans le monde réseau, il existe deux modèles largement dominants :le modèle OSI qui définit 7 couches et le modèle TCP/IP (modèle Internet) qui définit 4 couches

D'une façon générale, on peut dire que le modèle OSI est un modèle de réseau idéalisé (modèle conceptuel), tandis que le modèle TCP/IP est une implémentation pratique

I.5.1 Le modèle OSI

Le modèle OSI (Open Systems Interconnection) est un modèle théorique dont le but est de fixer les normes de communication entre les différents systèmes informatiques. Il est normalisé en 1984

Ce modèle offre un système de communication composé de 7 couches différentes. Le concepte derrière cette représentation est de décomposer la communication entre deux périphériques en différentes « étapes » bien définies afin qu'on puisse par la suite faire évoluer les composants de chacune des couches de manière indépendante plutôt que de devoir modifier l'intégralité du processus de communication dès le changement d'un composant.

Le modèle OSI ne donne qu'une définition générale de chaque couche sans spécifier les services ni les protocoles utilisés par chacune d'entre elles. C'est aux rédacteurs des protocoles de les créer de façon à ce qu'ils respectent les règles et normes d'une couche en détails. [6]

Les 7 couches définies par le modèle OSI sont les suivantes :

N° de la couche	Nom de la couche	Unité de données
7	Application	segments non transformées
6	Présentation	segments non transformées
5	Session	segments non transformées
4	Transport	Segments
3	Réseau	Paquets
2	Liaison des données	Frames
1	Physique	Bits

TABLE I.1 – Les couches du modèle OSI

I.5.1.1 Couche Application

C'est la couche la plus proche de l'utilisateur. La majorité des protocoles utilisés par les utilisateurs se situent dans cette couche (HTTP, SMTP, FTP,etc).

Cette couche interagit avec les applications logicielles qui implémentent des composants de communication. La couche application est le point d'accès aux services réseaux et aussi pour le fonction d'identification des interlocuteurs, de déterminer si les ressources sont disponibles et synchroniser les communications. La couche application en elle-même n'a aucun moyen de déterminer la disponibilité des ressources sur le réseau.[6]

I.5.1.2 Couche Présentation

Cette couche est chargée du formatage des données de la couche applicative afin qu'elles puissent être lues à nouveau par les applications. [6]

I.5.1.3 Couche Session

La couche session contrôle les connexions entre les machines. Cette couche permet l'ouver- ture et la fermeture de session et gère la synchronisation des échanges ainsi que les transactions. [6]

I.5.1.4 Couche Transpor

La couche transport fournit les moyens concrets pour transférer de taille variable d'une source vers une destination en conservant la qualité du service.

L'enjeu de cette couche est de réceptionner les données qui viennent des couches supérieures, de les découper et de la faire transiter jusqu'à la couche réseau

Cette couche est la première à communiquer directement avec la machine de destination : elle gère les communications de bout en bout entre processus. [6]

I.5.1.5 Couche Réseau

La couche réseau fournit les moyens concret pour transférer des données de taille variable (appelés « paquets ») entre différents réseaux .

Cette couche effectue nottament le routage et l'adressage des paquets dans cette couche, elle définit la route que vont emprunter les paquets pour aller d'un point de départ (source) à un point d'arrivée (destination). [6]

I.5.1.6 Couche Liaison des données

Cette couche gère les communications entre deux machines directement connectées entre elles. Donc les données brutes va découper en trames de tailles variables puis les envoyer de manière séquentielle.

Puis on va détecter et pouvoir corriger les erreurs pouvant survenir dans la couche physique, définir le protocole pour établir et mettre fin à une connexion entre deux périphériques connectés physiquement et définir le protocole de contrôle de flux (régulation du trafic) entre eux. [6]

I.5.1.7 Couche Physique

La couche physique est chargée de la transmission des signaux entre les machines. Son service est limité à l'émission et la réception d'un bit ou train de bits continu.

La couche physique est, comme son nom l'indique, la couche dans laquelle sont définis les protocoles du monde physique (les différents câbles de transmission). [6]

I.5.2 Modèle TCP/IP

Le modèle TCP/IP appelé modèle Internet, qui est normalisé en 1976, a été fixé bien avant l'annonciation du modèle OSI en 1984.

Ce modèle est une approche réaliste ou pratique d'un modèle réseau là ou le modèle OSI est un modèle idéalisé ou théorique. En conséquence, c'est le modèle TCP/IP qui est utilisé comme modèle de réseau de référence pour Internet

Le nom de modèle TCP/IP vient de ses deux protocoles « essentiels » : les protocoles TCP (Transmission Control Protocol) et IP (Internet Protocol). [6]

Il présente aussi une approche modulaire en quatre couches :

N° de la couche	Nom de la couche	Unité de données
4	Application	Données non transformées
3	Transport	Segments
2	Internet	Paquets
1	Accès réseau	Frames/Bits

TABLE I.2 – Les couches du modèle TCP/IP

I.5.2.1 Couche Application

Le modèle TCP/IP regroupe les trois couches de session, présentation et application du modèle OSI dans une seule couche application. En effet, d'un point de vue pratique, cela ne fait souvent pas beaucoup de sens de séparer ces couches

Cette couche contient tous les protocoles de haut niveau : FTP pour le transfert de fichiers, SMTP pour les mails, HTTP pour le WWW, DNS pour les noms de domaine.[6]

I.5.2.2 Couche Transport

Cette couche assure la communication logique entre processus. Cette couche détermine comment les données doivent être envoyées : de manière fiable ou pas.

Concrètement, on peut choisir entre deux protocoles dans la couche transport : TCP (Trans- mission Control Protocol) et UDP (User Datagram Protocol).

TCP est un protocole de transfert fiable orienté connexion. Ce protocole contrôle et s'assure qu'il n'y ait ni perte ni corruption de données. Il est donc en charge des erreurs. TCP est le protocole le plus utilisé sur le Web aujourd'hui.

UDP est un protocole de transfert non fiable et qui ne nécessite ps de connexion préalable. Ce protocole est particulièrement utilisé pour les échanges ou la perte de quelques données n'est pas grave (appel vidéo, jeu en ligne, etc), car il est plus rapide que TCP. [6]

I.5.2.3 Couche Internet

Le but principal de la couche Internet est d'assurer la communication logique entre hôte, c'est-à-dire de transmettre coûte que coûte les paquets d'un hôte à un autre et de faire en sorte qu'ils arrivent à destination. Le protocole principal de cette couche est le IP (Internet Protocol). Les paquets peuvent prendre différentes routes pour arriver à destination et arriver dans un ordre différent de l'ordre dans lequel ils ont été envoyés.

Cette couche n'assure pas la fiabilité de transmission pendant son fonctionnement mais fournit qu'un service peu fiable et une livraison optimale (via le routage et l'adressage). Étant

donné que la livraison de paquets entre divers réseaux est une opération intrinsèquement peu fiable et sujette aux pannes, la charge de la fiabilité a été placée avec les points d'extrémité d'un chemin de communication, c'est-à-dire les hôtes, plutôt que sur le réseau.

Ce sera aux protocoles de plus haut niveau d'assurer la fiabilité du service.[6]

I.5.2.4 Couche Accès réseau

La couche accès réseau du modèle TCP/IP regroupe les couches physique et liaison des données du modèle OSI. Cette couche définit comment envoyer des paquets IP à travers le réseau (via des protocoles comme Ethernet ou Wireless entre autres).[6]

I.5.3 Comparaison entre le modèle OSI et le modèle TCP/IP

N° de la couche	OSI	TCP/IP	Unité de données
7	Application	Application	Données non transformées
6	Présentation		
5	Session		
4	Transport	Transport	Segments
3	Réseau	Internet	Paquets
2	Liaison des données	Accès réseau	Frames
1	Physique		Bits

TABLE I.3 – Comparaison entre le modèle OSI et modèle TCP/IP

I.6 Les protocoles réseaux

Un protocole réseau est essentiel pour permettre aux appareils de communiquer et de par- tager des informations dans un réseau. il établit des règles et des normes qui assurent une interaction fluide et efficace entre les équipements connectés [7]

I.6.1 Le protocole IP (Internet Protocole)

Le protocole IP est un ensemble de règles qui régissent le routage et l'adressage des paquets de données, permettant ainsi leur transmission à travers les réseaux jusqu'à leur destination finale. Lorsqu'une information circule sur Internet, elle est fragmentée en unités plus petites appelées paquets. Chaque paquet contient des informations spécifiques à IP, qui facilitent son acheminement vers le bon destinataire. [8]

Le protocole IP ne garantit pas la livraison des paquets, car il ne possède pas de mécanismes internes de vérification ou de correction des erreurs. Ainsi, certains paquets peuvent être perdus, retardés ou arriver dans un ordre différent de celui d'origine, nécessitant l'intervention d'autres protocoles pour assurer une transmission fiable. [9]

I.6.2 Le protocole TCP (Transmission Control Protocol)

TCP est un protocole de communication de niveau supérieur basé sur IP. Il assure un transfert de données fiable et ordonné entre deux systèmes. Contrairement aux protocoles non

connectés, TCP établit d'abord une connexion avant d'envoyer des données sous forme de segments. Chaque segment est identifié par un numéro de séquence et contient des informations permettant de vérifier l'intégrité des données transmises. Grâce à ces mécanismes, TCP garantit que les paquets arrivent dans le bon ordre et sans erreur [10]

I.6.3 Le protocole UDP (User Datagram Protocol)

UDP est un protocole de communication sans connexion utilisé pour transmettre des paquets de données sur les réseaux, Il est souvent privilégié pour les applications nécessitant une faible latence et une tolérance à la perte de données, comme la diffusion en continu, les jeux en ligne et la téléphonie sur IP. Contrairement à TCP, UDP ne garantit ni la livraison des données ni leur ordre d'arrivée, ce qui en fait un protocole dit "non fiable". Cependant, cette absence de mécanismes de contrôle le rend plus rapide et plus léger. En effet, les datagrammes UDP sont généralement plus courts que les paquets TCP, ce qui accélère leur transmission. [11]

I.6.4 Le protocole DHCP (Dynamic Host Configuration Protocol

DHCP est un protocole réseau qui attribue automatiquement des adresses IP aux appareils connectés. Il évite la configuration manuelle et facilite la gestion du réseau. Un serveur DHCP fournit aussi des informations comme la passerelle et le masque de sous-réseau et le DNS

I.6.5 Le protocol DNS (Domain Name System)

DNS est un service qui convertit les noms de domaine en adresses IP, facilitant l'accès aux sites web. Il joue un rôle essentiel dans la navigation sur Internet en rendant les adresses plus compréhensibles pour les utilisateurs.

I.6.6 Le protocole ARP (Address Resolution Protocol)

ARP est un protocole de la couche réseau utilisé pour résoudre les adresse MAC (Media Access Control) en adresse IP sur un réseau local. Lorsqu'un ordinateur souhaite communiquer avec un autre appareil du même réseau, il doit connaître son adresse MAC. Pour cela, il envoie une requête ARP en diffusant un message à tous les appareils du réseau, demandant à qui appartient l'adresse IP recherchée. L'appareil correspondant répond en fournissant son adresse MAC, et l'ordinateur émetteur enregistre cette information dans sa table ARP. [12]

I.6.7 Le protocole ICMP (Internet Control Message Protocol)

ICMP (Internet Control Message Protocol) appartient à la couche réseau et joue un rôle clé dans le diagnostic des problèmes de communication sur un réseau. Il est principalement utilisé pour vérifier si les données parviennent bien à destination dans un délai acceptable. Ce protocole est couramment mis en œuvre sur des équipements réseau comme les routeurs. Son importance réside notamment dans la signalisation des erreurs et l'exécution de tests de connectivité.[13]

I.6.8 Le protocole VTP (VLAN Trunking Protocol)

VTP est un protocole propriétaire de Cisco qui facilite la gestion centralisée des VLANs au sein d'un même domaine. Il assure une cohérence des informations en permettant la création, la suppression et la modification des VLANs sur un commutateur principal, puis en diffusant

automatiquement ces changements aux autres commutateurs du domaine VTP. Cela garantit une configuration uniforme et simplifie l'administration du réseau. [14]

I.7 Un réseau local virtuel (VLAN)

I.7.1 Définition

Un VLAN (Virtual Local Area Network) est un réseau logique opérant à la couche liaison de données du modèle OSI. Il permet de segmenter un réseau local physique afin d'isoler certains appareils. Ainsi, même si ces équipements sont connectés à différents commutateurs, ils peuvent être regroupés dans un même VLAN et échanger des données comme s'ils faisaient partie du même réseau physique.[15]

I.7.2 Agrégation de VLAN

L'agrégation de VLAN est une technique essentielle dans les réseaux informatiques. Elle permet d'établir une liaison point à point entre deux périphériques réseau afin de transporter plusieurs VLANs sur un même lien physique. Contrairement à un VLAN classique, une agréga- tion de VLAN ne se limite pas à un seul VLAN spécifique, mais agit plutôt comme un conduit permettant le transport simultané de plusieurs VLANs entre les commutateurs et les routeurs. Cette approche facilite la gestion du réseau en réduisant le nombre de connexions physiques nécessaires et en améliorant l'efficacité de la communication entre les équipement. [16]

I.7.3 Les avantages des VLANs

- Ils améliorent la sécurité en isolant les groupes d'utilisateurs et en limitant les accès non autorisés.
- Les VLANs permettent de créer des sous-réseaux virtuels indépendants au sein d'un même réseau physique.
- Ils réduisent la latence en évitant que tout le trafic ne passe par un même réseau encombré.
- Ils permettent de diminuer les coûts en partageant des ressources physiques entre plusieurs réseaux logiques.

I.8 Adressage IP

I.8.1 Définition

L'adressage est l'ensemble des moyens qui permettent d'identifier un élément sur le réseau. Un adressage peut être physique (par exemple un réseau téléphonique fixe) ou logique (la téléphonie mobile).

Dans un réseau, chaque station doit avoir une identification claire grâce à son adresse unique qui est l'adresse MAC au niveau physique de tous les éléments actifs, tel que les imprimantes, les serveurs et les stations. De plus, l'attribution d'une adresse IP logique est la première étape et l'essentielle pour établir une connexion efficace. [17]

I.8.2 Adresse IPv4

L'adresse IPv4 est composée de 04 Octets (32 Bits) séparés par des points et convertis en décimale pour une meilleure lisibilité.[17]

L'adresse IPv4 est constitué de deux parties :

- **Réseau :** C'est la partie qui doit être identique dans toutes les adresses IP des PCs se trouvant dans le même réseau.
- **Machine :** C'est la partie qui permet d'identifier le PC (différente pour chaque machine).

I.8.3 Masque de réseau

Le masque réseau est un code de 32 bits qui permet de « masquer » une partie de l'adresse IP pour faire la différence entre l'ID de réseau de l'ID de l'hôte. [17]

I.8.4 Masque de sous-réseau

Le masque de sous-réseau permet de placer des hôtes dans des sous-réseaux ou ils pourront communiquer, formant des regroupements de machines au sein du même masque réseau. Em- prunter des bits au champ d'hôte et les désigner comme champ de sous-réseau. Le nombre de bits à sélectionner dépend du nombre maximal d'hôtes requis par sous-réseau, le découpage en sous-réseaux est utile dans le cas des réseaux de grande taille

Dans la conception d'un réseau, il est essentiel de définir le nombre de sous-réseau requis et le nombre d'hôte requis par sous réseau. [17]

L'emprunt de N bits donne :

- Nbr sous-réseaux utilisables = (2^ nombre de bits empruntés).
- Nbr hôtes utilisables = (2^ nombre de bits hôtes restants) - 2.

I.8.5 Classes d'adressage

Il existe plusieurs classes d'adressage (classe A,B,C,D,E) mais dans la plupart de nos études on parle juste sur les 3 première classes :

- **Class A :** réservée aux réseaux de grand taille (0.0.0.0 à 127.255.255.255 avec : 127.0.0.0 à 127.255.255.255 sont réservées).
- **Class B :** réservées aux réseaux de taille moyenne ou grande (128.0.0.0 à 191.255.255.255).
- **Class C :** réservées aux réseaux de petites taille (192.0.0.0 à 223.255.255.255).

Adresses réservées

- Adresse technique : réseau 127.0.0.0, adresse de bouclage 127.0.0.1.
- Adresse du réseau – première adresse IP du réseau (ID hôte : tout les bits à 0).
- Adresse de diffusion (broadcast) – dernière adresse IP du réseau (ID hôte : tout les bits à 1).
- Adresse des classes D et E.

Adresse IP Privée

Adresse IP pouvant être utilisés hors Internet par les particuliers dans une entreprise, éta- blissement administrative ou dans une maison. [17]

- **Classe A** (Une plage) :
  - 10.0.0.0 à 10.255.255.255
- **Classe B** (16 plages) :
  - 172.16.0.0 à 172.16.255.255
  - 172.31.0.0 à 172.31.255.255

- **Classe C** (256 plages) :
  — 192.168.0.0 à 192.168.0.255
  — 192.168.255.0 à 192.168.255.255

Adresse IP Publique

C'est une adresse IP qui est unique dans le monde entier, pouvant être routés sur le réseau Internet, ce sont des adresses obtenues auprès d'un fournisseur d'accès Internet (FAI), à l'exception des adresses privées tous le reste des adresses des classes A,B,C sont des adresses publiques. [17]

I.9 Coclusion

Ce chapitre nous aidera à bien comprendre les bases du réseau informatique, notamment les différents équipements d'interconnexion, les protocoles réseau et les différentes classfication, ce qui nous facilitera l'approfondissement dans les chapitres à venir, Dans le chapitre suivant, nous allons présenter l'organisme d'accueil (groupe Cevital) ainsi que sa localisation géographique. Nous verrons également quels sont les matériels qu'il utilise dans son architecture.

Chapitre II

Étude de l’existant

II.1 Introduction

Dans le cadre du notre projet, ce chapitre se concentre sur l'étude de l'existant au sein de l'entreprise Cevital. Nous allons parler sur tous ce qui concerne cette entreprise commençant par une petite présentation sur Cevital son historique et aussi explorer leur organigramme, leurs valeurs, son architecture . à la fin nous allons poser une problématique sur laquelle repose notre projet, nous proposons certains solutions qui vont être détaillées dans les chapitres suivants.

II.2 Présentation de l'entreprise et son histoire

FIGURE II.1 – Logo Cevital [F9]

Cevital est une entreprise algérienne privée, fondée en 1998 par l'homme d'affaires Issad Rebrab à Béjaïa. À l'origine, le groupe s'est concentré sur le secteur agroalimentaire, mettant en place une raffinerie de sucre, une unité de fabrication d'huile, ainsi qu'un site pour le condi- tionnement de divers produits alimentaires.

Porté par une volonté claire de croissance, Cevital s'est rapidement imposé comme le plus important groupe privé du pays. Son activité ne s'est pas limitée à l'agroalimentaire : il s'est ouvert à des domaines aussi variés que l'industrie, la distribution, la construction, l'électromé- nager, la fabrication de verre, la logistique ou encore l'électronique

En 2007, le groupe a franchi une nouvelle étape avec la création de Mediterranean Float Glass, spécialisée dans le verre plat. Il a également commencé à se développer à l'internatio- nal : en 2013, il fait l'acquisition de l'entreprise française OXXO, spécialisée dans la menuiserie industrielle, et l'année suivante, il rachète la marque française d'électroménager Brandt ,une avancée majeure dans sa stratégie d'expansion à l'étranger.

Aujourd'hui, Cevital représente un pilier majeur de l'économie algérienne, employant des milliers de personnes et développant des projets d'envergure dans divers domaines. .[18]

II.3 Situation géographique de Cevital

Cevital Agro-Industrie, considéré comme le plus grand complexe privé en Algérie, est im- planté à Béjaïa, à proximité du port et de la route nationale 26, à environ 280 kilomètres d'Alger. Cette position stratégique lui permet de bénéficier d'un accès direct à des infrastruc- tures essentielles telles que l'aéroport, le port ainsi que la zone industrielle d'Akbou. L'entreprise dispose également de son propre quai privé, un atout majeur pour ses activités logistiques.

En plus de ses installations à Béjaïa, le groupe est présent dans plusieurs autres villes algériennes à travers ses bureaux régionaux. À l'échelle internationale, Cevital a élargi son champ d'action en développant des filiales et des installations dans différents pays, où elle se consacre principalement à la commercialisation et à la distribution de ses produits.

FIGURE II.2 – Vue satellitaire du complexe Cevital

II.4 Organisme du Cevital

L'entreprise CEVITAL est constituée de différentes directions. On cite :

- **La direction des finances et comptabilité :** le rôle de cette direction est de préparer et mettre à jour les budgets, de tenir la comptabilité et préparer les états comptables et financiers et de pratiquer le contrôle de gestion. [19]
- **La direction commerciale :** elle a en charge de commercialiser toutes les gammes des produits, le développement du fichier client de l'entreprise et de la gestion de la relation client. [19]
- **La direction des ressources humaines :** Cette direction a pour rôle principal de fournir un soutien administratif à l'ensemble du personnel de CEVITAL. Elle est également responsable de la gestion des activités sociales et de l'accompagnement de la direction générale ainsi que des managers dans la gestion des ressources humaines sous tous ses aspects. [19]
- **La direction industrielle :** elle est responsable du développement et de l'évolution des sites de production. En collaboration avec la direction générale, elle définit les objectifs ainsi que le budget pour chaque site. Elle procède à l'analyse des dysfonctionnements ren- contrés sur les sites, qu'ils concernent les équipements, l'organisation ou d'autres aspects, et met en place des solutions techniques ou humaines visant à améliorer continuellement la productivité, la qualité des produits et les conditions de travail. Elle anticipe également les besoins en matériel et veille à la gestion des achats necessaries. [19]
- **La direction des systèmes d'information :** elle est responsable de la mise en place des outils et des technologies de l'information essentiels pour soutenir et améliorer l'acti- vité, la stratégie et la performance de l'entreprise. Elle veille à la cohérence des moyens informatiques et de communication mis à disposition des utilisateurs, à leur mise à niveau, à leur maîtrise technique, ainsi qu'à leur disponibilité et leur opérationnalité continues, tout en garantissant leur sécurité. [19]

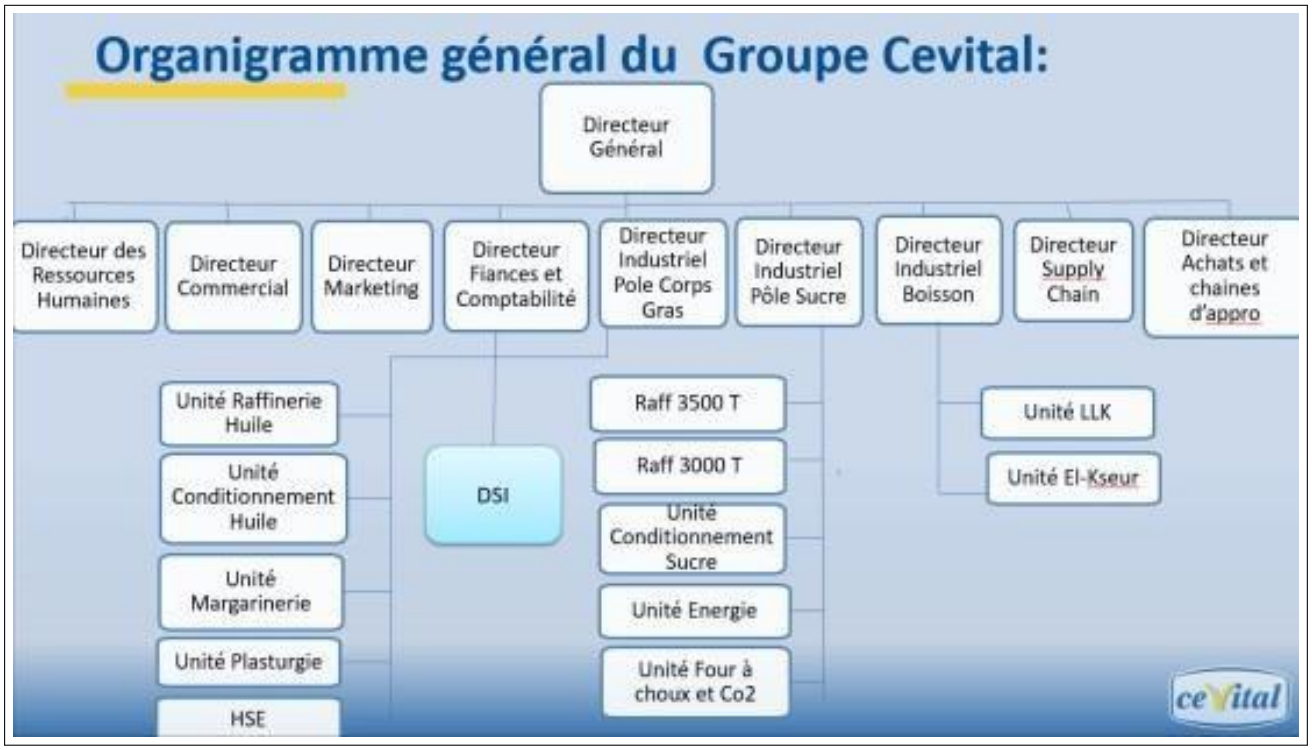


FIGURE II.3 – Organigramme général du groupe Cevital

II.5 Organigramme de la direction du système d'informa- tion

- **Directeur du système d'information :** Il est responsable de résoudre les problèmes avec un minimum de coût et dans les délais les plus courts, tout en adoptant des solutions informatiques qui renforcent la productivité et la performance de l'entrepris.
- **Administrateur réseau :** Chargé de l'administration du réseau afin d'assurer une circulation fluide et efficace de l'information au sein de l'entreprise, ce professionnel s'as- sure du bon fonctionnement, de la fiabilité et des performances des équipements et de l'infrastructure réseau, tout en restant attentif aux demandes des utilisateurs.
- **Administrateur système :** Il est responsable de la conception et de l'installation de l'infrastructure informatique et réseau d'une entreprise. Il veille à son bon fonctionnement, tout en assurant la gestion et la maintenance des systèmes qui y sont intégrés.
- **Responsable support :** Il est chargé de fournir une assistance aux utilisateurs en les accompagnant dans l'utilisation de leur matériel. Il intervient également à distance pour diagnostiquer et résoudre les problèmes techniques, tout en assurant un support téléphonique au sein de l'organisation.

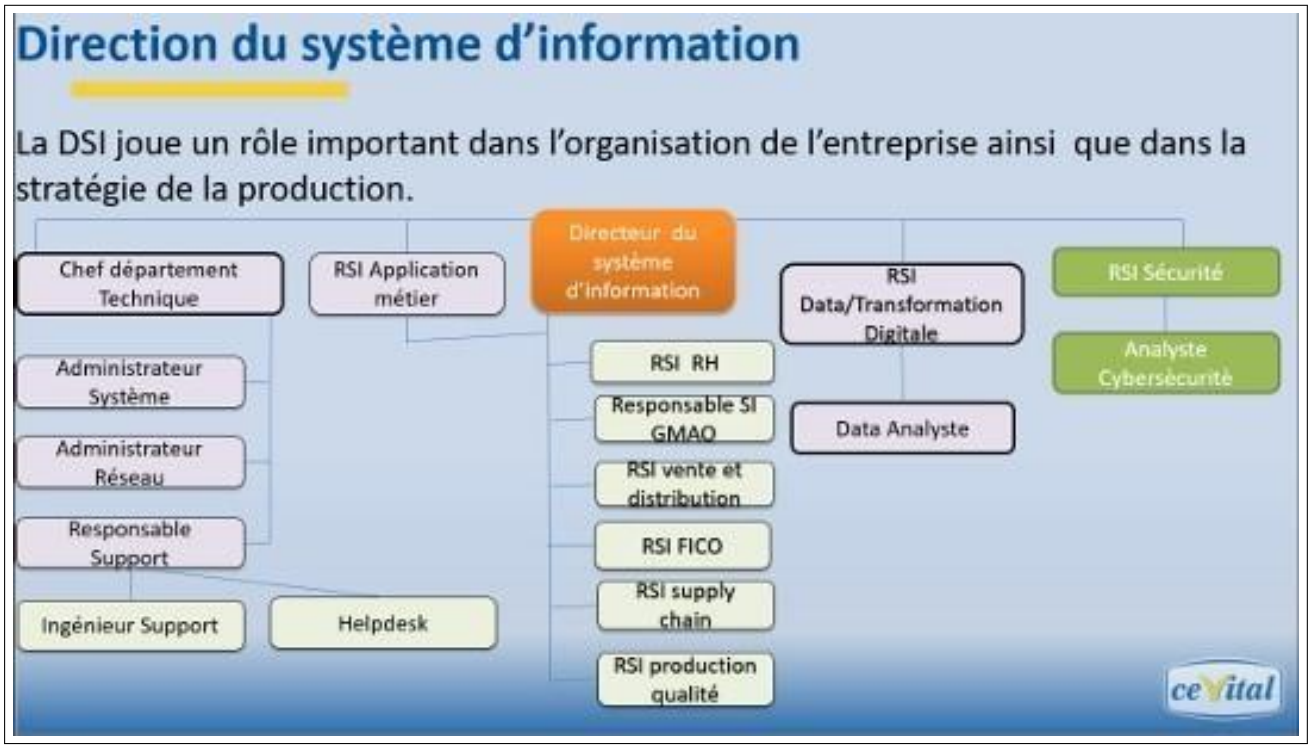


FIGURE II.4 – Direction du système d'information

II.6 Valeurs du Groupe CEVITAL

Il y a quatre règles d'or à respecter (IRIS) :

> **Initiative :** Le collaborateur anticipe les éventuels problèmes et suggère des solutions créatives en mettant à profit son expertise dans le domaine.

> **Respect :** Un principe fondamental prévaut entre les collaborateurs, ainsi qu'avec les partenaires internes et externes.

> **Intégrité :** Une valeur essentielle consiste à ce que les collaborateurs adoptent, à travers leurs actions, une éthique professionnelle irréprochable.

> **Solidarité :** Les collaborateurs doivent se soutenir mutuellement en partageant leurs expériences et leurs connaissances.

II.7 Infrastructure de l'entreprise

CEVITAL Agro-industrie possède plusieurs unités de production , réparties comme suit :

- Une raffinerie d'huile.
- Une margarinerie.
- Une conserverie.
- Deux raffineries de sucre
- Une unité de fabrication et de conditionnement de boissons rafraîchissantes (site El Kseur).
- Des silos portuaires.
- Une unité de conditionnement d'eau minérale (située à Tizi-Ouzou).
- Une unité de sucre liquide.[20]

II.8 Architecture du réseau informatique de CEVITAL

Le réseau interne de CEVITAL est étendu, reliant les différents bâtiments, unités de pro- duction et la direction du complexe. Il peut être segmenté en plusieurs parties, incluant le backbone, un pare-feu, une zone démilitarisée (DMZ), une couverture Wi-Fi, un routeur, ainsi qu'un centre de données (data center) où sont hébergés les serveurs de l'entreprise. La majorité des équipements utilisés sont de marque Cisco, et sont interconnectés grâce à la fibre optique ou aux câbles en cuivre.

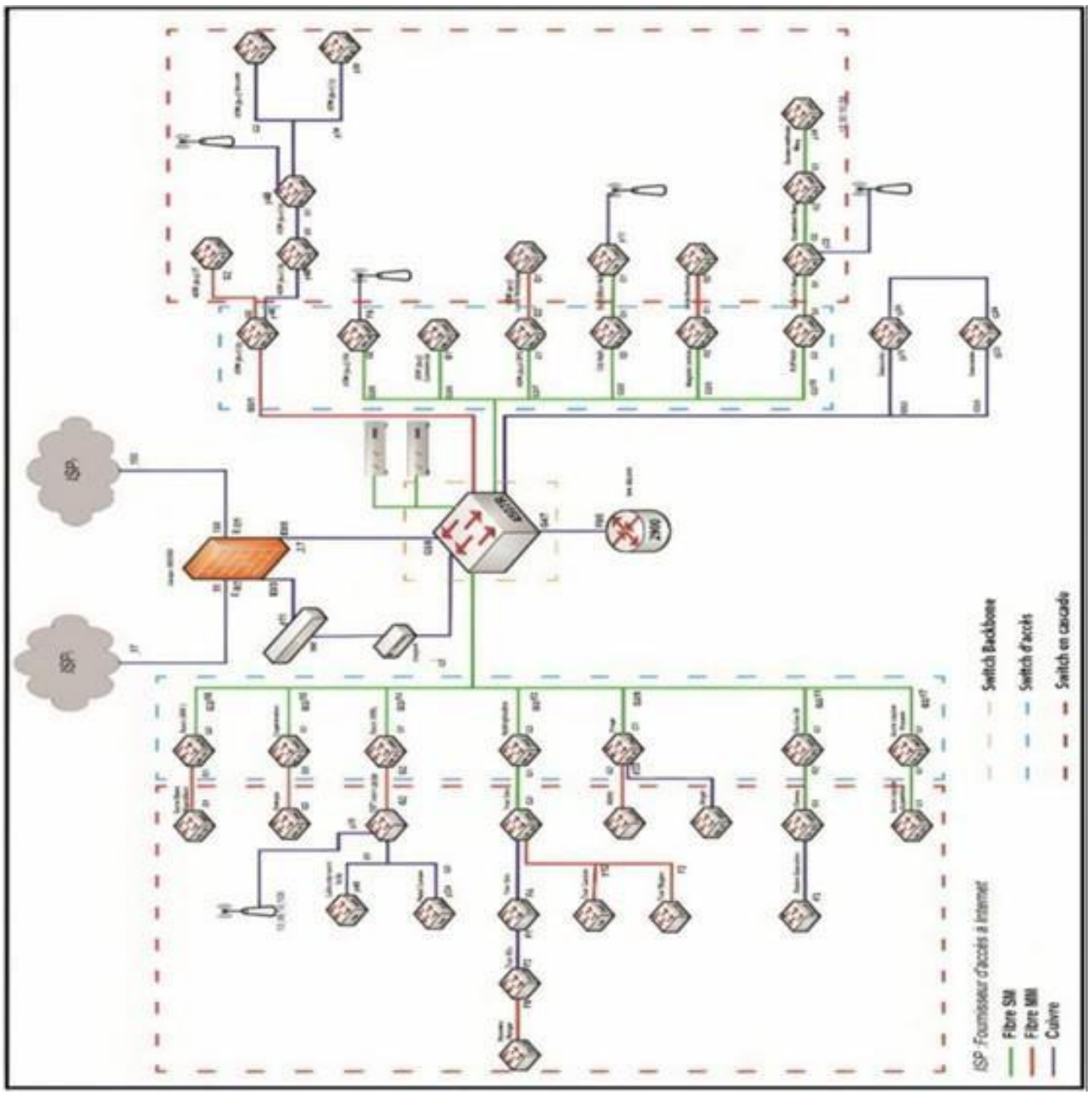


FIGURE II.5 – Architecture du réseau informatique du site Cevital-Bejaia

II.9 Les VLANs de l'entreprise

On trouve dans le tableau II.1 on trouve les détails des différents VLANs de l'entreprise (adresse réseau, passerelle) :

Direction	VLAN	Adresse réseau	Passerelle
DRH	VLAN 10	10.50.10.0/24	10.50.10.254
Direction des Appro	VLAN 11	10.50.11.0/24	10.50.11.254
DSI	VLAN 12	10.50.12.0/24	10.50.12.254
Raff sucre 3000T	VLAN 13	10.50.13.0/24	10.50.13.254
Raff Huile	VLAN 14	10.50.14.0/24	10.50.14.254
Division utilités	VLAN 15	10.50.15.0/24	10.50.15.254
Supply-chain	VLAN 16	10.50.16.0/24	10.50.16.254
Unité margarinerie	VLAN 17	10.50.17.0/24	10.50.17.254
Printer	VLAN 18	10.50.18.0/24	10.50.18.254
Téléphone	VLAN 20	10.50.20.0/24	10.50.20.254
Voice	VLAN 21	10.50.21.0/24	10.50.21.254
Direction R&D	VLAN 22	10.50.22.0/24	10.50.22.254
Performance industriel	VLAN 23	10.50.23.0/24	10.50.23.254
Unité Cdt Huile	VLAN 24	10.50.24.0/24	10.50.24.254
Management switch	VLAN 25	10.50.25.0/24	10.50.25.254
DFC	VLAN 26	10.50.26.0/24	10.50.26.254
Commercial	VLAN 27	10.50.27.0/24	10.50.27.254
Direction générale	VLAN 28	10.50.28.0/24	10.50.28.254
Direction qualité et management système	VLAN 29	10.50.29.0/24	10.50.29.254
Raff sucre 3500T	VLAN 30	10.50.30.0/24	10.50.30.254
Cdt sucre	VLAN 31	10.50.31.0/24	10.50.31.254
Caméra	VLAN 32	10.50.32.0/24	10.50.32.254
Projets	VLAN 33	10.50.33.0/24	10.50.33.254
Trituration	VLAN 36	10.50.36.0/24	10.50.36.254

TABLE II.1 – Les VLANs de l'entreprise.

II.10 Matériel utilisé dans l'architecture existante

Les équipements utilisés dans l'architecture réseau de Cevital sont :

— **Distributeur (Backbone) Cisco Catalyst 4507R :** Ce dispositif constitue un élément fondamental de la structure réseau de l'entreprise. Grâce à sa capacité à gérer un volume important de trafic, il assure une communication fluide entre les différents éléments du réseau. Il relie les commutateurs d'accès, les serveurs, les routeurs ainsi que le pare-feu,

et permet la circulation des données entre les VLAN. Il facilite également la connexion à Internet via le pare-feu, et peut être configuré pour distribuer automatiquement les adresses IP en tant que serveur DHCP. On l'appelle aussi communément le commutateur principal du réseau.

FIGURE II.6 – Switch Distributeur Cisco Catalyst 4507R [F10]

— **Routeur Cisco 2900 :** Il assure le routage des données entre les différents sites du réseau de manière simple et efficace.

FIGURE II.7 – Routeur Cisco 2900 [F11]

— **Switch Cisco Catalyst 2960 et 2950 :** Ils sont reliés au backbone. Ces équipements sont déployés dans les différents secteurs et bâtiments de l'entreprise.

FIGURE II.8 – Switch Cisco Catalyst 2960 [F12]

— **Point d'accès WIFI :** L'entreprise a déployé divers points d'accès Wi-Fi dans certaines zones du complexe afin d'assurer une connexion sans fil optimale et une couverture réseau élargie.

— **FIREWALL (Pare feu) :** Le pare-feu est déployé pour garantir la sécurité du réseau, isoler certains segments, et surveiller ainsi que sécuriser l'accès à Internet. Pour renforcer cette protection, quatre pare-feu sont interconnectés en redondance.

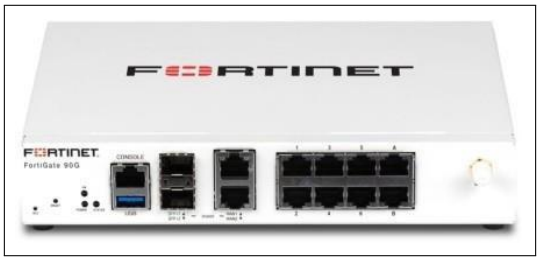


FIGURE II.9 – Firewall fortinet [F13]

— **Data center :** « Centre des Données » est un lieu ou une chambre qui est responsable sur la disponibilité et la continuité de toutes les réseaux de Cevital, cette chambre regroupe toutes les équipements nécessaire pour une architecture réseau (routeurs, switches niveau 2 et 3, pare-feu, etc), elle est équipé d'un système de refroidissement spécial qui assure le contrôle de la température moyenne des équipements, l'accès à ce lieu est autorisée juste aux responsables et les techniciens de la DSI (Direction Système d'Information), donc on peut considère l'un des pièces les plus sécurisées de Cevital et le noyau du réseau de l'entreprise.

FIGURE II.10 – Data center [F14]

II.11 Codification des équipements de Cevital

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

II.12 Liaison inter- sites (architecture WAN)

fin de garantir une communication optimale et un partage efficace des ressources, CEVITAL a mis en place des connexions entre son site de Bejaïa et plusieurs autres sites distants de

l'entreprise, y compris notamment

- Une liaison fibre optique point à point entre Bejaïa et Alger
- Des liaisons par satellite (VSAT) entre Bejaïa et les sites d'El-Kseur (Cojek), Tizi Ouzou (Lala Khadija) et El Kheroub (Constantine). [21]

II.13 Critique de l'existant

À la suite d'une analyse approfondie de l'infrastructure réseau actuelle de CEVITAL, plu- sieurs lacunes ont été mises en évidence. Cette évaluation nous a permis d'identifier un ensemble conséquent de contraintes fonctionnelles, susceptibles d'avoir un impact négatif sur les perfor- mances globales du réseau. Dans certains cas, ces limitations peuvent même engendrer des dysfonctionnements répétés. Les principaux constats issus de notre étude du réseau en place sont présentés ci-dessous.

- Le réseau utilise une liaison en cascade entre les switches, ce qui limite la bande passante, rend le système vulnérable aux pannes en cas de défaillance d'un switch, et engendre des coûts supplémentaires pour l'entreprise.
- L'utilisation d'un seul backbone concentre tout le trafic, ce qui risque de le surcharger et de dégrader les performances du réseau.

II.14 Problématique

Dans chaque entreprise industrielle, le côté informatique et réseau joue un rôle très important dans la continuité de la majorité des tâches essentielles dans l'entreprise. Toutefois, garantir la haute disponibilité et la performance du réseau nécessite la mise en place de mécanismes d'équilibrage de charge efficaces. Quels sont alors les protocoles et les moyens les plus adaptés pour atteindre cet objectif, tout en évitant les problèmes de factorisation et les pannes dues à un mauvais choix de protocoles ou d'équipements tels que les commutateurs ?

II.15 Propositions

- Utilisation des serveurs de répartition de charge (Load Balacers) pour garantir une répar- tition équitable (éviter la surcharge sur un seul serveur)
- Utilisation des liaisons doubles entre les équipements pour répartir le trafic et améliorer la bande passante.
- Utilisation des techniques de compression de donner pour optimiser le réseau et améliorer l'efficacité du transfert de données comme GZIP (GNU zip) qui est une méthode de compression de données utilisée dans les communications réseau avant l'envoi.

II.16 Solution

Pour avoir un équilibrage du charge dans un réseau d'entreprise, faudra appliqué des pro- tocoles et des solutions plus applicables pour gérer la distribution des paquets ; pour cela on utilise le HSRP (Hot Standby Router Protocol) pour garantir une disponibilité élevée à partir d'une mise en place d'une redondance matérielle dans ce réseau.

On utilisera aussi le protocole STP (Spanning Tree Protocol) pour éviter les boucles de commutation en désactivant les liaisons redondantes inutiles, l'objectif de ce protocole est d'annuler la manière de fonctionnement des routeurs passif/actif vers un fonctionnement simultané (diviser la charge des paquets).

Ces protocoles vont prévoir une disponibilité et vont assurer une connectivité continue et améliorer la fiabilité du réseau, et évite les pannes et les interruption du réseau,

II.17 Conclusion

Comme conclusion pour ce chapitre, on peut dire que la disponibilité de réseau dans une entreprise est très important pour la continuité de la reproduction de tous les services principaux, pour cela Cevital a utilisé plusieurs protocoles et technologie pour assure cette continuité sous le « l'équilibrage du charge » et « la haut disponibilité », ce qui donne à Cevital l'un des meilleurs architectures réseau à l'échelle national et régional.

Chapitre III

Équilibrage de charge dans un réseau

III.1 Introduction

L'équilibrage de charge dans un réseau est une technique permettant de répartir intelligem- ment les flux de données entre plusieurs ressources ou serveurs , Que ce soit pour les applications en ligne, les services internes d'une entreprise ou les infrastructures critiques comme les serveurs de fichiers ou de messagerie. L'équilibrage de charge garantit la performance, la disponibilité, et la résilience du système , Ce chapitre explore les objectifs, le fonctionnement, les types et les algorithmes de cette pratique indispensable dans les réseaux modernes. Enfin , nous citons quelques protocoles comme HSRP , GLBP , VRRP .

III.2 Définition d'un load balancing

L'équilibrage de charge consiste à répartir les tâches informatiques entre plusieurs machines. Sur Internet, il est fréquemment utilisé pour distribuer le trafic réseau entre plusieurs serveurs. Cette méthode permet d'alléger la charge de chaque serveur, d'améliorer leur efficacité, d'opti- miser les performances et de diminuer la latence. L'équilibrage de charge est donc indispensable au bon fonctionnement de la majorité des applications en ligne. [22]

III.3 Les objectifs de l'équilibrage de charge

Il existe plusieurs objectifs, on sites les 4 suivantes :

III.3.1 Haute disponibilité

L'équilibrage de charge permet plusieurs fonctionnalités qui assure la haute disponibilité ,ces fonctionnalités permettent de détecter et de récupérer des hôtes de cluster qui tombe en panne ou hors ligne, il équilibre aussi la charge du réseau lorsque les hôtes sont ajoutés ou supprimés, il permet aussi de récupérer et redistribuer la charge de travail en quelques dix secondes. [23]

III.3.2 Tolérance aux pannes

L'équilibrage de charge est très utile pour éviter les pannes même encore les rediriger d'une façon automatiquement que le trafic n'arrête pas au sein de l'entreprise. Ce processus se fait avec un équilibreur qui détecte le serveur qui tombe en panne et arrête l'envoi automatique du trafic vers ce serveur et le redirige vers un serveurs qui fonctionne toujours normal. Cette redirige se fait rapidement au point qu'il n'est pas visible au temps réel (fraction du seconds). [24]

III.3.3 Scalabilité

L'équilibrage de charge appliqué sur les serveurs d'une entreprise le donne un avantage qu'il soit évolutif et adaptatif au mise à échelle horizontale, c'est-à-dire il répond facilement aux demandes croissantes de trafic, par exemple si vous constatez une baisse ou des pic de trafic, il peut facilement augmenter ou diminuer le nombre des serveurs pour répondre à des besoins urgents. Il peuvent aussi gérer les volumes de requêtes importants et soudains, surtout à la période de promotions ou de soldes de fin d'année. [24]

III.3.4 Optimisation des performances

La plupart des entreprises commerciales obligent d'avoir un réseau vaste pour la maintenance de leurs données au niveau de leurs serveurs, l'équilibrage de charge est essentiel pour répartir la vitesse de trafic et les performances optimales entre tous les utilisateurs pour garantir qu'aucune serveur n'est surchargé et que la charge de travail est bien repartie (uniformément). [37]

III.4 Fonctionnement de l'équilibrage de charge

On peut divisé ce fonctionnement en deux parties :

III.4.1 Les composants essentiels

La figure figure III.1 montre les composants principaux d'un système d'équilibrage de charge :

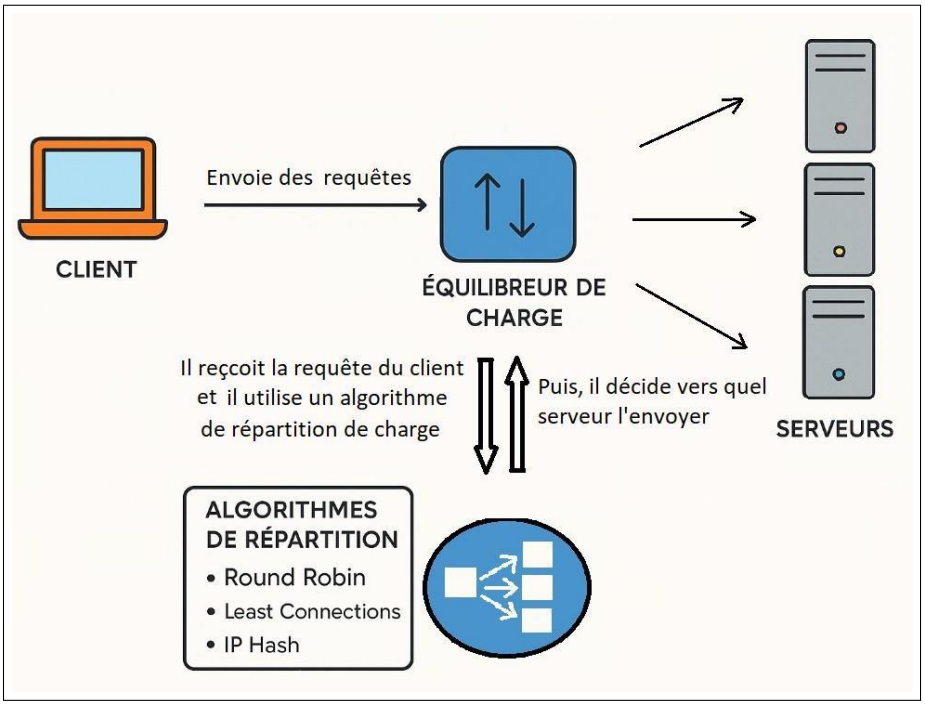


FIGURE III.1 – Système d'équilibrage de charge

III.4.2 Processus d'équilibrage

Cette opération se fait à partir d'un équilibreur de charge qui est un dispositif réseau qui réparti le trafic entrant sur plusieurs serveurs pour optimiser les performances et garantir la disponibilité des services, c'est-à-dire, il rend les serveurs utilisables d'une manière équitables.

L'équilibreur de charge fait une analyse de répartition des clients puis les dirige vers le ser- veur le plus approprié en utilisent des algorithmes de répartitions comme Round Robin, Least connections, IP Hashing, il sert aussi à la surveillance de l'état des serveurs et une tolérance aux pannes et la minimisation du temps d'arrêt.

En général, l'équilibrage de charge sert à garantir toutes performances pour avoir la dispo- nibilité et continuité des services applicatifs sur les serveurs d'une entreprise. [26]

III.5 Types d'équilibrage de charge

Les trois types d'équilibrage sont :

III.5.1 Équilibrage DNS

L'équilibrage de charge DNS opère au niveau de la couche d'application et se sert du pro- tocole UDP (User Datagram Protocol) sur la couche de transport du modèle TCP/IP pour la transmission des données, le DNS préfère le UDP mieux que le TCP en raison de sa rapidité et de la légèreté de ses paquets.

L'implémentation de l'équilibrage de charge DNS est assez facile comparativement à d'autres options et s'avère particulièrement bénéfique pour les PME (les petites entreprises et moyennes) au budgets limités. Elle ne demande pas des configurations complexes ni d'équipements ou logiciels spécialisés pour la répartition de charge, ce qui la rend utilisable par les organisations ayant des ressources IT (informatique) limités. Cette équilibrage peut être paramétrer afin de guider les utilisateurs vers des serveurs localisés dans des diverses régions géographiques. Cette option est particulièrement utile pour les entités internationales puisqu'elle offre la possibilité de faire transiter le trafic vers l'instance d'application de la plus proche et/ou de le réacheminement en vue d'assurer le respect du RGPD (responsabilise les organismes publics et privés qui traitent leurs données). [27]

III.5.2 Équilibrage au niveau réseau

Ce type d'équilibrage fonctionne au niveau de la couche transport du modèle OSI, donc il utilise les informations de cette couche (adresse IP source et destination, ports TCP/UDP) pour transporter le trafic réseau. Cette mise en œuvre est l'un des plus rapides, mais elle est moins efficace dans ce qui concerne la répartition uniforme de trafic.

Dans cette couche, le protocole TCP crée une connexion virtuelle entre deux hôtes, le pre- mier c'est l'hôte au le navigateur s'exécute et le deuxième c'est l'hôte sur l'application de serveur s'exécute. Des fois les paquets IP seront perdu ou désordre à cause de la nature fiable des réseaux, pour cela le TCP applique des mécanismes qui permet de corriger ces erreurs, transformant ainsi les flux de paquets IP en un canal de communication fiable. À chaque appli- cation est attribué un numéro de port TCP unique pour permettre la livraison à l'application appropriée sur les hôtes sur lesquels plusieurs applications sont en cours d'exécution.

Ce type d'équilibrage à plusieurs avantages comme l'optimisation de trafic et la réduction du temps d'attente pour les réseaux locaux et longue distance. [28]

III.5.3 Équilibrage au niveau Applicatif (couche d'application)

Ce type s'appelle aussi l'équilibrage de charge HTTP/ HTTPS ; il permet aux administra- teurs réseau de répartir le trafic en fonction des informations provenant de l'adresse HTTP, ce qui permet le mappage dynamique des ports hôtes et la distribution du trafic avec des données transmises via une adresse HTTP (URL, en-tête, cookies, etc). Le protocole HTTP sert à dé- finit le types de codage des données pour la communication entre les navigateurs Web et les serveurs Web (applications qui comprend le codage HTTP).

L'équilibrage de charge de cette couche permet au serveur de prendre des décisions d'équi- librage plus intelligentes et consiste l'une des options d'équilibrage les plus flexibles.

Ce type d'équilibrage consiste l'une des options d'équilibrage charge les plus flexibles, [29]

III.6 Algorithmes d'équilibrage de charge

Dans cette section, nous présentons quatre algorithmes standards d'équilibrage de charge :

III.6.1 Round robin

Round Robin est un algorithme de répartition de charge particulièrement simple et lar- gement utilisé dans les systèmes distribués. Son principe repose sur une logique cyclique , la première requête est envoyée au premier serveur, la seconde au deuxième, et ainsi de suite jus- qu'au dernier. Une fois que tous les serveurs ont été utilisés, le cycle recommence en attribuant la requête suivante à nouveau au premier serveur. L'équilibreur de charge ne tient pas compte de l'urgence des requêtes ni de la charge des serveurs, ce qui permet un traitement égal pour toutes les demandes. Cette méthode est efficace dans les environnements homogènes où les ressources sont équitablement réparties entre les serveurs..[30]

Avantages

- Facile à mettre en œuvre et ne nécessite pas de ressources complexes.
- Distribue les requêtes de manière équitable entre les serveurs.

Inconvénients

- Ne prend pas en compte la charge de chaque serveur.
- Peut entraîner une répartition inefficace si les requêtes sont de tailles différentes.

III.6.2 Least connection

Les requêtes sont attribuées aux serveurs en fonction du nombre de connexions actives en cours , le serveur avec le moins de connexions reçoit la prochaine requête. Cette stratégie est fortement adaptée aux clusters homogènes, où chaque serveur dispose de ressources simi- laires. Ne pas suivre cette méthode peut provoquer des ralentissements dans le traitement des requêtes.[31]

Avantages

- Il optimise la répartition de la charge en dirigeant les requêtes vers le serveur avec le moins de connexions actives.
- Il est particulièrement efficace dans les environnements où les durées des connexions sont variées, assurant ainsi une meilleure gestion de la charge.

Inconvénients

- Il crée une surcharge de calcul car il doit constamment suivre et mettre à jour le nombre de connexions actives sur chaque serveur.
- Il peut rencontrer des problèmes avec les connexions longues, car ces serveurs continuent de recevoir des requêtes malgré leur forte charge.

III.6.3 IP hashing

IP Hashing est une méthode de répartition de charge entre un ensemble de serveurs. Il utilise l'adresse IP du client comme une clé d'entrée pour déterminer le serveur cible. L'idée principale de cet algorithme est d'appliquer une fonction de hachage (Hash Function) à l'adresse IP afin de la transformer en une valeur numérique. Cette valeur est ensuite utilisée pour sélectionner un serveur de manière régulière et déterministe. [32]

Avantages

- Une même adresse IP sera toujours dirigée vers le même serveur, ce qui aide à maintenir des sessions stables.
- Réduction du besoin de stockage centralisé des sessions : Comme un client est toujours redirigé vers le même serveur, il est souvent inutile de partager les données de session entre les serveurs.

Inconvénients

- Si le nombre de serveurs change (ajout ou suppression), de nombreuses adresses seront redirigées vers d'autres serveurs, ce qui peut perturber la stabilité des sessions.
- Ne prend pas en compte la charge actuelle des serveurs, ce qui peut entraîner une répar- tition déséquilibrée du trafic.

III.7 Les protocoles qui permettent l'équilibrage de charge

Nous allons citer quelques protocoles utiles pour l'équilibrage de charge :

III.7.1 Protocole HSRP (Hot Standby Routing Protocol)

C'est un protocole utilisé pour assurer la continuité d'accès à Internet dans réseau, même si il tombe en panne. Il permet à plusieurs routeurs de partager une seule adresse IP dite « virtuelle », qui sert de passerelle pour les utilisateurs. Un routeur principal est actif, un autre est en attente, prêt à prendre le relais automatiquement en cas de problème. Ce système évite les coupures de connexion et garantir une haute disponibilité du réseau. [33]

III.7.2 Protocole VRRP (Virtual Router Redundancy Protocol)

C'est un protocole qui permet à plusieurs routeurs de collaborer pour assurer une seule et même passerelle IP aux machines d'un réseau. L'un des routeurs est désigné comme maître (ou actif), et les autres sont en veille. Si le routeur maître tombe en panne, un autre prend automatiquement le relais, sans interruption visible pour les utilisateurs. Cela garantit une connexion réseau continue, même en cas de défaillance d'un équipement. [34]

III.7.3 HSRP et VRRP en équilibrage de charge

L'équilibrage de charge ne se fait pas automatiquement ; il doit être configuré manuellement. Pour répartir le trafic entre deux routeurs par défaut, il faut créer deux routeurs par défaut, il faut créer deux adresses IP virtuelles appartenant à deux groupes VRRP différents mais qui se chevauchent. On configure le premier routeur comme principal pour la première adresse IP virtuelle, et en même temps comme routeur de secours pour la seconde. Ensuite, vous faites l'inverse pour le second router (il sera principal pour la deuxième adresse IP virtuelle et secours pour la première). Enfin, i répartis les hôtes du réseau ; la moitié utilisera la première adresse IP comme passerelle, et l'autre moitié utilisera la deuxième, ce qui permet de partager la charge entre les deux routeurs. [35]

III.7.4 Protocole GLBP (Gateway Load Balancing Procol)

C'est un protocole qui permet de répartir la charge réseau entre plusieurs passerelles, contrai- rement aux protocoles traditionnels ou une seule passerelle active est utilisée par groupe. Dans un groupe GLBP, un routeur est élu Active Virtual Gateway (AVG) selon la priorité la plus élevée ou, en cas d'égalité, selon la plus haute adresse IP. L'AVG attribue des adresses MAC virtuelles aux routeurs appelés Active Virtual Forwarders (AVF), qui assurent le transfert réel du trafic. L'AVG répond également aux requêtes ARP pour l'adresse IP virtuelle et distribue la charge entre les AVFs. [36]

III.7.5 Comparaison entre les protocoles

Le protocole GLBP est configurables seulement dans les routeurs. Par contre les deux autres protocoles HSRP et VRRP sont des protocoles configurables ainsi au niveau des switches du niveau 3.

Pour qu'il face un équilibrage de charge, le HSRP et le VRRP doivent être configurés manuellement, contrairement au GLBP qui applique l'équilibrage de charge automatiquement

Le protocole GLBP et HSRP sont des protocoles de propriétaire CISCO par contre le VRRP est un protocole standart

Dans notre architecture nous utilisons des switches niveau 3, donc le GLBP n'est pas un choix applicable. HSRP c'est un protocole propriétaire de Cisco et puisque nous allons simuler notre architecture sur Cisco Packet Tracer donc nous avons choisis les protocoles HSRP et STP.

III.8 Conclusion

Dans ce chapitre nous avons présenté l'équilibrage de charge en définissant ses objectifs, son fonctionnement, ses types et les principaux algorithmes utilisés. Cette étude a permis de montrer l'importance de l'équilibrage de charge pour assurer de bonnes performances, une meilleure disponibilité et une plus grande fiabilité des réseaux.

Chapitre IV

Conception et Réalisation

IV.1 Introduction

Dans les entreprises et dans le domaine de l'industrie consiste à avoir un réseau informatique fiable, disponible et répond aux exigences de performances élevés, cela les oblige d'avoir une infrastructure qui applique l'équilibrage de charge pour garantir la connectivité, la disponibilité et les performances sur les serveurs de l'entreprise.

Ce chapitre expose la conception et la réalisation de notre projet intitulé la mise en place d'une infrastructure qui garantie l'équilibrage de charge d'un réseau de Cevital. Nous allons appliqué toutes les configuration ainsi que les protocoles nécessaires telles que la configuration des VLANs, VTP et protocoles STP, SSH, HSRP, Line console, bpdu gaurd et port fast, tous cela se fait sur le logiciel du simulation Cisco Packet Tracer. Les étape seront détaillées, claires et accompagnées par des figures qui facilite la compréhension. Enfin , nous présentons les tests de validation de l'efficacité de la topologie réalisé

IV.2 Présentation du simulateur Cisco Packet Tracer 8.2.2

Cisco Packet Tracer est un logiciel de simulation de réseaux conçu principalement pour les équipements Cisco, c'est un outil gratuit qui permet de réaliser des architecteurs réseaux et de simuler leurs comportements de différents protocoles , L'utilisateur met en place son réseau en utilisant des équipements tels que des routeurs, des commutateurs et des ordinateurs..etc. Ces dispositifs doivent être reliés à l'aide de différents types de câbles, comme les câbles coaxiaux, la fibre optique,...etc. Une fois tous les éléments connectés, il sera alors possible de configurer les adresses IP, d'activer les services nécessaires et d'effectuer plusieurs réglages sur chaque équipement.

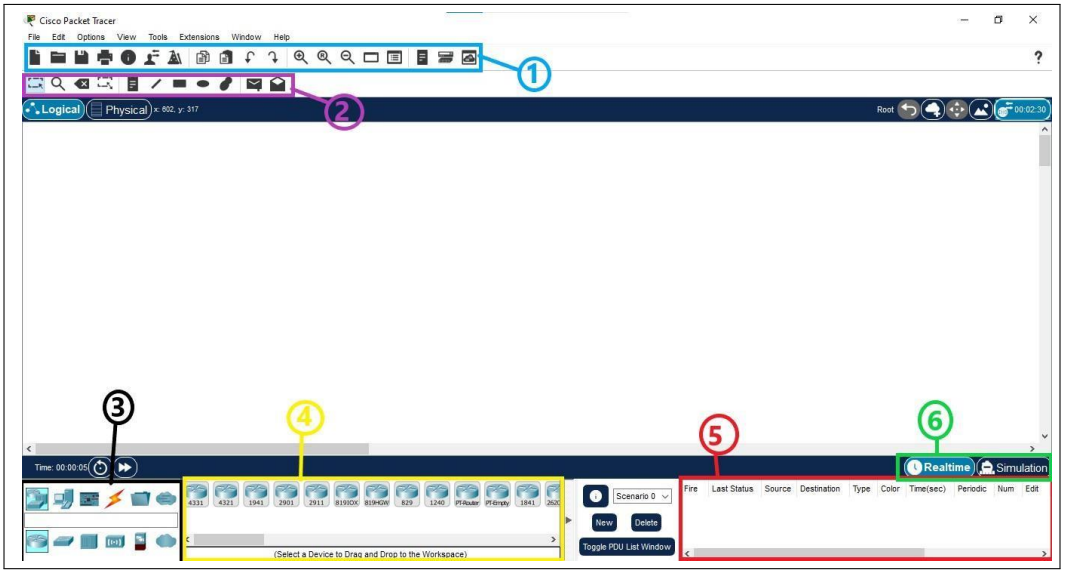


FIGURE IV.1 – Interface de cisco packet tracer

Zone 01 : c'est la barre d'outils principale regrouper des icônes pour les actions cou- rantes, comme la création des fichiers, l'enregistrement, l'impression, et d'autres fonctionnalités importantes.

Zone 02 : c'est la barre d'outils secondaire contient des outils qui aide dans la sélection, le déplacement ,la suppression d'éléments, et aussi la possibilité de tester le ping entre les équipement (envoi d'un ping).

Zone 03 : c'est la zone de sélection d'équipement permet de choisir le type d'équipement à ajouter dans la catégorie sélectionné (routeurs, switchs, hub, câbles. etc).

Zone 04 : c'est la zone qui présente les différentes catégories d'équipements disponibles, se qui simplifier la sélection des éléments spécifiques dans l'import quel réseau.

Zone 05 : c'est la zone de simulation qui affiche le résultat de teste de ping entre les équipements (la continuité).

Zone 06 : c'est l'icône qui permet de visualisé passage des paquets dans un réseau à travers le mode simulation, il a deux mode (Realtime et Simulation).

IV.3 Nouvelle architecture du réseau Cevital

Notre nouvelle architecture a été conçue pour améliorer l'ancienne structure de Cevital, en garantissant une meilleure performance, une haute disponibilité et une continuité de service optimale.

Elle est basée sur une conception à deux couches : la couche Core et la couche d'accès

- **Couche Core :** Dans cette couche, nous avons deux switches cœur de niveau 3 afin d'assurer une connectivité plus rapide et de répartir l'acheminement du trafic entre les deux switches
- **Couche Accès :** Dans cette couche, les utilisateurs sont reliés aux switches de niveau 2

Pour améliorer l'ancienne architecture, nous allons ajouter un switch de couche 3 ainsi que quelques protocoles tels que HSRP pour garantir la continuité de service et la haute disponi- bilité, VTP pour gérer les VLANs, et STP pour éviter les boucles. De plus, les fonctionnalités PortFast et BPDU Guard seront utilisées pour sécuriser le réseau et faciliter la connexion des périphériques.

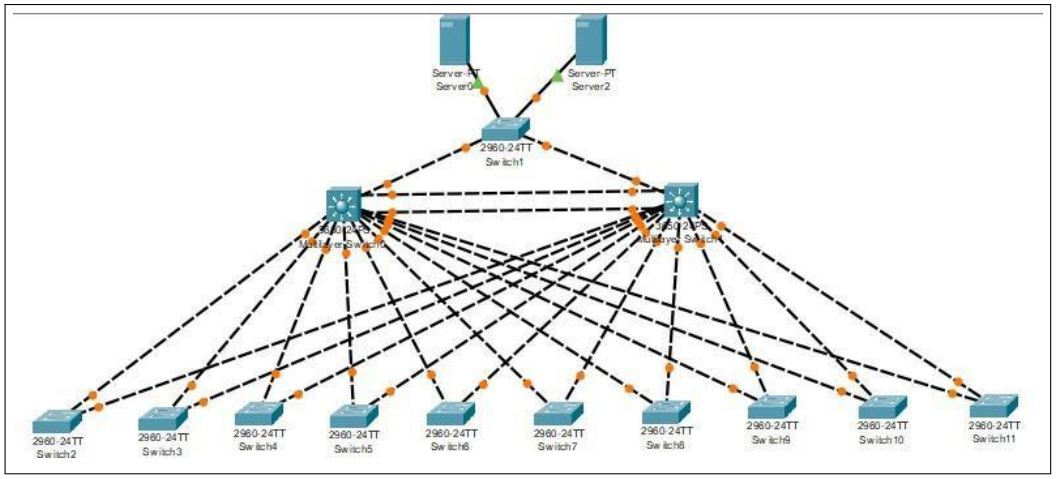


FIGURE IV.2 – Nouvelle architecture

IV.3.1 Présentation des équipements utilisé

Dans le tableau ci-dessous on exposer les différents équipements qu'on a utilisé dans notre topologie et leur nombre, ainsi que leurs nomination

Couche	Équipement du modèle type	Nombre	Nomination
Couche core	Switch cisco C3650-24PS	2	SWC
Couche d'accès	Switch cisco C2960-24TT	10	SWA
PC	PC-PT	20	PC
Serveur	Server-PT	2	Server
Switch serveur	Switch cisco C2960-24TT	1	SWAS

TABLE IV.1 – Les équipements utilisés sur la topologie.

IV.3.2 Vlans de l'entreprise

Ce tableau présente toutes les directions du Cevital et leurs VLANs utilisés, ainsi que les differntes adresses IP du chaque direction (IP SWC1, IP SWC2, Passerelle)

Direction	VLAN	IP SWC1	IP SWC2	Passerelle
DRH	VLAN10	10.50.10.252	10.50.10.253	10.50.10.254
Direction des Appro	VLAN11	10.50.11.252	10.50.11.253	10.50.11.254
DSI	VLAN12	10.50.12.252	10.50.12.253	10.50.12.254
Raff Huile	VLAN13	10.50.13.252	10.50.13.253	10.50.13.254
Raff sucre 300T	VLAN14	10.50.14.252	10.50.14.253	10.50.14.254
Division utilités	VLAN15	10.50.15.252	10.50.15.253	10.50.15.254
Supply-chain	VLAN16	10.50.16.252	10.50.16.253	10.50.16.254
Unité margarinerie	VLAN17	10.50.17.252	10.50.17.253	10.50.17.254
Server	VLAN18	10.50.18.252	10.50.18.253	10.50.18.254
Téléphone	VLAN20	10.50.20.252	10.50.20.253	10.50.20.254
Voice	VLAN21	10.50.21.252	10.50.21.253	10.50.21.254
Direction R&D	VLAN22	10.50.22.252	10.50.22.253	10.50.22.254
Performance industriel	VLAN23	10.50.23.252	10.50.23.253	10.50.23.254
Unité Cdt Huile	VLAN24	10.50.24.252	10.50.24.253	10.50.24.254
Management switch	VLAN25	10.50.25.252	10.50.25.253	10.50.25.254
DFC	VLAN26	10.50.26.252	10.50.26.253	10.50.26.254
Commercial	VLAN27	10.50.27.252	10.50.27.253	10.50.27.254
Direction générale	VLAN28	10.50.28.252	10.50.28.253	10.50.28.254
Direction qualité et management système	VLAN29	10.50.29.252	10.50.29.253	10.50.29.254
Raff sucre 3500T	VLAN30	10.50.30.252	10.50.30.253	10.50.30.254
Cdt sucre	VLAN31	10.50.31.252	10.50.31.253	10.50.31.254
Caméra	VLAN32	10.50.32.252	10.50.32.253	10.50.32.254
Projets	VLAN33	10.50.33.252	10.50.33.253	10.50.33.254
Trituration	VLAN36	10.50.36.252	10.50.36.253	10.50.36.254

TABLE IV.2 – Les Vlans de l'entreprise.

IV.3.3 Allumage des switches C3650-24 PS

L'allumage des switches C3650-24 PS nécessite l'ajout d'une alimentation de modèle AC-POWER-SUPPLY

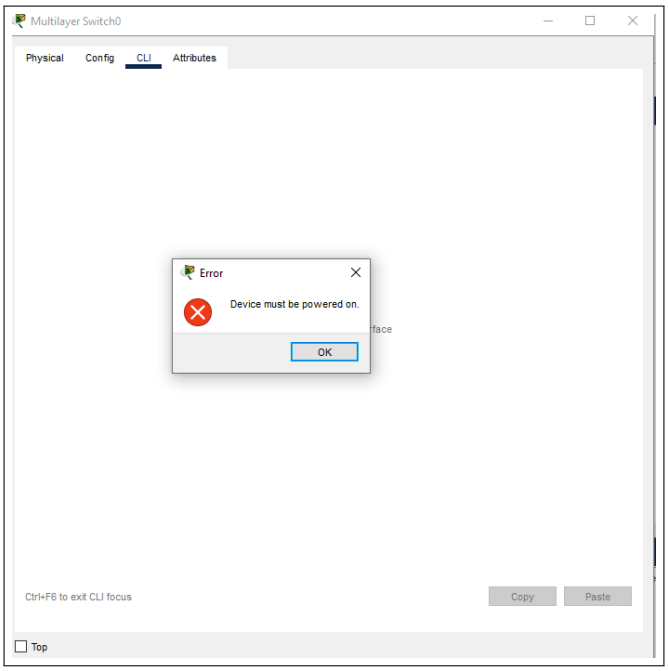


FIGURE IV.3 – Switch sans alimentation

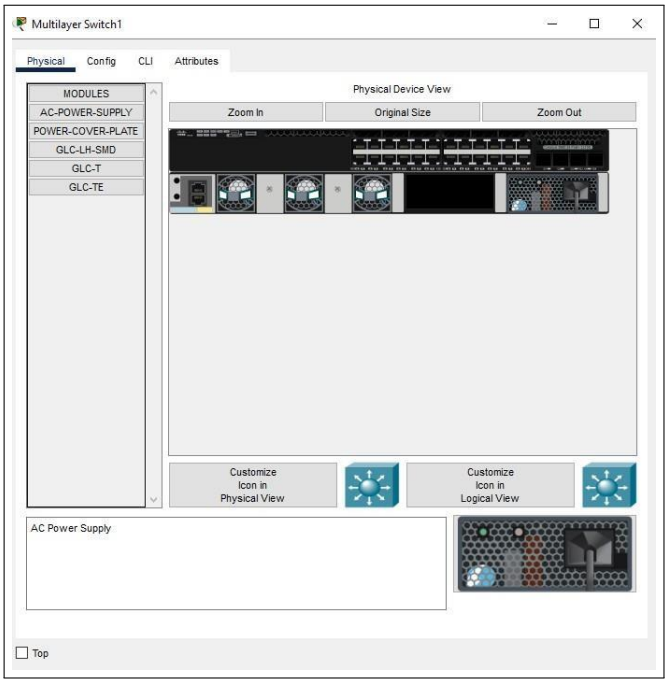


FIGURE IV.4 – Switch doté d'une alimentation

IV.4 Configuration de Hostname

Comme première étape de réalisation de notre topologie, nous commençons par l'attribu- tion des noms significatifs pour avoir reconnaitre chaque équipement, tous ça se fait avec la commande « hostname ».

```
Switch>enable
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SWC1
SWC1(config)#
```

FIGURE IV.5 – Configuration de Hostname

IV.4.1 Sauvgarder de la configuration

Après chaque étape de configuration, il est important de sauvegarder les paramètres avec la commande **« copy running-config startup-config »**, afin de ne pas perdre les modifications en cas d'extinction des appareils

```
SWC2(config)#do copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

FIGURE IV.6 – Suavgarder de la configuration

IV.5 Configuration du VTP

Afin de faciliter le travail et de réduire les efforts, nous allons configurer le protocole VTP en définissant le switch SWC1 comme serveur, tandis que les autres switches seront configurés comme clients. Cela nous permettra d'ajouter et de supprimer des VLANs directement depuis le switch SWC1

- Configurer SWC1 comme un VTP serveur :

```
SWC1(config)#vtp mode server
Device mode already VTP SERVER.
SWC1(config)#vtp version 2
SWC1(config)#vtp domain CEV.com
Changing VTP domain name from NULL to CEV.com
SWC1(config)#vtp password cev
Setting device VLAN database password to cev
```

FIGURE IV.7 – Configuration du VTP server sur SWC1

- Configurer les autres switches comme un VTP client

```
SWC2(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWC2(config)#vtp domain CEV.com
Changing VTP domain name from NULL to CEV.com
SWC2(config)#vtp password cev
Setting device VLAN database password to cev
SWC2(config)#S
```

FIGURE IV.8 – Configuration du VTP client

IV.5.1 Vérification du VTP

On va vérifier si le VTP est bien configuré à l'aide de la commande **« show vtp status».**

```
SWC1(config)#do sh vtp stat
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                       : 000C.CF25.1000
Configuration last modified by 0.0.0.0 at 3-1-93 00:02:14
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
Configuration Revision          : 0
MD5 digest                      : 0x33 0xBB 0xF9 0xD3 0x04 0xCB 0x3F 0x46
                                  0xD2 0xB2 0x99 0x54 0xA1 0x38 0x79 0x08
```

FIGURE IV.9 – Vérification de la configuration du VTP

IV.6 Création des Vlans

On va créer tous les VLANs d'entreprise sur le SWC1 comme indiqué ci-dessous.

```
SWC1(config-vlan)#vlan 10
SWC1(config-vlan)#name DRH
SWC1(config-vlan)#vlan 11
SWC1(config-vlan)#name Direction_des_Appro
SWC1(config-vlan)#vlan 12
SWC1(config-vlan)#name DSI
```

FIGURE IV.10 – Création des Vlans sur SWC1

IV.6.1 Vérification de la création des Vlans

Pour la vérification , on va utiliser la commande **« show vlan brief ».**

```
10   DRH                                active
11   Direction_des_Appro                active
12   DSI                                active
13   Raff_Huile                         active
14   Raff_sucre_300T                    active
15   Division_utilits                   active
16   Supply-chain                       active
17   Unit_margarinerie                  active
18   Server                             active
20   Tlphone                            active
21   Voice                              active
22   Direction_R&D                      active
23   Performance_industriel             active
24   Unit_Cdt_Huile                     active
25   Management_switch                  active
26   DFC                                active
27   Commercial                         active
28   Direction_gnrale                   active
29   Direction_qualit_et_management_systme active
30   Raff_sucre_3500T                   active
31   Cdt_sucre                          active
32   Camra                              active
33   Projets                            active
36   Trituration                        active
```

FIGURE IV.11 – Vérification de la Création des Vlans

IV.7 Configuration des Liens trunks

Nous allons configurer des liaisons trunk sur les ports qui relient les switches afin de per- mettre le passage des VLANs et qu'ils soient visibles sur tous les switches

```
SWC1(config)#interface range gigabitEthernet 1/0/1-12
SWC1(config-if-range)#switchport mode trunk




SWC1(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/4, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to
```

FIGURE IV.12 – Configuration des liens trunks sur le SWC1

IV.7.1 Vérification des liens trunks

Pour la vérification , on va utiliser la commande **« show interfaces trunk ».**

```
SWC1(config-if-range)#do sh interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Gigl/0/1    on           802.1q         trunking      1
Gigl/0/2    on           802.1q         trunking      1
Gigl/0/3    on           802.1q         trunking      1
Gigl/0/4    on           802.1q         trunking      1
Gigl/0/5    on           802.1q         trunking      1
Gigl/0/6    on           802.1q         trunking      1
Gigl/0/7    on           802.1q         trunking      1
Gigl/0/8    on           802.1q         trunking      1
Gigl/0/9    on           802.1q         trunking      1
Gigl/0/10   on           802.1q         trunking      1
Gigl/0/11   on           802.1q         trunking      1
Gigl/0/12   on           802.1q         trunking      1
```

FIGURE IV.13 – Vérification des liens trunks sur SWC1

IV.7.2 Vérification des vlans sur les clients

La configuration des liens trunk permet désormais la propagation des VLANs vers les autres switches du réseau

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gigl/0/13, Gigl/0/14, Gigl/0/15,
Gigl/0/16
                                                 Gigl/0/17, Gigl/0/18, Gigl/0/19,
Gigl/0/20
                                                 Gigl/0/21, Gigl/0/22, Gigl/0/23,
Gigl/0/24
                                                 Gigl/1/1, Gigl/1/2, Gigl/1/3, Gigl/1/4
10   DRH                               active
11   Direction_des_Appro               active
12   DSI                               active
13   Raff_Huile                        active
14   Raff_sucre_300T                   active
15   Division_utilits                  active
16   Supply-chain                      active
17   Unit_margarinerie                 active
18   Server                            active
20   Tlphone                           active
21   Voice                             active
22   Direction_R&D                     active
23   Performance_industriel            active
24   Unit_Cdt_Huile                    active
25   Management_switch                 active
26   DFC                               active
27   Commercial                        active
28   Direction_gnrale                  active
29   Direction_qualit_et_management_systme active
30   Raff_sucre_3500T                  active
31   Cdt_sucre                         active
32   Camra                             active
33   Projets                           active
36   Trituration                       active
```

FIGURE IV.14 – Propagation des Vlans sur SWC2

IV.8 Configuration des liens EtherChannel

Nous allons configurer l'EtherChannel sur les commutateurs SWC1 et SWC2, obtenir un nouveau port et le placer en mode trunk, La même configuration sera réalisée sur SWC1 et SWC2.

```
SWC1(config-if)#interface range gigabitEthernet 1/0/12-13
SWC1(config-if-range)#channel-group 1 mode on
```

FIGURE IV.15 – Configuration de l'Etherchannel

```
SWC1(config)#interface port-channel 1
SWC1(config-if)#switchport mode trunk
```

FIGURE IV.16 – Configuration en mode trunk

IV.9 Configuration d'adresses IP virtuelles pour les VLANs sur SWC1 et SWC2

Dans cette étape, nous allons attribuer une adresse IP à chaque VLAN. Les adresses doivent être différentes sur SWC1 et SWC2 : l'adresse se terminant par 252 sera utilisée pour SWC1, et celle se terminant par 253 pour SWC2

```
SWC1(config)#interface vlan10
SWC1(config-if)#ip address 10.50.10.252 255.255.255.0
SWC1(config-if)#no shutdown
SWC1(config-if)#exit
SWC1(config)#interface vlan11
SWC1(config-if)#ip address 10.50.11.252 255.255.255.0
SWC1(config-if)#no shutdown
SWC1(config-if)#exit
SWC1(config)#interface vlan12
SWC1(config-if)#ip address 10.50.12.252 255.255.255.0
SWC1(config-if)#no shutdown
SWC1(config-if)#exit
SWC1(config)#interface vlan13
SWC1(config-if)#ip address 10.50.13.252 255.255.255.0
SWC1(config-if)#no shutdown
SWC1(config-if)#exit
SWC1(config)#interface vlan14
SWC1(config-if)#ip address 10.50.14.252 255.255.255.0
SWC1(config-if)#no shutdown
SWC1(config-if)#exit
SWC1(config)#interface vlan15
SWC1(config-if)#ip address 10.50.15.252 255.255.255.0
SWC1(config-if)#no shutdown
SWC1(config-if)#exit
SWC1(config)#interface vlan16
SWC1(config-if)#ip address 10.50.16.252 255.255.255.0
SWC1(config-if)#no shutdown
SWC1(config-if)#exit
SWC1(config)#interface vlan17
SWC1(config-if)#ip address 10.50.17.252 255.255.255.0
SWC1(config-if)#no shutdown
SWC1(config-if)#exit
SWC1(config)#interface vlan18
SWC1(config-if)#ip address 10.50.18.252 255.255.255.0
SWC1(config-if)#no shutdown
SWC1(config-if)#exit
```

FIGURE IV.17 – Configuration des SVI sur SWC1

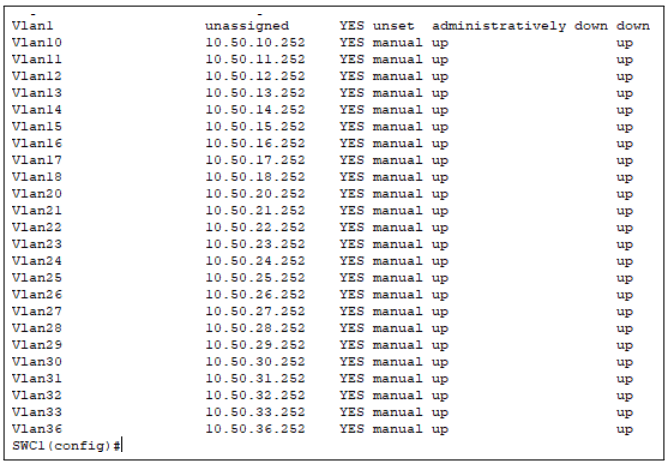
```
SWC2(config)#interface vlan20
SWC2(config-if)#ip address 10.50.20.253 255.255.255.0
SWC2(config-if)#no shutdown
SWC2(config-if)#exit
SWC2(config)#interface vlan21
SWC2(config-if)#ip address 10.50.21.253 255.255.255.0
SWC2(config-if)#no shutdown
SWC2(config-if)#exit
SWC2(config)#interface vlan22
SWC2(config-if)#ip address 10.50.22.253 255.255.255.0
SWC2(config-if)#no shutdown
SWC2(config-if)#exit
SWC2(config)#interface vlan23
SWC2(config-if)#ip address 10.50.23.253 255.255.255.0
SWC2(config-if)#no shutdown
SWC2(config-if)#exit
SWC2(config)#interface vlan24
SWC2(config-if)#ip address 10.50.24.253 255.255.255.0
SWC2(config-if)#no shutdown
SWC2(config-if)#exit
```

FIGURE IV.18 – Configuration des SVI sur SWC2

IV.9.1 Vérification des SVI sur SW1 et SW2

Pour la vérification , on va utiliser la commande **« show ip interface brief ».**

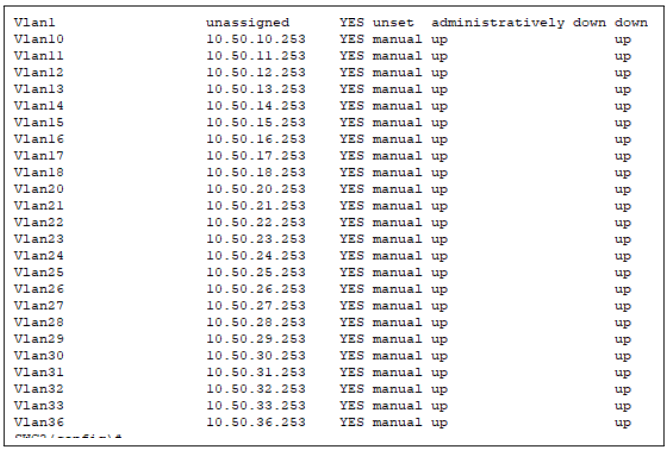
- **Sur SWC1**



```
Vlan1                  unassigned      YES unset  administratively down down
Vlan10                 10.50.10.252    YES manual up                    up
Vlan11                 10.50.11.252    YES manual up                    up
Vlan12                 10.50.12.252    YES manual up                    up
Vlan13                 10.50.13.252    YES manual up                    up
Vlan14                 10.50.14.252    YES manual up                    up
Vlan15                 10.50.15.252    YES manual up                    up
Vlan16                 10.50.16.252    YES manual up                    up
Vlan17                 10.50.17.252    YES manual up                    up
Vlan18                 10.50.18.252    YES manual up                    up
Vlan20                 10.50.20.252    YES manual up                    up
Vlan21                 10.50.21.252    YES manual up                    up
Vlan22                 10.50.22.252    YES manual up                    up
Vlan23                 10.50.23.252    YES manual up                    up
Vlan24                 10.50.24.252    YES manual up                    up
Vlan25                 10.50.25.252    YES manual up                    up
Vlan26                 10.50.26.252    YES manual up                    up
Vlan27                 10.50.27.252    YES manual up                    up
Vlan28                 10.50.28.252    YES manual up                    up
Vlan29                 10.50.29.252    YES manual up                    up
Vlan30                 10.50.30.252    YES manual up                    up
Vlan31                 10.50.31.252    YES manual up                    up
Vlan32                 10.50.32.252    YES manual up                    up
Vlan33                 10.50.33.252    YES manual up                    up
Vlan36                 10.50.36.252    YES manual up                    up
SWC1(config)#
```

FIGURE IV.19 – Vérification des SVI sur SWC1

- **Sur SWC2**

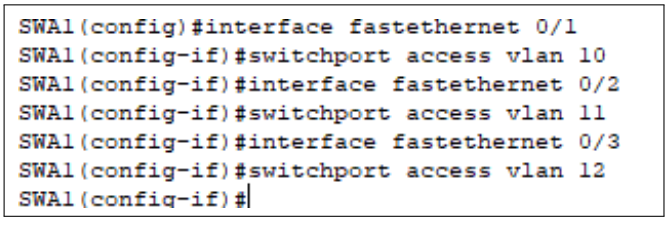


```
Vlan1                  unassigned      YES unset  administratively down down
Vlan10                 10.50.10.253    YES manual up                    up
Vlan11                 10.50.11.253    YES manual up                    up
Vlan12                 10.50.12.253    YES manual up                    up
Vlan13                 10.50.13.253    YES manual up                    up
Vlan14                 10.50.14.253    YES manual up                    up
Vlan15                 10.50.15.253    YES manual up                    up
Vlan16                 10.50.16.253    YES manual up                    up
Vlan17                 10.50.17.253    YES manual up                    up
Vlan18                 10.50.18.253    YES manual up                    up
Vlan20                 10.50.20.253    YES manual up                    up
Vlan21                 10.50.21.253    YES manual up                    up
Vlan22                 10.50.22.253    YES manual up                    up
Vlan23                 10.50.23.253    YES manual up                    up
Vlan24                 10.50.24.253    YES manual up                    up
Vlan25                 10.50.25.253    YES manual up                    up
Vlan26                 10.50.26.253    YES manual up                    up
Vlan27                 10.50.27.253    YES manual up                    up
Vlan28                 10.50.28.253    YES manual up                    up
Vlan29                 10.50.29.253    YES manual up                    up
Vlan30                 10.50.30.253    YES manual up                    up
Vlan31                 10.50.31.253    YES manual up                    up
Vlan32                 10.50.32.253    YES manual up                    up
Vlan33                 10.50.33.253    YES manual up                    up
Vlan36                 10.50.36.253    YES manual up                    up
```

FIGURE IV.20 – Vérification des SVI sur SWC2

IV.10 Configuration les ports en mode d'accès

Nous allons maintenant configurer les ports des switches de couche d'accès en mode accès afin que les PC puissent accéder aux VLANs, en attribuant un seul VLAN à chaque port de type FastEthernet



```
SWA1(config)#interface fastethernet 0/1
SWA1(config-if)#switchport access vlan 10
SWA1(config-if)#interface fastethernet 0/2
SWA1(config-if)#switchport access vlan 11
SWA1(config-if)#interface fastethernet 0/3
SWA1(config-if)#switchport access vlan 12
SWA1(config-if)#
```

FIGURE IV.21 – L'attribution des ports aux Vlans

IV.10.1 Vérification des ports attribués aux Vlans

On va vérifier l'attribution des ports à l'aide de la commande **« show vlan brief ».**

```
SWA1(config-if)#do sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------
1    default                           active
10   DRH                               active    Fa0/1
11   Direction_des_Appro               active    Fa0/2
12   DSI                               active    Fa0/3
13   Raff_Huile                        active    Fa0/4
14   Raff_sucre_300T                   active    Fa0/5
15   Division_utilits                  active    Fa0/6
16   Supply-chain                      active    Fa0/7
17   Unit_margarinerie                 active    Fa0/8
18   Printer                           active    Fa0/9
20   Tlphone                           active    Fa0/10
21   Voice                             active    Fa0/11
22   Direction_R&D                     active    Fa0/12
23   Performance_industriel            active    Fa0/13
24   Unit_Cdt_Huile                    active    Fa0/14
25   Management_switch                 active    Fa0/15
26   DFC                               active    Fa0/16
27   Commercial                        active    Fa0/17
28   Direction_gnrale                  active    Fa0/18
29   Direction_qualit_et_management_systme active    Fa0/19
30   Raff_sucre_3500T                  active    Fa0/20
31   Cdt_sucre                         active    Fa0/21
32   Camra                             active    Fa0/22
33   Projets                           active    Fa0/23
36   Trituration                       active    Fa0/24
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

FIGURE IV.22 – Vérification des ports attribués aux Vlans

IV.11 Configuration du DHCP

Pour faciliter la gestion et l'attribution des adresses IP, nous allons configurer le service DHCP sur les deux switches core. Pour éviter les conflits, chaque plage d'adresses sera divisée en deux : de 1 à 127 pour la première moitié, et de 128 à 254 pour la seconde. Chaque switch core se verra attribuer une seule moitié. Ainsi, sur SWC1, nous allons exclure les adresses de 128 à 254, et sur SWC2, celles de 1 à 127. et les adresses de 252 à 254 seront également exclues

- **Sur le SWC1**

```
Enter configuration commands, one per line.  End with CNTL/Z.
SWC1(config)#ip dhcp excluded-address 10.50.10.128 10.50.10.254
SWC1(config)#ip dhcp excluded-address 10.50.11.128 10.50.11.254
SWC1(config)#ip dhcp excluded-address 10.50.12.128 10.50.12.254
SWC1(config)#ip dhcp excluded-address 10.50.13.128 10.50.13.254
SWC1(config)#ip dhcp excluded-address 10.50.14.128 10.50.14.254
SWC1(config)#ip dhcp excluded-address 10.50.15.128 10.50.15.254
SWC1(config)#ip dhcp excluded-address 10.50.16.128 10.50.16.254
SWC1(config)#ip dhcp excluded-address 10.50.17.128 10.50.17.254
SWC1(config)#ip dhcp excluded-address 10.50.18.128 10.50.18.254
SWC1(config)#ip dhcp excluded-address 10.50.20.128 10.50.20.254
SWC1(config)#ip dhcp excluded-address 10.50.21.128 10.50.21.254
SWC1(config)#ip dhcp excluded-address 10.50.22.128 10.50.22.254
SWC1(config)#ip dhcp excluded-address 10.50.23.128 10.50.23.254
SWC1(config)#ip dhcp excluded-address 10.50.24.128 10.50.24.254
SWC1(config)#ip dhcp excluded-address 10.50.25.128 10.50.25.254
SWC1(config)#ip dhcp excluded-address 10.50.26.128 10.50.26.254
SWC1(config)#ip dhcp excluded-address 10.50.27.128 10.50.27.254
SWC1(config)#ip dhcp excluded-address 10.50.28.128 10.50.28.254
SWC1(config)#ip dhcp excluded-address 10.50.29.128 10.50.29.254
SWC1(config)#ip dhcp excluded-address 10.50.30.128 10.50.30.254
SWC1(config)#ip dhcp excluded-address 10.50.31.128 10.50.31.254
SWC1(config)#ip dhcp excluded-address 10.50.32.128 10.50.32.254
SWC1(config)#ip dhcp excluded-address 10.50.33.128 10.50.33.254
SWC1(config)#ip dhcp excluded-address 10.50.36.128 10.50.36.254
```

FIGURE IV.23 – Exclusion des adresses DHCP sur SWC1.

- **Sur le SWC2**

```
Enter configuration commands, one per line.  End with CNTL/Z.
SWC2(config)#ip dhcp excluded-address 10.50.10.1 10.50.10.127
SWC2(config)#ip dhcp excluded-address 10.50.11.1 10.50.11.127
SWC2(config)#ip dhcp excluded-address 10.50.12.1 10.50.12.127
SWC2(config)#ip dhcp excluded-address 10.50.13.1 10.50.13.127
SWC2(config)#ip dhcp excluded-address 10.50.14.1 10.50.14.127
SWC2(config)#ip dhcp excluded-address 10.50.15.1 10.50.15.127
SWC2(config)#ip dhcp excluded-address 10.50.16.1 10.50.16.127
SWC2(config)#ip dhcp excluded-address 10.50.17.1 10.50.17.127
SWC2(config)#ip dhcp excluded-address 10.50.18.1 10.50.18.127
SWC2(config)#ip dhcp excluded-address 10.50.20.1 10.50.20.127
SWC2(config)#ip dhcp excluded-address 10.50.21.1 10.50.21.127
SWC2(config)#ip dhcp excluded-address 10.50.22.1 10.50.22.127
SWC2(config)#ip dhcp excluded-address 10.50.23.1 10.50.23.127
SWC2(config)#ip dhcp excluded-address 10.50.24.1 10.50.24.127
SWC2(config)#ip dhcp excluded-address 10.50.25.1 10.50.26.127
SWC2(config)#ip dhcp excluded-address 10.50.26.1 10.50.26.127
SWC2(config)#ip dhcp excluded-address 10.50.27.1 10.50.27.127
SWC2(config)#ip dhcp excluded-address 10.50.28.1 10.50.28.127
SWC2(config)#ip dhcp excluded-address 10.50.29.1 10.50.29.127
SWC2(config)#ip dhcp excluded-address 10.50.30.1 10.50.30.127
SWC2(config)#ip dhcp excluded-address 10.50.31.1 10.50.31.127
SWC2(config)#ip dhcp excluded-address 10.50.32.1 10.50.32.127
SWC2(config)#ip dhcp excluded-address 10.50.33.1 10.50.33.127
SWC2(config)#ip dhcp excluded-address 10.50.36.1 10.50.36.127
```

FIGURE IV.24 – Exclusion des adresses DHCP de 1 à 127 sur SWC2.

IV.11.1 Vérification des adresses exclues

Avec la commande **« show running-config ».**

```
ip dhcp excluded-address 10.50.10.128 10.50.10.254
ip dhcp excluded-address 10.50.11.128 10.50.11.254
ip dhcp excluded-address 10.50.12.128 10.50.12.254
ip dhcp excluded-address 10.50.13.128 10.50.13.254
ip dhcp excluded-address 10.50.14.128 10.50.14.254
ip dhcp excluded-address 10.50.15.128 10.50.15.254
ip dhcp excluded-address 10.50.16.128 10.50.16.254
ip dhcp excluded-address 10.50.17.128 10.50.17.254
ip dhcp excluded-address 10.50.18.128 10.50.18.254
ip dhcp excluded-address 10.50.20.128 10.50.20.254
ip dhcp excluded-address 10.50.21.128 10.50.21.254
ip dhcp excluded-address 10.50.22.128 10.50.22.254
ip dhcp excluded-address 10.50.23.128 10.50.23.254
ip dhcp excluded-address 10.50.24.128 10.50.24.254
ip dhcp excluded-address 10.50.26.128 10.50.26.254
ip dhcp excluded-address 10.50.27.128 10.50.27.254
ip dhcp excluded-address 10.50.28.128 10.50.28.254
ip dhcp excluded-address 10.50.29.128 10.50.29.254
ip dhcp excluded-address 10.50.30.128 10.50.30.254
ip dhcp excluded-address 10.50.31.128 10.50.31.254
ip dhcp excluded-address 10.50.32.128 10.50.32.254
ip dhcp excluded-address 10.50.33.128 10.50.33.254
ip dhcp excluded-address 10.50.36.128 10.50.36.254
ip dhcp excluded-address 10.50.25.128 10.50.25.254
```

FIGURE IV.25 – Vérification des adresses exclues sur SWC1

```
ip dhcp excluded-address 10.50.11.1 10.50.11.127
ip dhcp excluded-address 10.50.12.1 10.50.12.127
ip dhcp excluded-address 10.50.13.1 10.50.13.127
ip dhcp excluded-address 10.50.14.1 10.50.14.127
ip dhcp excluded-address 10.50.15.1 10.50.15.127
ip dhcp excluded-address 10.50.16.1 10.50.16.127
ip dhcp excluded-address 10.50.17.1 10.50.17.127
ip dhcp excluded-address 10.50.18.1 10.50.18.127
ip dhcp excluded-address 10.50.20.1 10.50.20.127
ip dhcp excluded-address 10.50.21.1 10.50.21.127
ip dhcp excluded-address 10.50.22.1 10.50.22.127
ip dhcp excluded-address 10.50.23.1 10.50.23.127
ip dhcp excluded-address 10.50.24.1 10.50.24.127
ip dhcp excluded-address 10.50.26.1 10.50.26.127
ip dhcp excluded-address 10.50.27.1 10.50.27.127
ip dhcp excluded-address 10.50.28.1 10.50.28.127
ip dhcp excluded-address 10.50.29.1 10.50.29.127
ip dhcp excluded-address 10.50.30.1 10.50.30.127
ip dhcp excluded-address 10.50.31.1 10.50.31.127
ip dhcp excluded-address 10.50.32.1 10.50.32.127
ip dhcp excluded-address 10.50.33.1 10.50.33.127
ip dhcp excluded-address 10.50.36.1 10.50.36.127
ip dhcp excluded-address 10.50.10.1 10.50.10.127
ip dhcp excluded-address 10.50.10.252 10.50.10.254
ip dhcp excluded-address 10.50.11.252 10.50.11.254
ip dhcp excluded-address 10.50.12.252 10.50.12.254
ip dhcp excluded-address 10.50.13.252 10.50.13.254
ip dhcp excluded-address 10.50.14.252 10.50.14.254
ip dhcp excluded-address 10.50.15.252 10.50.15.254
ip dhcp excluded-address 10.50.16.252 10.50.16.254
ip dhcp excluded-address 10.50.17.252 10.50.17.254
ip dhcp excluded-address 10.50.18.252 10.50.18.254
ip dhcp excluded-address 10.50.20.252 10.50.20.254
```

```
ip dhcp excluded-address 10.50.20.252 10.50.20.254
ip dhcp excluded-address 10.50.21.252 10.50.21.254
ip dhcp excluded-address 10.50.22.252 10.50.22.254
ip dhcp excluded-address 10.50.23.252 10.50.23.254
ip dhcp excluded-address 10.50.24.252 10.50.24.254
ip dhcp excluded-address 10.50.26.252 10.50.26.254
ip dhcp excluded-address 10.50.27.252 10.50.27.254
ip dhcp excluded-address 10.50.28.252 10.50.28.254
ip dhcp excluded-address 10.50.29.252 10.50.29.254
ip dhcp excluded-address 10.50.30.252 10.50.30.254
ip dhcp excluded-address 10.50.31.252 10.50.31.254
ip dhcp excluded-address 10.50.32.252 10.50.32.254
ip dhcp excluded-address 10.50.33.252 10.50.33.254
ip dhcp excluded-address 10.50.36.252 10.50.36.254
ip dhcp excluded-address 10.50.25.1 10.50.26.127
```

FIGURE IV.26 – Vérification des adresses exclues sur SWC2

IV.11.2 Création des pools d'adresse DHCP

Maintenant que nous avons exclu les adresses inutiles, nous allons procéder à la création des pools pour chaque VLAN sur les switches SWC1 et SWC2, à l'exception des VLANs 25 (management), 18 (Server) et 32 (caméras). La passerelle par défaut de chaque sous-réseau sera ensuite définie

```
Enter configuration commands, one per line.  End with CNTL/Z.
SWC1(config)#ip dhcp pool vlan10
SWC1(dhcp-config)#network 10.50.10.0 255.255.255.0
SWC1(dhcp-config)#default-router 10.50.10.254
SWC1(dhcp-config)#exit
```

FIGURE IV.27 – Création d'un pool pour le Vlan 10 sur le SWC1

IV.11.3 Vérification de la création des pools DHCP

Avec la commande **« show running-config »**

```
!
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
 default-router 10.50.11.254
ip dhcp pool vlan12
 network 10.50.12.0 255.255.255.0
 default-router 10.50.12.254
ip dhcp pool vlan13
 network 10.50.13.0 255.255.255.0
 default-router 10.50.13.254
ip dhcp pool vlan14
 network 10.50.14.0 255.255.255.0
 default-router 10.50.14.254
ip dhcp pool vlan15
 network 10.50.15.0 255.255.255.0
 default-router 10.50.15.254
ip dhcp pool vlan16
 network 10.50.16.0 255.255.255.0
 default-router 10.50.16.254
ip dhcp pool vlan17
 network 10.50.17.0 255.255.255.0
 default-router 10.50.17.254
ip dhcp pool vlan20
 network 10.50.20.0 255.255.255.0
 default-router 10.50.20.254
ip dhcp pool vlan21
 network 10.50.21.0 255.255.255.0
 default-router 10.50.21.254
```

```
ip dhcp pool vlan22
 network 10.50.22.0 255.255.255.0
 default-router 10.50.22.254
ip dhcp pool vlan23
 network 10.50.23.0 255.255.255.0
 default-router 10.50.23.254
ip dhcp pool vlan24
 network 10.50.24.0 255.255.255.0
 default-router 10.50.24.254
ip dhcp pool vlan26
 network 10.50.26.0 255.255.255.0
 default-router 10.50.26.254
ip dhcp pool vlan27
 network 10.50.27.0 255.255.255.0
 default-router 10.50.27.254
ip dhcp pool vlan28
 network 10.50.28.0 255.255.255.0
 default-router 10.50.28.254
ip dhcp pool vlan29
 network 10.50.29.0 255.255.255.0
 default-router 10.50.29.254
ip dhcp pool vlan30
 network 10.50.30.0 255.255.255.0
 default-router 10.50.30.254
ip dhcp pool vlan31
 network 10.50.31.0 255.255.255.0
 default-router 10.50.31.254
ip dhcp pool vlan33
 network 10.50.33.0 255.255.255.0
 default-router 10.50.33.254
ip dhcp pool vlan36
 network 10.50.36.0 255.255.255.0
 default-router 10.50.36.254
!
```

FIGURE IV.28 – Vérification de la création des pools

Maintenant, nous allons essayer d'attribuer des adresses IP aux PC de manière dynamique et vérifier si le DHCP fonctionne.

- **Sur le PC**

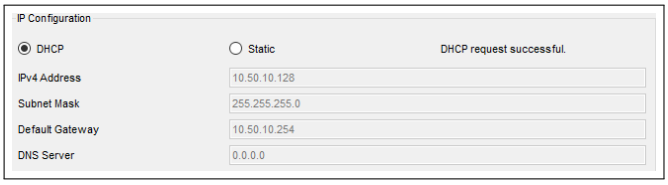


FIGURE IV.29 – Attribution d'adresse ip dynamiquement

IV.12 Configuration du routage inter-réseaux

Afin de permettre la communication entre les réseaux internes, il est nécessaire d'activer le routage en utilisant la commande **« ip routing »** sur les deux switches de niveau 3 : SWC1 et SWC2.

```
SWC2>enable
SWC2#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWC2(config)#ip routing
```

```
SWC1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWC1(config)#ip routing
SWC1(config)#
```

FIGURE IV.30 – Configuration du routage inter-réseaux sur SWC1 et SWC2

IV.13 Configuration du STP

Le Spanning Tree Protocol (STP) est essentiel pour maintenir la stabilité des réseaux en évitant les boucles de commutation. Il établit une topologie logique sans boucle, garantissant une connectivité fiable entre la couche core et la couche d'accès.

Nous allons configurer la moitié des VLANs (10-22) en Root Bridge sur SWC1 et l'autre moitié des VLANs (23-36) en Root Bridge sur SWC2

```
SWC1>enable
SWC1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWC1(config)#spanning-tree mode pvst
SWC1(config)#spanning-tree vlan 10-22 root primary
SWC1(config)#spanning-tree vlan 23-36 root secondary
```

FIGURE IV.31 – Configuration du STP sur SWC1

```
SWC2(config)#spanning-tree vlan 10-22 root secondary
SWC2(config)#spanning-tree vlan 23-36 root primary
SWC2(config)#
```

FIGURE IV.32 – Configuration du STP sur SWC2

IV.13.1 Vérification du STP

On va vérifier si le STP est bien configuré à l'aide de la commande **« show running-config ».**

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

FIGURE IV.33 – Vérification du STP sur le SWC1

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

FIGURE IV.34 – Vérification du STP sur le SWC2

IV.14 Configuration de l'HSRP

Nous allons configurer le protocole HSRP sur les deux switchs. Sur le switch SWC1, nous attribuerons une priorité de 200 à la moitié des VLANs pour qu'ils soient actifs, et une priorité de 150 à l'autre moitié pour qu'ils soient en mode standby. Sur le switch SWC2, nous appliquerons l'inverse. la répartition des VLANs sera la même que celle utilisée lors de la configuration du protocole STP. (La première moitié comprend les VLANs 10 à 22, et la deuxième moitié comprend les VLANs 23 à 36)

- **Sur le SWC1**

```
SWC1(config)#interface vlan 10
SWC1(config-if)#standby 10 ip 10.50.10.254
SWC1(config-if)#standby 10 priority 200
SWC1(config-if)#standby 10 preempt
SWC1(config-if)#exit
```

FIGURE IV.35 – Configuration du HSRP pour La première moitié sur SWC1

```
SWC1(config)#interface vlan 23
SWC1(config-if)#standby 23 ip 10.50.23.254
SWC1(config-if)#standby 23 priority 150
SWC1(config-if)#standby 23 preempt
SWC1(config-if)#exit
```

FIGURE IV.36 – Configuration du HSRP pour la deuxième moitié sur SWC1

- **Sur le SWC2**

```
SWC2(config)#interface vlan 10
SWC2(config-if)# standby 10 ip 10.50.10.254
SWC2(config-if)# standby 10 priority 150
SWC2(config-if)# standby 10 preempt
SWC2(config-if)#exit
```

FIGURE IV.37 – Configuration du HSRP pour La première moitié sur SWC2

```
SWC2(config)#interface vlan 23
SWC2(config-if)# standby 23 ip 10.50.23.254
SWC2(config-if)# standby 23 priority 200
SWC2(config-if)# standby 23 preempt
SWC2(config-if)#exit
```

FIGURE IV.38 – Configuration du HSRP pour La première moitié sur SWC2

IV.14.1 Vérification du HSRP

Avec la commande **« show standby brief ».**

- **Sur le SWC1**

```
SWC1(config)#do show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   200 P Active   local           10.50.10.253    10.50.10.254
Vl11        11   200 P Active   local           10.50.11.253    10.50.11.254
Vl12        12   200 P Active   local           10.50.12.253    10.50.12.254
Vl13        13   200 P Active   local           10.50.13.253    10.50.13.254
Vl14        14   200 P Active   local           10.50.14.253    10.50.14.254
Vl15        15   200 P Active   local           10.50.15.253    10.50.15.254
Vl16        16   200 P Active   local           10.50.16.253    10.50.16.254
Vl17        17   200 P Active   local           10.50.17.253    10.50.17.254
Vl18        18   200 P Active   local           10.50.18.253    10.50.18.254
Vl20        20   200 P Active   local           10.50.20.253    10.50.20.254
Vl21        21   200 P Active   local           10.50.21.253    10.50.21.254
Vl22        22   200 P Active   local           10.50.22.253    10.50.22.254
Vl23        23   150 P Standby  10.50.23.253    local           10.50.23.254
Vl24        24   150 P Standby  10.50.24.253    local           10.50.24.254
Vl25        25   150 P Standby  10.50.25.253    local           10.50.25.254
Vl26        26   150 P Standby  10.50.26.253    local           10.50.26.254
Vl27        27   150 P Standby  10.50.27.253    local           10.50.27.254
Vl28        28   150 P Standby  10.50.28.253    local           10.50.28.254
Vl29        29   150 P Standby  10.50.29.253    local           10.50.29.254
Vl30        30   150 P Standby  10.50.30.253    local           10.50.30.254
Vl31        31   150 P Standby  10.50.31.253    local           10.50.31.254
Vl32        32   150 P Standby  10.50.32.253    local           10.50.32.254
Vl33        33   150 P Standby  10.50.33.253    local           10.50.33.254
Vl36        36   150 P Active   local           unknown         10.50.36.254
```

FIGURE IV.39 – Vérification du HSRP sur SWC1

- **Sur le SWC2**

```
SWC2(config)#do show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   150 P Standby  10.50.10.252    local           10.50.10.254
Vl11        11   150 P Standby  10.50.11.252    local           10.50.11.254
Vl12        12   150 P Standby  10.50.12.252    local           10.50.12.254
Vl13        13   150 P Standby  10.50.13.252    local           10.50.13.254
Vl14        14   150 P Standby  10.50.14.252    local           10.50.14.254
Vl15        15   150 P Standby  10.50.15.252    local           10.50.15.254
Vl16        16   150 P Standby  10.50.16.252    local           10.50.16.254
Vl17        17   150 P Standby  10.50.17.252    local           10.50.17.254
Vl18        18   150 P Standby  10.50.18.252    local           10.50.18.254
Vl20        20   150 P Standby  10.50.20.252    local           10.50.20.254
Vl21        21   150 P Standby  10.50.21.252    local           10.50.21.254
Vl22        22   150 P Standby  10.50.22.252    local           10.50.22.254
Vl23        23   200 P Active   local           10.50.23.252    10.50.23.254
Vl24        24   200 P Active   local           10.50.24.252    10.50.24.254
Vl25        25   200 P Active   local           10.50.25.252    10.50.25.254
Vl26        26   200 P Active   local           10.50.26.252    10.50.26.254
Vl27        27   200 P Active   local           10.50.27.252    10.50.27.254
Vl28        28   200 P Active   local           10.50.28.252    10.50.28.254
Vl29        29   200 P Active   local           10.50.29.252    10.50.29.254
Vl30        30   200 P Active   local           10.50.30.252    10.50.30.254
Vl31        31   200 P Active   local           10.50.31.252    10.50.31.254
Vl32        32   200 P Active   local           10.50.32.252    10.50.32.254
Vl33        33   200 P Active   local           10.50.33.252    10.50.33.254
Vl36        36   200   Standby  unknown         local           10.50.36.254
```

FIGURE IV.40 – Vérification du HSRP sur SWC2.

IV.15 Sécurisation des switches

Pour protéger l'entreprise contre les risques de piratage et garantir la sécurité, il est néces- saire de suivre certaines étapes

IV.15.1 Configuration de line console

On va configurer une ligne console pour les switches de niveau 2 et de niveau 3, et définir un mot de passe comme **PS222cf3**

```
Enter configuration commands, one per line.  End with CNTL/Z.
SWA10(config)#line con 0
SWA10(config-line)#password PS222cf3
SWA10(config-line)#login
SWA10(config-line)#exit
```

FIGURE IV.41 – Configuration de ligne console.

IV.15.2 Sécurisation du mode privilégié

```
SWA10(config)#enable secret C3v1t41112
```

FIGURE IV.42 – Configuration de ligne console.

IV.15.3 Configuration de SSH

SSH est un protocole qui permet de créer une connexion sécurisée entre deux ordinateurs. Il est surtout utilisé pour se connecter à distance à un serveur, ce qui permet d'exécuter des commandes ou de transférer des fichiers en toute sécurité.

Nous allons configurer le SSH pour tous les switches, on va créer deux comptes, le premier (username "massi" et son mot de passe d'accès "mas-22") et le deuxième (username "khaled" et son mot de passe "kha-22"),

- **Sur les switches niveau 3**

```
SWC1(config)#ip domain-name CEV.SSH
SWC1(config)#crypto key generate rsa
The name for the keys will be: SWC1.CEV.SSH
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

SWC1(config)#ip ssh version 2
*Mar 1 6:55:39.132: %SSH-5-ENABLED: SSH 1.99 has been enabled
SWC1(config)#username khaled password kha-22
SWC1(config)#username massi password mas-22
SWC1(config)#line vty 0 1
SWC1(config-line)#login local
SWC1(config-line)#transport input ssh
SWC1(config-line)#exit
```

FIGURE IV.43 – Configuration de la SSH sur SWC1

- **Sur les switches niveau 2**

Pour configurer SSH sur un switch de couche 2, il faut d'abord attribuer une adresse IP à l'interface VLAN 25 (managment switch) sur et une passrelle 10.50.25.254 chaque switch, afin de permettre l'accès à distance depuis n'importe quel réseau, et non seulement depuis le réseau local. Ensuite, il faut configurer le protocole SSH

```
SWA1(config)#int vlan 25
SWA1(config-if)#ip address 10.50.25.1 255.255.255.0
SWA1(config-if)#ip default-gateway 10.50.25.254
```

FIGURE IV.44 – Attribution des adresses IP et la passerelle

IV.16 Configurations de PortFast

PortFast permet une activation rapide du port en le plaçant directement en état forwarding, sans passer par les états intermédiaires du STP (listening et learning). Cela réduit considéra- blement le temps d'attente lors du démarrage d'un appareil, ce qui est particulièrement utile pour les stations de travail ou les imprimantes qui ont besoin d'un accès réseau immédiat. Nous allons configurer la fonctionnalité PortFast sur les switchs de couche d'accès, plus précisément sur les ports fastethernet allant de 1 à 24, car ce sont ces ports qui sont généralement utilisés pour connecter les ordinateurs (PCs)

```
Enter configuration commands, one per line.  End with CNTL/Z.
SWA1(config)#int range fa0/1-24
SWA1(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
```

FIGURE IV.45 – Configuration du PortFast

IV.17 Configurations de BPDU gaurd

Le BPDU GUARD est utilisé pour sécuriser les ports des commutateurs afin d'empêcher tout intrus de connecter un commutateur externe à l'un des commutateurs de l'entreprise. Il permet également de bloquer les ports inutilisés. Ces commandes s'appliquent uniquement aux ports d'accès (au niveau de la couche d'accès) qui sont connectés à des terminaux (machines finales). Nous allons configurer le BPDU gaurd sur les switchs de couche d'accès, plus précisément sur les ports fastetherne allant de 1 à 24

```
SWA1(config-if-range)#spanning-tree bpduguard enable
```

FIGURE IV.46 – Configuration du BPDU GUARD

IV.18 Configurations des serveurs

Dans la partie consacrée aux serveurs, nous allons configurer certains serveurs tels que HTTP et FTP afin que tous les utilisateurs puissent y accéder.

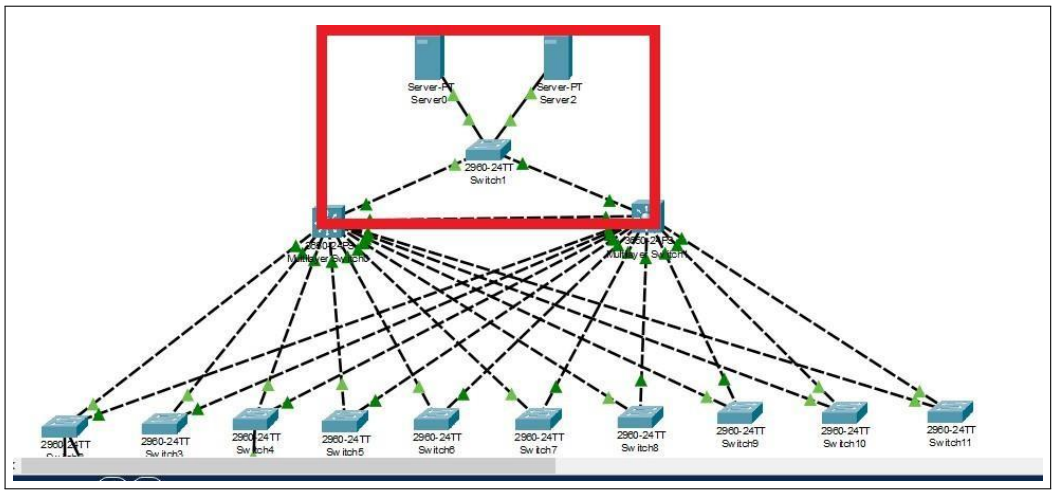


FIGURE IV.47 – Partie serveurs

IV.18.1 Configuration de la HTTP

Il faut d'abord attribuer des adresses IP statiques, par exemple : il prendra l'adresse 10.50.18.1

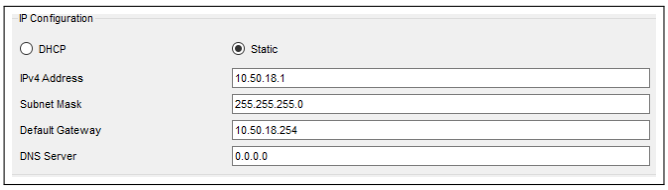


FIGURE IV.48 – Attribution d'adresse statiquement Dans la

section Service, on sélectionne HTTP, puis on active l'option "On".

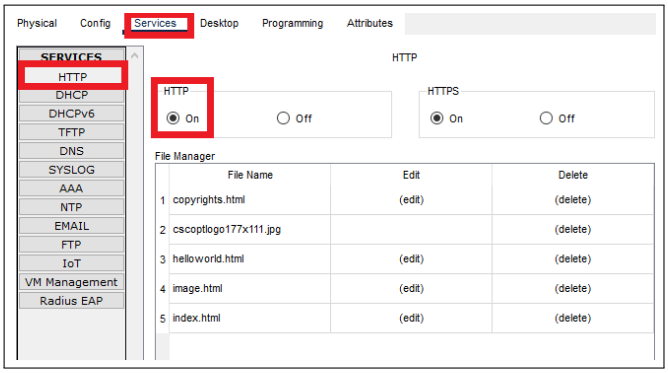


FIGURE IV.49 – Configuration de la HTTP

IV.18.2 Configuration de la FTP

On va attribuer l'adresse 10.50.18.2, puis dans l'onglet "Service", on va choisir "FTP" et créer un compte avec tous les droits (write , read , delet , rename , list), avec le nom d'utilisateur "khaled" et le mot de passe "kha-22" et après cliquer «Add »

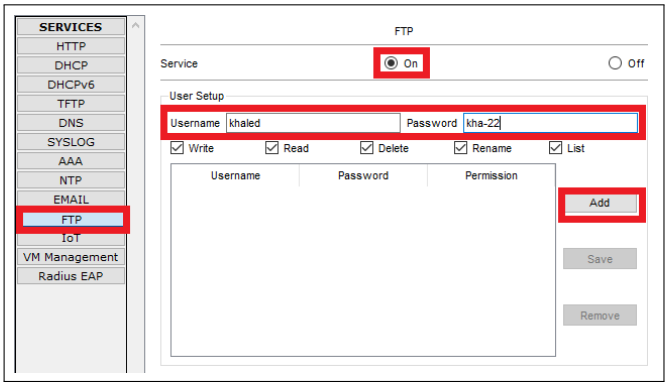


FIGURE IV.50 – Configuration de la FTP

IV.19 Test de validation

Afin de tester le bon fonctionnement de notre LAN, nous allons simuler plusieurs scénarios, chacun représentant une situation où un élément est en panne, afin d'observer comment le réseau réagit à ces pannes

IV.19.1 Test de connectivité entre VLANs

Pour tester la connectivité entre deux PC situés dans des VLANs différents, on va utiliser la commande de ping en continu depuis le PC1 (VLAN 11) vers le PC4 (VLAN 10).

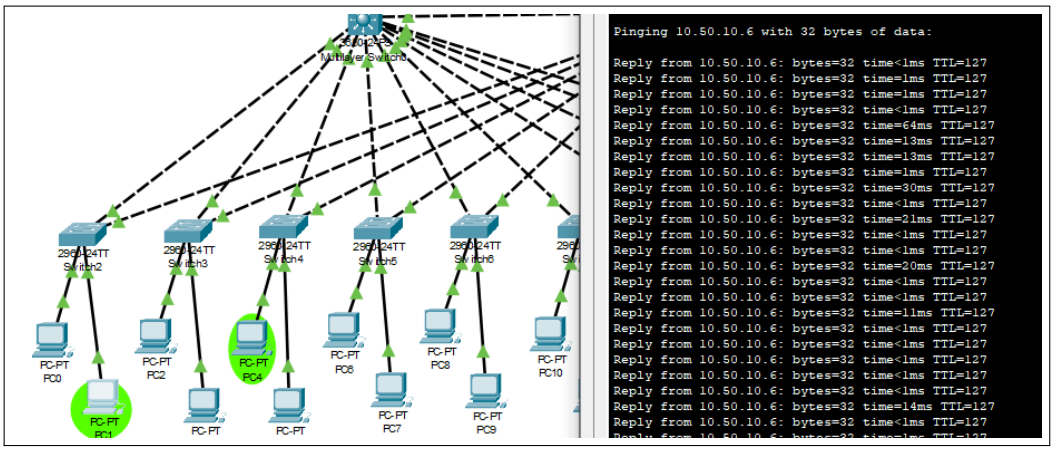


FIGURE IV.51 – Test de connectivité inter-VLAN

Comme on peut le voir, les pings ont bien réussi, ce qui signifie qu'il y a une connectivité entre les VLANs.

IV.19.2 Test de la panne d'un câble

Nous allons envoyer un ping continu depuis le PC1 vers le PC4, puis nous allons désactiver puis le réactiver le chemin principal du paquet et observer ce qui se passe.

- **Désactivation de l'interface principale**

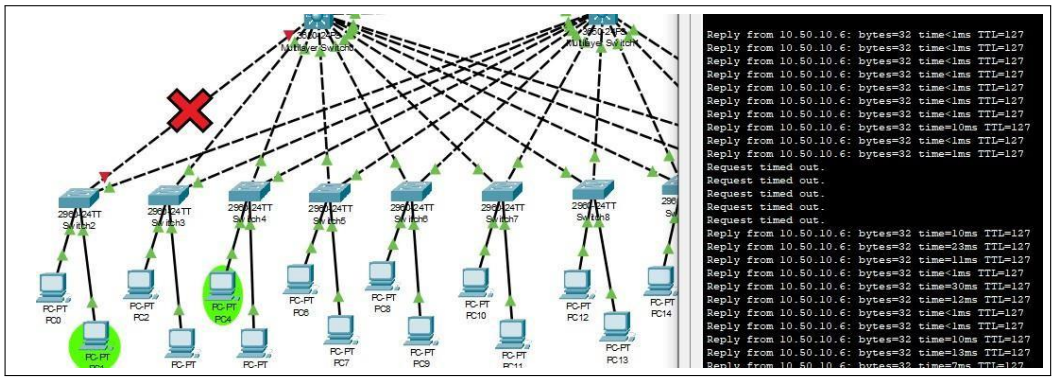


FIGURE IV.52 – Simulation d'une panne sur la route principale du VLAN 10

À la suite d'une panne sur le chemin principal du VLAN 11, le protocole STP a automatiquement pris le relais pour maintenir la continuité du service. Le trafic a été redirigé vers le commutateur non racine (SWC2), qui a temporairement assuré le rôle de passerelle pour ce VLAN , une interruption momentanée de la connectivité a été observée pendant le temps nécessaire à la reconfiguration de la topologie par le protocole STP.

- **Réactivation de l'interface principale**

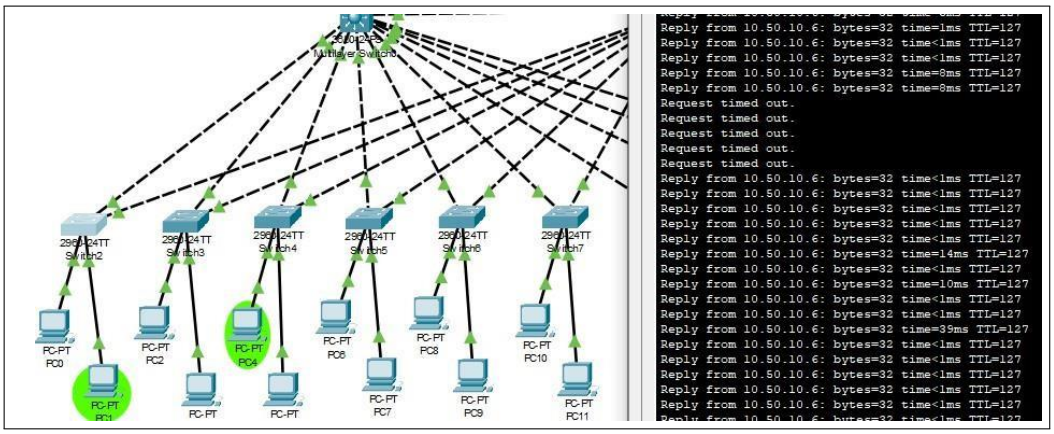


FIGURE IV.53 – Réactivation de la route principale du VLAN 11

La réactivation de l'interface principale a provoqué une brève interruption du ping, car lorsque la route principale du VLAN 11 est rétablie et remise en service, le protocole STP la détecte automatiquement et redirige le trafic vers celle-ci

IV.19.3 Test de la panne du SWC1

La simulation a été réalisée en provoquant une panne matérielle sur le switch SWC1, qui est le switch principal du VLAN 11.

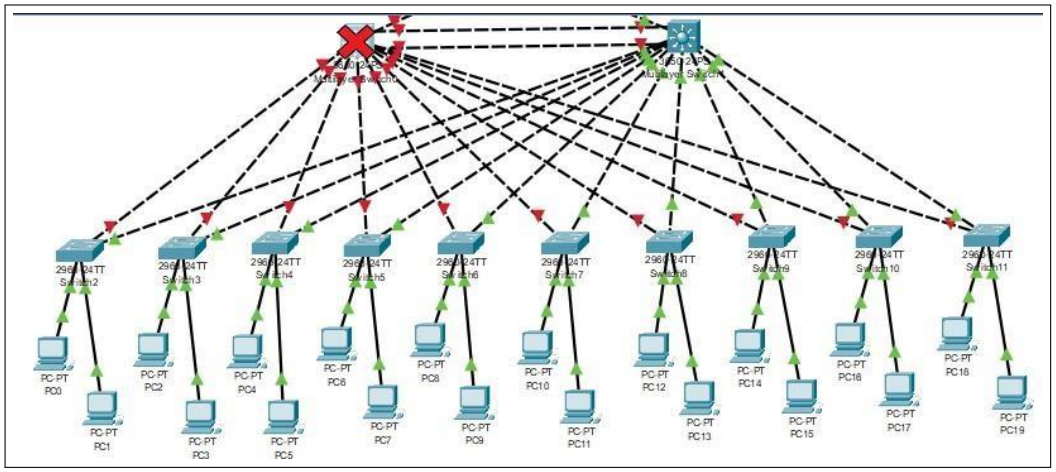


FIGURE IV.54 – La panne du SWC1

La simulation de la panne a entraîné une interruption temporaire du ping. Le switch SWC2, disposant de la seconde priorité HSRP la plus élevée, a assuré la relève en devenant le switch principal du VLAN 11. Ce basculement a occasionné la perte de 6 paquets, le temps que le switch en veille prenne le relais.

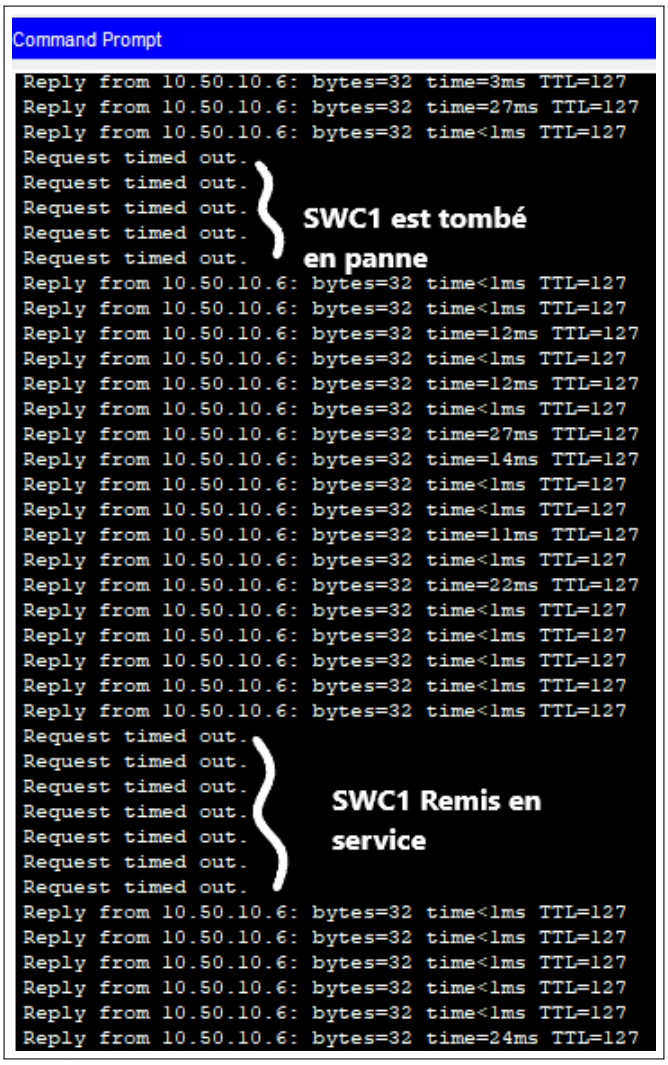


FIGURE IV.55 – Observation du trafic réseau pendant les simulations

Le test s'est déroulé avec succès. Lors de la remise en service du switch principal, une brève interruption du ping a été observée. Toutefois, le mécanisme de préemption HSRP a rapidement permis à SWC1 de reprendre son rôle de switch principal pour le VLAN 11. La communication a ensuite repris normalement, sans interruption.

IV.20 Conclusion

Ce chapitre s'est concentré sur la mise en place d'une infrastructure d'équilibrage de charge dans un réseau pour l'entreprise (Cevital). En s'appuyant sur des protocoles éprouvés tels que SSH,STP et HSRP ainsi que d'autres configurations basiques, cette méthodologie employée a permis l'équilibrage de charge et de garantir les performances, la disponibilité, la continuité des services applicatifs sur les serveurs de l'entreprise.

Conclusion Générale

L’équilibrage de charge joue un rôle essentiel dans la gestion efficace des réseaux modernes. Il permet de répartir le trafic de manière optimale entre différentes ressources, assurant ainsi de meilleures performances, une haute disponibilité des services, une utilisation équilibrée des serveurs et une résilience face aux pannes., les infrastructures réseau peuvent répondre de manière fiable et évolutive aux besoins croissants des utilisateurs et des applications.

Ce projet de fin d’étude a été consacré à la mise en place d’une infrastructure d’équilibrage de charge pour garantir la performance, la disponibilité et la continuité des services applicatifs sur les serveurs de l’entreprise, à travers des chapitres réalisés dans ce mémoire, nous avons par- couru un chemin allant des principes fondamentaux des réseaux informatiques à la réalisation d’une architecture réseau qui répond aux performances essentiels en appliquant un équilibrage de charge.

Pour bien approfondir dans notre étude, nous avons fait une étude de l’existant du l’en- treprise Cevital, nous avons posé une problématique sur le but du notre projet puis proposée des solutions afin de trouver une réponse efficace , puis nous avons fait une étude détaillée au processus de répartition de charge, non passerons par leur définition, ses avantages, son fonctionnement, ses différents types et algorithmes.

Afin de réaliser la partie pratique de notre projet, nous avons choisit d’utiliser Cisco Packet Tracer 8.2.2 comme simulateur au raison de ses divers avantages comme la simplicité de la configuration des équipements et la richesse des protocoles qui facilite la réalisation de notre topologie

Nous avons simulé une architecture réseau dans laquelle nous avons mis en place une infrastructure d’équilibrage de charge en utilisant les protocoles SSH, STP, HSRP et d’autres configurations essentielles comme les VLANs, VTP, Line console, bpdu guard et port fast. Ce processus réalisé a été efficace se qui a réparti la charge au niveau des serveurs de l’entreprise

En conclusion, ce mémoire a permis de confirmer l’importance et la nécessité du l’équilibrage de charge afin de garantir la disponibilité des services applicatifs des serveurs d’entreprise et la continuité des différentes tâches industrielles au Cevital, la conception du cette simulation et les détailles théoriques présentés, nous donne une idée sur la mise en placed’une infrastructure de répartition, et aussi comment améliorer les performances et la fluidité des réseaux informatiques dans les environnements industriels exigeants.

Annexes

Annexes : Désignation des interfaces utilisé dans la nouvelle architecture proposée

VLAN	Root	DHCP	Réseau	IP sur SWC1	IP sur SWC2	Gateway
10	SWC1	Dynamique	10.50.10.0/24	10.50.10.252	10.50.10.253	10.50.10.254
11	SWC1	Dynamique	10.50.11.0/24	10.50.11.252	10.50.11.253	10.50.11.254
12	SWC1	Dynamique	10.50.12.0/24	10.50.12.252	10.50.12.253	10.50.12.254
13	SWC1	Dynamique	10.50.13.0/24	10.50.13.252	10.50.13.253	10.50.13.254
14	SWC1	Dynamique	10.50.14.0/24	10.50.14.252	10.50.14.253	10.50.14.254
15	SWC1	Dynamique	10.50.15.0/24	10.50.15.252	10.50.15.253	10.50.15.254
16	SWC1	Dynamique	10.50.16.0/24	10.50.16.252	10.50.16.253	10.50.16.254
17	SWC1	Dynamique	10.50.17.0/24	10.50.17.252	10.50.17.253	10.50.17.254
18	SWC1	Statistique	10.50.18.0/24	10.50.18.252	10.50.18.253	10.50.18.254
20	SWC1	Dynamique	10.50.20.0/24	10.50.20.252	10.50.20.253	10.50.20.254
21	SWC1	Dynamique	10.50.21.0/24	10.50.21.252	10.50.21.253	10.50.21.254
22	SWC1	Dynamique	10.50.22.0/24	10.50.22.252	10.50.22.253	10.50.22.254
23	SWC2	Dynamique	10.50.23.0/24	10.50.23.252	10.50.23.253	10.50.23.254
24	SWC2	Dynamique	10.50.24.0/24	10.50.24.252	10.50.24.253	10.50.24.254
25	SWC2	Statistique	10.50.25.0/24	10.50.25.252	10.50.25.253	10.50.25.254
26	SWC2	Dynamique	10.50.26.0/24	10.50.26.252	10.50.26.253	10.50.26.254
27	SWC2	Dynamique	10.50.27.0/24	10.50.27.252	10.50.27.253	10.50.27.254
28	SWC2	Dynamique	10.50.28.0/24	10.50.28.252	10.50.28.253	10.50.28.254
29	SWC2	Dynamique	10.50.29.0/24	10.50.29.252	10.50.29.253	10.50.29.254
30	SWC2	Dynamique	10.50.30.0/24	10.50.30.252	10.50.30.253	10.50.30.254
31	SWC2	Dynamique	10.50.31.0/24	10.50.31.252	10.50.31.253	10.50.31.254
32	SWC2	Statistique	10.50.32.0/24	10.50.32.252	10.50.32.253	10.50.32.254
33	SWC2	Dynamique	10.50.33.0/24	10.50.33.252	10.50.33.253	10.50.33.254
36	SWC2	Dynamique	10.50.36.0/24	10.50.36.252	10.50.36.253	10.50.36.254

Équipement source	Équipement distant	Type de port	Câblage
Couche core	Couche d’accès	GigabitEthernet	Câble croisé
Couche d’accès	PC	FastEthernet	Câble droit
Switch serveur	Serveur	FastEthernet	Câble droit
SWC1	SWC2	GigabitEthernet	Câble croisé

Annexes : Désignation des interfaces utilisé dans la nouvelle architecture proposée

Équipement locale	Équipement distant	interface locale	Interface distante
SWC1	SWC2	G1/0/12-13	G1/0/12-13
SWC1	SWA (1-10)	G1/0/2-11	G0/1
SWC2	SWA (1-10)	G1/0/2-11	G0/2
SWC1	SWS	G1/0/12	G0/1
SWC2	SWS	G1/0/12	G0/2

Bibliographie

[2] Claude Servin, Réseaux et télécoms, 2003, éditeur Dunod, P54-55

[3] Guy Pujolle, Cours réseaux et télécoms, édition Eyrolles 2004

[9] Christian Bulfone. Le protocole IP, édition 2015

[10] Postel, J. (1980). User datagram protocol (No. rfc768)

[11] Postel, J. (1981). Internet control message protocol ; rfc792. ARPANET Working Group Requests for Comments, 792.

[12] Droms, R. (1997). Dynamic host configuration protocol (No. rfc2131)

[15] Belgacem JARRAY, Réseaux informatique, éditions 2015

[16] McPherson, D., & Dykes, B. (2001). VLAN Aggregation for Efficient IP Address Allocation (No. rfc3069).

[19] memoireMise en place d'un réseau LAN/WAN redundant(Haute disponibilité) - Cas CE-VITAL -BENLALA Riane - BELHADDAD Sara

[20] : Source interne de CEVITAL.

[21] memoireMise en œuvred'une solution de haute disponibilité (HSRP) pour un réseau local : caspratiqueréseau LAN de CEVITAL agro-industrie. SendjakedineAhlame- Tissoukai Lydia

[30] Yagoubi, Bellabas. Modèle d'équilibrage de charge pour les grilles decalcul. Revue africaine de la recherche en informatique et mathématiquesappliquées (ARIMA). Vol. 7. pp. 1-19. 2007.

Webographie

Webgraphie

[1] https ://www.baiebrassage.fr/blog/definition-reseau-informatique.html consulté le 25 mars 2025

[4] http ://www.alloscholl.com/assets/docemnts/course-130/reseaux-d-entreprise-cours.pdf

[5] https ://cours-informatique-gratuit.fr/dictionnaire/modem/ consulté le 27 mars 2025

[6] https ://www.pierre-giraud.com/http-reseau-securite-cours/modele-reseau-osi-tcp-ip/ consulté le 27 mars 2025

[7] https ://pandorafms.com/blog/fr/protocoles-de-gestion-reseau/ consulté le 23 mars 2025

[8] https ://www.cloudflare.com/fr-fr/learning/network-layer/internet-protocol/ consulté le 23 mars 2025

[13] https ://www.cloudflare.com/fr-fr/learning/ddos/glossary/internet-control-message-protocol-icmp/ consulté le 24 mars 2025

[14] https ://www.geeksforgeeks.org/vlan-trunking-protocol-vtp/ consulte le 23 averil2025

[17] https ://elearning.centre-univ-mila.dz/a2025/mod/resource/view.php ?id=17555 consulte le 27 mars 2025

[18] https ://www.cevital.com/lhistoire-du-groupe/ consulte le 23 averil2025

[22] https ://www.cloudflare.com/fr-fr/learning/performance/what-is-load-balancing/ consulte le 23 averil2025

[23] https ://learn.microsoft.com/en-us/windows-server/networking/technologies/network-load- balancing consulte le 23 averil2025

[24] https ://www.techtarget.com/searchnetworking/definition/load-balancing consulte le 23 averil2025

[25] https ://fastercapital.com/fr/contenu/Equilibrage-de-charge—optimisation-des-performances- du-reseau—IPi-et-equilibrage-de-charge.htmlAvantages-de-l–quilibrage-de-charge-pour-l-optimisation- des-performances-du-r-seau consulte le 19 averil2025

[26] https ://www.syloe.com/glossaire/load-balancer/ consulte le 23 averil2025

[27] https ://www.f5.com/fr_fr/glossary/dns-load-balancing consulte le 19 averil2025

[28] https ://www.f5.com/glossary/load-balancer consulte le 19 averil2025

[29] https ://www.cdw.com/content/cdw/en/articles/networking/how-do-load-balancers-work.html consulte le 19 averil2025

[31] https ://www.ionos.fr/digitalguide/serveur/know-how/load-balancer-repartition-de-charge- sur-un-serveur/ consulte le 20 averil2025

Webgraphie

[32] https ://webhostinggeeks.com/blog/what-is-ip-hash/ consulte le 19 averil2025

[33] https ://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234- consulte le 19 averil2025hsrpguidetoc.html

[34] https ://community.fs.com/fr/article/understanding-virtual-router-redundancy-protocol-vrrp.html consulte le 19 averil2025

[35] https ://notes.networklessons.com/vrrp-load-balancing consulte le 19 averil2025

[36] Exemple de configuration de GLBP sur les commutateurs Catalyst 6500 - Cisco consulte le 19 averil2025

[37] https ://www.cloudns.net/blog/load-balancing/ consulte le 19 averil2025

Références des figures

Références des figures

[F1] https ://resource.fs.com/mall/generalImg/PADEbK0X3oYTL6xAjZccx7yzn5i.png [F2] https

://resource.fs.com/mall/generalImg/I4lAbGS8No6FHrxeQACcaW0cnPh.png [F3] https

://resource.fs.com/mall/generalImg/EQaDbtPlooyllMx7DOEcgyp6nBb.png [F4] https

://images.app.goo.gl/e4j9tDenpCcMdvi19

[F5] https ://images.app.goo.gl/u6pmfLVCHFfqMJqP9

[F6] https ://cablage-informatique.com/wp-content/uploads/2020/08/topologie-en-bus-en-reseau- ou-en-etoile-avantages-et-inconvenients.jpg

[F7] https ://images.app.goo.gl/pQHydHE55tGjWx3P6 [F8] https

://images.app.goo.gl/ScbrNHYfxhZZCRda9

[F9] https ://upload.wikimedia.org/wikipedia/commons/thumb/6/61/Cevital*l**ogo*$_2$016.*svg*/2560*px*−*Cevital**l**ogo*$_2$016.*svg.png*

[F10] https ://itandoffice.com/cdn/shop/files/66e7301f4b7e86df64d3854e$_8$00*x.png*

[F11] https ://www.cisco.com/c/dam/assets/support/product-images/series/routers-2900-series- integrated-services-routers-isr-alternate3.jpg

[F12] https ://www.cisco.com/c/dam/assets/support/product-images/series/switches-catalyst- 2960-xr-series-switches-alternate4.jpg

[F13] https ://www.avfirewalls.com/images/FortiGate/FG-90G.jpg

[F14] https ://teamsystem.dz/wp-content/uploads/2019/10/colocation-data-center.jpg

Résumé

Ce mémoire est base sur la mise en place d'une infrastructure d'équilibrage de charge pour garantir la performance, la disponibilité et la continuité des services applicatifs sur les serveurs de l'entreprise. Suite à une observation approfondie de l'ancienne architecture de Cevital, nous avons identifié certains défauts structurels. A l'aide des protocoles HSRP et STP nous avons pu résoudre ces vulnérabilités. Nous avons ainsi obtenu une architecture hiérarchique assurant une haute disponibilité en appliquant l'équilibrage de charge. Pour la réalisation du cette archi- tecture on avis utiliser Cisco Packet Tracer comme un simulateur pour appliquer les différentes configurations.

Mots clés : réseau local , HSRP , STP , équilibrage de charge , Cevital , Cisco Packet Tracer

This thesis is based on the implementation of a load balancing infrastructure to ensure the performance, availability, and continuity of application services on the company's servers. Following an in-depth analysis of Cevital's former architecture, we identified several structural weaknesses. Using the HSRP and STP protocols, we were able to address these vulnerabilities. As a result, we achieved a hierarchical architecture that ensures high availability by applying load balancing. To implement this architecture, we used Cisco Packet Tracer as a simulator to apply the various configurations.

Keywords : local network, HSRP, STP, load balancing, Cevital, Cisco Packet Tracer