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, Télécommunications 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'un réseau LAN/WAN redondant (Haute disponibilité) - Cas CEVITAL

Préparé par :

- M^lle^ BENLALA Riane.
- M^lle^ BELHADDAD Sara.

Dirigé par :

M. DIBOUNE Abdelhani.

M. ARAB Younes.

Examiné par :

M. BELLAHSENE Hocine (président).

M. KHIERDINE Abdelkrim (examinateur).

Année universitaire : **2022/2023**

Remerciements

En premier lieu et avant tout, nous remercions ALLAH Tout-puissant de nous avoir donné la force et le courage pour la réalisation de ce travail et qui nous a procuré ce succès.

Un chaleureux merci pour notre cher promoteur M. A. DIBOUNE pour avoir accepté de nous encadrer tout au long du semestre, et de travailler avec nous pour la réalisation de ce projet.

Un grand merci pour l'organisme d'accueil CEVITAL, qui nous a acceptées comme stagiaires et qui nous a donné une chance pour découvrir le domaine professionnel. Ainsi, que pour tous les travailleurs qui nous ont aidés de près ou de loin durant notre période du stage.

Nos vifs et particuliers remerciements du plus profond de nos cœurs, vont droit vers M. Y. ARAB notre encadreur de stage, d'un premier lieu pour son chaleureux accueil et son acceptation de nous encadrer même si la surcharge de son travail ne l'avait pas permise. D'un second lieu, pour son suivi, ses conseils prodigués et ses bonnes orientations qui ont été vraiment une voie éclairée durant notre projet, et qui a su nous faire profiter de sa vaste expérience.

Nos sincères gratitudes, aux membres du jury pour leur accord à faire participer de la commission d'examinateurs.

Nos sincères reconnaissances pour tous nos enseignants, et employés du département ATE à qui on doit notre avancement.

Enfin, nous tenons à exprimer nos meilleurs remerciements à nos parents, nos frères et sœurs, ainsi, que toute personne qui nous a soutenues et encouragées.

RIANE & SARA

Dédicace

Je dédie ce modeste travail à la personne qui n'a pas pu voir la fin de ce travail, et que j'aurais aimé qu'elle soit présente, qu'ALLAH l'accueille dans son vaste paradis. Ma chère sœur SARAH, ta mort inattendue et rapide laisse un grand vide parmi tous ceux qui t'ont aimée, et tu nous rappelles qu'ici-bas, notre vie est peu de chose.

A mes parents pour leur patience et bienveillance que Dieu les préserve, à ma chère sœur Wissam et mon frère Fayçal, sans oublier mon adorable petite nièce Nihad,

A mon très cher beau-frère Hamid pour tout ce qui m'a offert,

A ma précieuse binôme pour sa patience,

A tous mes amis proches, ma famille et à tous ceux qui m'ont soutenu de près ou de loin.

J'exprime mes sentiments les plus profonds et leur dédie mon humble travail.

RIANE.

Je dédie ce travail

A

Mes chers parents ;

Mes sœurs WISSAM et MASSYLIA ;

Ma chère binôme et mes amis pour tous les bons moments et délires qu'on a vécus ensemble durant ces quatre dernières années.

SARA

Table des matières

Sommaire

Sommaire

Sommaire

Sommaire

Liste des figures

Liste des figures

Liste des figures

Liste des listings

Liste des listings

Liste des tableaux

Liste des tableaux

Liste des abréviations

Liste des abréviations

LAN: Local Area Network

MAN: Metropolitan Area Network

WAN: Wide Area Network

IP: Internet Protocol

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

HTTP: Hypertext Transfer Protocol

OSI: Open Systems Interconnection

TCP/IP: Transmission Control Protocol/Internet Protocol

FTP: File Transfer Protocol

SMTP: Simple Mail Transfer Protocol

DNS: Domain Name System

ICMP: Internet Control Message Protocol

ATM: Asynchronous Transfer Mode

ARP: Address Resolution Protocol

MAC: Media Access Control

DHCP: Dynamic Host Configuration Protocol

VLAN: Virtual Local Area Network

DSI: direction du système d'information

DMZ : zone démilitarisée

VPN: Virtual Private Network

RMS: Remote Monitoring System

FHRP: First Hop Redundancy Protocol

VRRP: Virtual Router Redundancy Protocol

HSRP: Hot Standby Router Protocol

GLPB: Gateway Load Balancing Protocol

STP: Spanning-Tree Protocol

BPDU: Bridge Protocol Data Unit

VTP: Vlan trunking Protocol

PAgP: Port Aggregation Protocol

LACP: Link Aggregation Control Protocol

Liste des abréviations

RIP: Routing Information Protocol

EIGRP: Enhanced Interior Gateway Routing Protocol

DUAL: Diffusing Update Algorithm

OSPF: Open Shortest Patch First

IGRP: Interior Gateway Routing Protocol

ABR: Area Border Router

SSH: Secure Socket Shell

SVI: Switch Virtual Interface

TTL: Time To Live

WIFI: WIreless Fidelity

CSMA/CD: Carrier Sense Multiple Access with Collision Detection

FHRP: First Hop Redundancy Protocol

Introduction générale

Introduction

L'importance des réseaux informatiques dans le fonctionnement des entreprises n'est plus à démontrer. En effet, les réseaux sont devenus des outils indispensables pour la communication, la collaboration, la gestion des données, l'accès aux ressources, et bien d'autres fonctions vitales pour l'entreprise.

Cependant, la disponibilité des réseaux est souvent mise à rude épreuve par les pannes matérielles ou logicielles, les attaques informatiques, les catastrophes naturelles, et d'autres facteurs de risque. Les temps d'arrêt du réseau peuvent avoir des conséquences désastreuses sur le fonctionnement de l'entreprise, entraînant des pertes financières, des perturbations dans les activités quotidiennes, et une perte de confiance des clients.

Pour répondre à cette problématique, les réseaux redondants et hautement disponibles sont devenus une solution de plus en plus populaire pour garantir la continuité des activités de l'entreprise. Les réseaux redondants sont conçus pour offrir une disponibilité maximale en cas de panne ou de défaillance, en fournissant des liens de secours, des mécanismes de basculement automatique, et d'autres fonctionnalités de résilience.

Dans ce mémoire, nous allons présenter la mise en place d'un réseau LAN/WAN redondant (haute disponibilité) pour l'entreprise CEVITAL, en expliquant les besoins et les contraintes de l'entreprise en matière de réseau, et nous envisagerons une solution de réseau redondant qui répondra à ces besoins. Nous allons ensuite mettre en place la solution sur les équipements de réseau, en configurant les protocoles de routage dynamique, les liens de secours, et les autres fonctionnalités de redondance. Et pour finir, il sera possible d'évaluer les performances de la solution mise en place, en mesurant la disponibilité et la résilience du réseau face aux pannes et aux défaillances.

Ce mémoire vise à fournir une étude complète et pratique de la mise en place d'un réseau LAN/WAN redondant pour cette entreprise, en présentant les défis, les solutions et les résultats de l'implémentation de cette solution.

Le présent mémoire comporte trois chapitres

Le premier chapitre sera consacré à la mise en revue de quelques notions de base des réseaux informatiques, visant une meilleure compréhension du reste du mémoire.

Au cours du deuxième chapitre, nous allons présenter l'organisme d'accueil Cevital Bejaia, son historique et les nombreux départements qui font partie de son infrastructure, puis nous critiquerons le réseau de Cevital tout en exposant la problématique de notre travail et quelques éventuelles solutions. Dans la deuxième partie de ce chapitre, nous parlerons de la haute disponibilité ainsi que de quelques notions théoriques utiles pour une compréhension des éléments servant à résoudre notre problématique tels que HSRP, STP, VTP, EtherChannel.

Le troisième chapitre est divisé en deux parties, dans la première nous abordons d'une part la conception du modèle LAN dont la procédure de préparation, la schématisation, la nomination des équipements, la désignation des interfaces et les VLAN et d'autre part nous allons clôturer ce rapport par la réalisation de ce modèle type à travers le simulateur Paquet Tracer. Puis dans la deuxième partie, nous allons interconnecter ce modèle vers les autres sites distants de l'entreprise afin de configurer le réseau WAN amélioré. Nous clôturons avec des tests de validation de la configuration globale utilisée dans le souci de vérifier si vraiment les objectifsont été atteints.

A la fin, nous terminons notre travail avec une conclusion générale et quelques perspectives.

CHAPITRE I. GENERALITES SUR LES RESEAUX INFORMATIQUES

I.1 Introduction

Afin de bien mener notre travail sur l'étude et l'optimisation d'un réseau local étendu, il est primordial de bien assimiler les notions de base sur les réseaux informatiques. A travers ce chapitre nous allons exposer quelques concepts théoriques sur les réseaux informatiques afin de mieux comprendre leur fonctionnement. De ce fait, toutes les notions nécessaires seront présentées.

I.2 Définition d'un réseau informatique

Un réseau informatique est un ensemble d'ordinateurs et de périphériques connectés les uns aux autres afin de permettre le partage de ressources et de données. Il peut être utilisé pour communiquer, transférer des fichiers, partager des imprimantes et des scanners, accéder à Internet et à d'autres réseaux.

La mise en place d'un réseau nécessite une certaine expertise technique, notamment en ce qui concerne la sécurité, la configuration des paramètres réseau et la résolution des problèmes. Il existe également des normes et des protocoles de communication standardisés qui facilitent l'interopérabilité des dispositifs sur un réseau [1].

I.3 Les composants d'un réseau informatique

Un réseau informatique est composé de plusieurs éléments physiques et logiques qui permettent aux périphériques de communiquer et de partager des ressources. Voici les principaux composants d'un réseau informatique :

- **Les périphériques :** ce sont les appareils connectés au réseau, tels que les ordinateurs, les imprimantes, les scanners, les serveurs, les téléphones IP, les points d'accès sans fil, les caméras de surveillance, etc. [2].

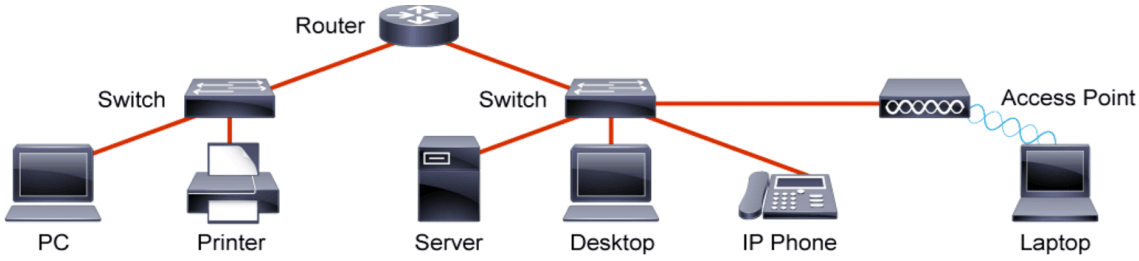


Figure 1: Les périphériques d'un réseau [F1].

- **Les médias de transmissions :** ce sont les supports physiques qui permettent la transmission de données entre les périphériques. Les médias de transmission courants sont les câbles en cuivre, les fibres optiques, les ondes radio [3].

  a) Les câbles en cuivre : le câble de cuivre est un élément indispensable à toute installation électrique. Les propriétés du cuivre en font un matériau exceptionnel dans le transport d'énergie et ses particularités sont exploitées dans de nombreux

domaines [4].

b) Les câbles coaxiaux : Le câble coaxial est un câble à deux conducteurs de pôles opposés séparés par un isolant. Il est utilisé pour la transmission de signaux numériques ou analogiques par fréquences hautes ou basses [5].

c) Câble à paires torsadées : Un câble à paire torsadée est un type de câble fabriqué en assemblant deux fils isolés séparés dans un motif torsadé et en les faisant passer parallèlement l'un à l'autre. Ce type de câble est largement utilisé dans différents types d'infrastructures de données et de voix [6].

d) La fibre optique : La fibre optique est un câble permettant de propager des ondes lumineuses entre deux lieux. La lumière est conduite sans perte au cœur du câble, et elle suit les éventuelles courbures de son support. Elle est généralement utilisée en informatique, pour la transmission de données à très haut débit et sur de grandes distances [7].

e) Les ondes radio : Une onde radio est une forme d'onde électromagnétique qui se propage dans l'espace, transportant de l'énergie à travers le champ électrique et le champ magnétique, qui ont des fréquences allant de quelques kilohertz à plusieurs gigahertz, et sont utilisées pour la transmission d'informations, notamment pour la radio diffusion, la télévision, la communication sans fil [8].

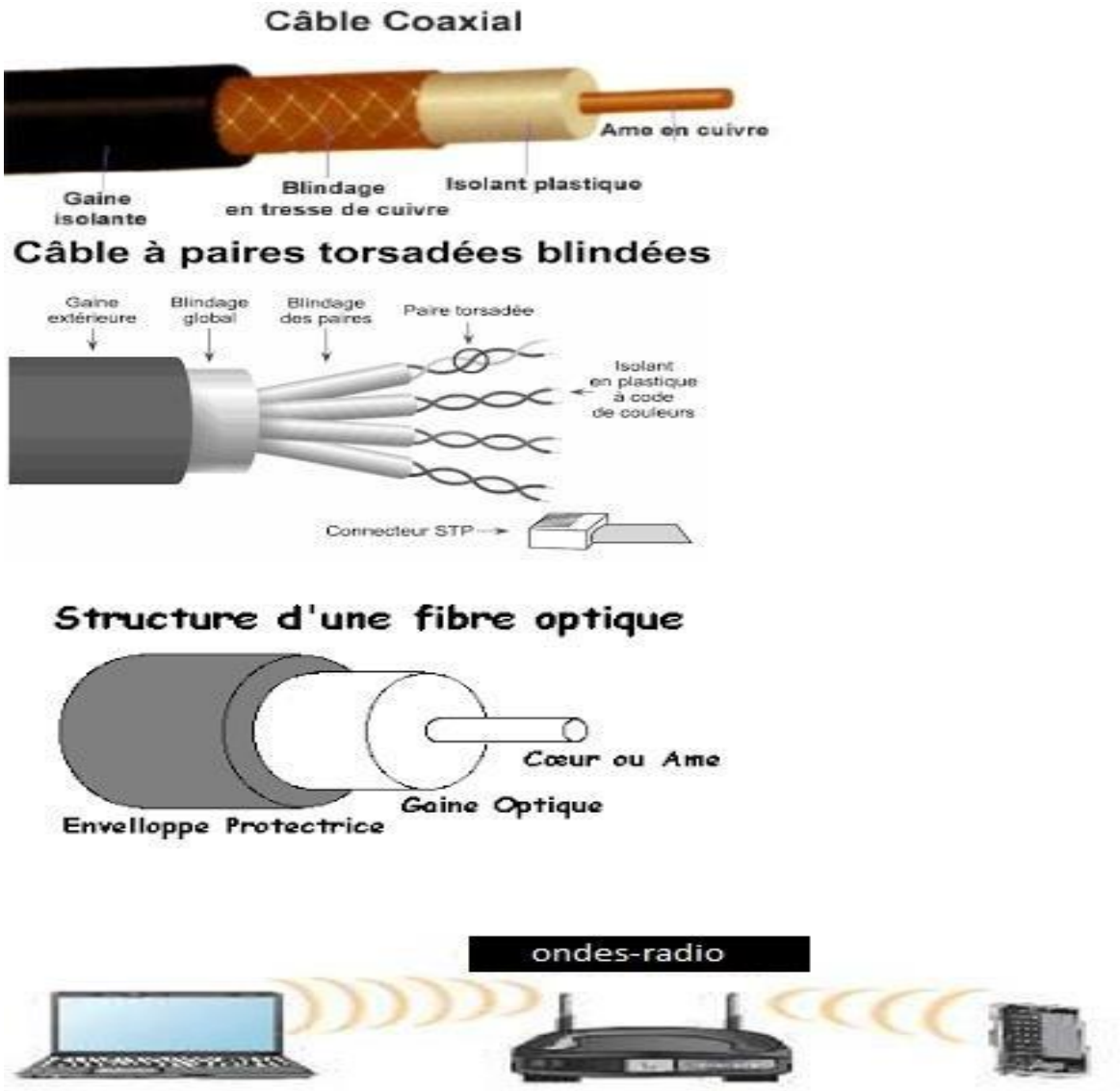


Figure 2: Les médias de transmission [F2].

- **Équipements réseau :** les équipements réseau sont des dispositifs matériels et logiciels qui acheminent et gèrent le trafic réseau. Les équipements réseau courants incluent les commutateurs, les routeurs, les pare-feu, les concentrateurs, les points d'accès sans fil, etc.

1. **Les routeurs :** ce sont des dispositifs de niveau 3 qui permettent de connecter plusieurs réseaux entre eux et d'acheminer les données entre ces réseaux. Ils sont souvent utilisés pouracheminer les paquets en fonction de l'adresse IP de destination. Les routeurs sont utilisés pour interconnecter les réseaux locaux (LAN) et les réseaux étendus (WAN)[9].

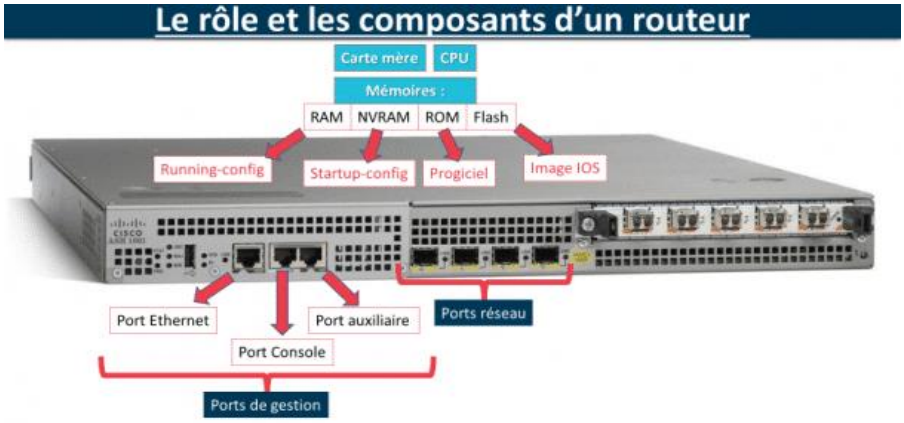


Figure 3: Le routeur [F3].

2. **Les commutateurs (Switch) :** ce sont des dispositifs qui permettent de connecter plusieurs périphériques dans un même réseau local (LAN) et de faciliter la communication entre eux. Ils permettent de transférer les trames de données d'un port à un autre port en fonction de l'adresse MAC de destination [10].

Figure 4: Le commutateur [F4].

3. **Le concentrateur (Hub) :** est un dispositif réseau qui permet de connecter plusieurs périphériques ensemble en un seul point de connexion. Il agit comme un répartiteur de signal, en prenant un seul signal entrant et en le distribuant à plusieurs périphériques connectés. Les concentrateurs étaient couramment utilisés pour connecter des ordinateurs entre eux dans les réseaux locaux (LAN), mais ils ont été largement remplacés par des commutateurs (switches) plus performants et plus efficaces [11].

Figure 5:Le concentrateur [5].

4. **Les pare-feu :** ce sont des dispositifs qui permettent de protéger les réseaux contre les attaques et les intrusions en filtrant le trafic réseau entrant et sortant [12].

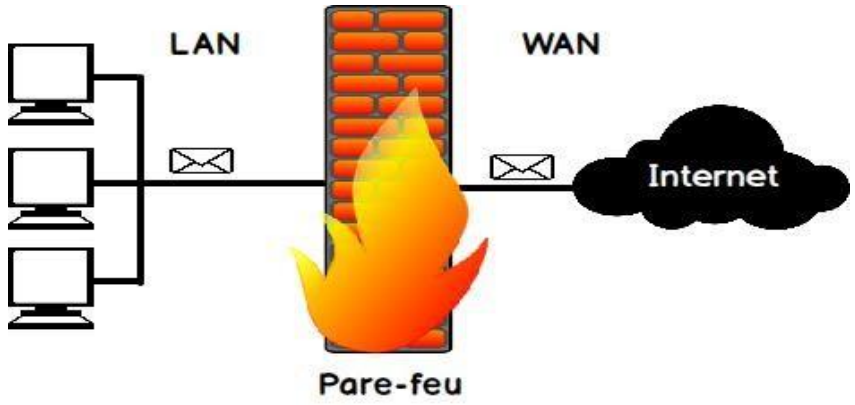


Figure 6: Le pare-feu [F6].

5. **Les points d'accès sans-fil :** ce sont des dispositifs qui permettent de connecter des périphériques à un réseau sans fil. Les points d'accès sans fil peuvent être connectés à des commutateurs ou à des routeurs pour fournir une connectivité sans fil aux périphériques [13].

Figure 7 : Point d'accès [F7].

- **Les protocoles :** ce sont des règles et des normes utilisées pour faciliter la communication entre les périphériques d'un réseau. Les protocoles les plus courants sont le protocole IP, le protocole TCP, le protocole UDP et le protocole HTTP [14].

- **L'adressage :** ensemble des techniques et méthodes donnant un identifiant unique aux périphériques d'un réseau. Il permet aux périphériques de communiquer entre eux et de transférer des données de manière efficace et fiable.

- **Les logiciels :** ce sont les programmes qui permettent aux périphériques de communiquer entre eux et de partager des ressources. Les logiciels les plus courants pour les réseaux sont les systèmes d'exploitation, les applications réseau et les services réseau.

- **Les administrateurs réseau :** ce sont les personnes qui sont responsables de la conception, de la mise en œuvre, de la gestion et de la maintenance des réseaux informatiques. Les administrateurs réseau surveillent les performances du réseau, résolvent les problèmes, mettent à jour les logiciels et les équipements, et assurent la

sécurité et la disponibilité du réseau.

I.4 Classification des réseaux informatiques

Les réseaux informatiques peuvent être classés en fonction de leur taille, de leur portée géographique et de leur architecture [15].

I.4.1 Classification selon leur taille

- **LAN (Local Area Network) :** un réseau local est un réseau informatique qui relie des ordinateurs et des périphériques dans une zone géographique limitée, comme un bureau, une maison ou un campus universitaire.
- **MAN (Metropolitan Area Network) :** c'est un ensemble de réseaux de connexion à haut débit qui interconnectent plusieurs réseaux locaux en un seul réseau de grande taille avec un pont commun. Ce pont est appelé "backbone lines" qui est généralement établi par fibre optique pour augmenter la vitesse de transfert des données.
- **WAN (Wide Area Network) :** c'est un réseau étendu qui s'étend sur de vastes zones géographiques et relie plusieurs réseaux plus petits comme LAN et MAN.

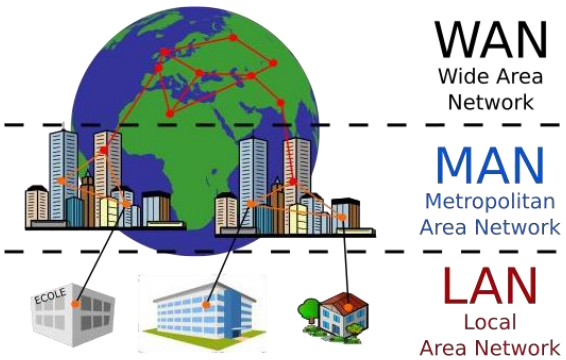


Figure 8:Type de réseaux [F8].

I.4.2 Classification selon l'architecture des réseaux

On distingue généralement deux types d'architectures [16] :

- **Le réseau client/serveur**

Dans cette architecture, les ressources et les services sont fournis par un ou plusieurs serveurs à des clients. Les clients demandent des services au serveur, qui les fournit en retour. Cette architecture est souvent utilisée dans les entreprises pour gérer les données et les applications.

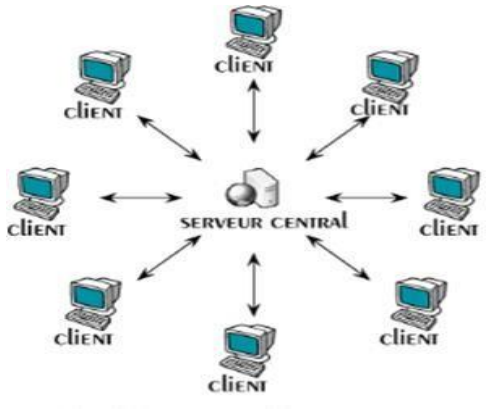


Figure 9: Architecture Client/serveur [9].

- **Le réseau post à post (Peer to Peer)**

Dans cette architecture, chaque ordinateur est à la fois client et serveur, et peut échanger desdonnées avec d'autres ordinateurs du réseau. Cette architecture est souvent utilisée pour le partage de fichiers et la collaboration.

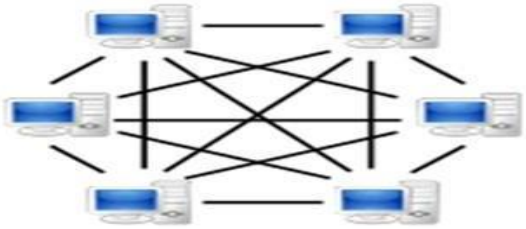


Figure 10: Les réseaux post à post [10].

I.4.3 Classification selon leur topologie

La topologie d'un réseau décrit comment les différents nœuds sont reliés entre eux (topologie physique) et comment l'information est transmise (topologie logique).

I.4.3.1 Topologie physique

C'est la manière dont les dispositifs d'un réseau informatique sont physiquement connectés les uns aux autres. Elle définit la disposition des câbles, des connexions et des équipements dans un réseau.

Il existe plusieurs types de topologies physiques de réseau, notamment :

- **Topologie en bus :** dans une topologie en bus, tous les périphériques sont connectés à une ligne unique appelée "bus". Les données circulent sur le bus et sont transmises à tous les périphériques connectés à la ligne [17].

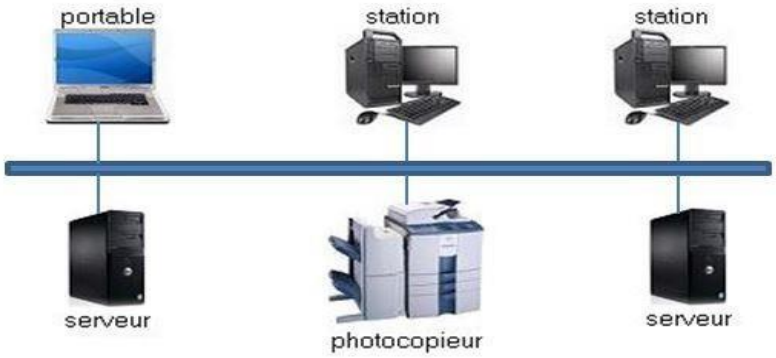


Figure 11: Topologie en bus [11].

- **Topologie en étoile :** dans une topologie en étoile, tous les périphériques sont connectés à un concentrateur central qui agit comme un point de distribution. Les données circulent entre les périphériques via le concentrateur, routeur et commutateur [18].

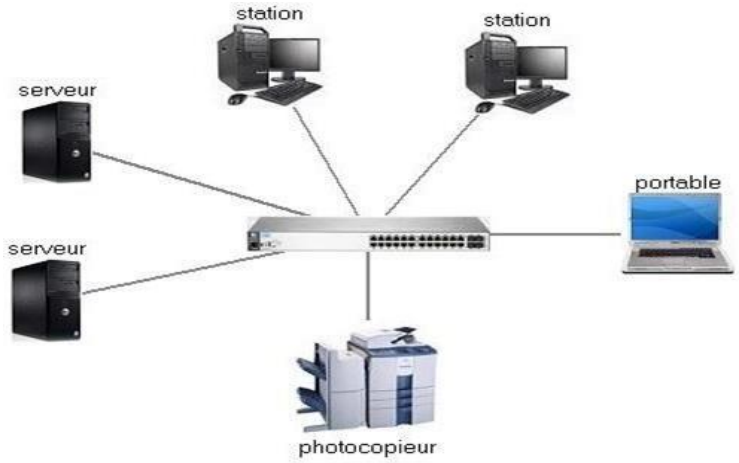


Figure 12: topologie en étoile [12].

- **Topologie en anneau :** dans une topologie en anneau, chaque périphérique est connecté à ses voisins dans un cercle ou une boucle. Les données circulent dans un seul sens autour de l'anneau, et chaque périphérique peut recevoir et envoyer des données [19].

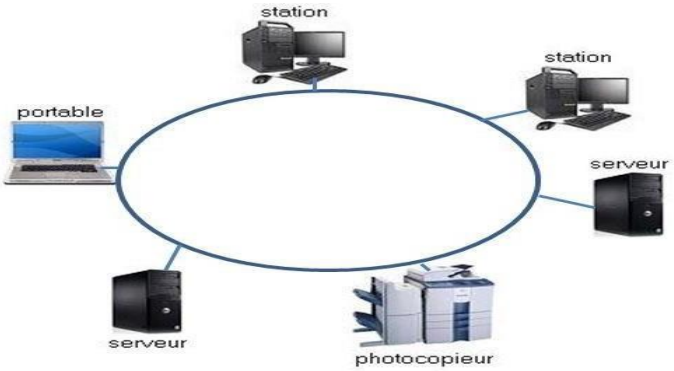


Figure 13: Topologie en anneau [13].

- **Topologie maillée :** dans une topologie en maillage, chaque périphérique est connecté directement à chaque autre périphérique du réseau. Cette topologie est très fiable et résiliente, car elle permet aux données de contourner les périphériques défaillants [20].

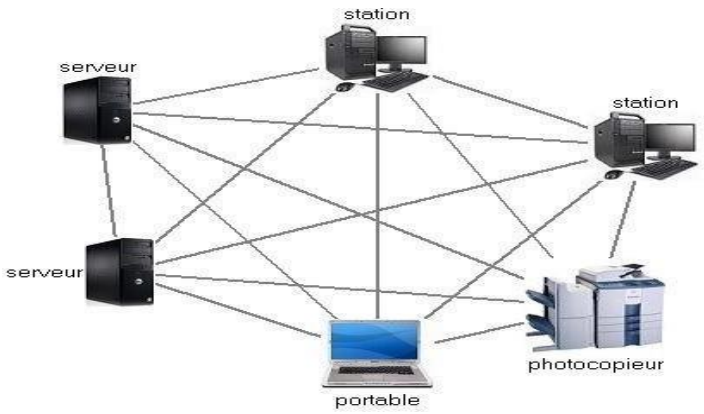


Figure 14: Topologie maillée [14].

- **Topologie en arbre :** dans une topologie en arbre, les périphériques sont organisés en plusieurs niveaux hiérarchiques. Les périphériques du niveau inférieur sont connectés à des périphériques du niveau supérieur, et ainsi de suite, jusqu'à atteindre le nœud central de l'arbre [21].

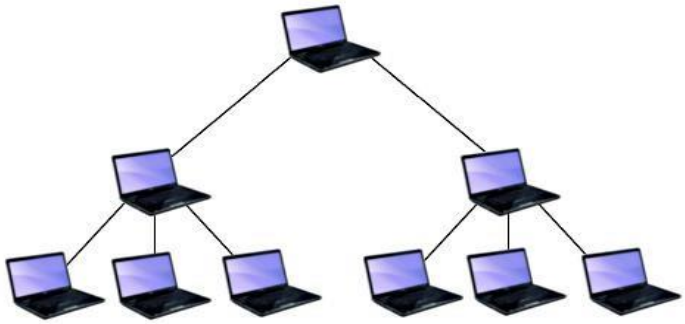


Figure 15: Topologie en arbre [15].

I.4.3.2 Topologie logique

Désigne la méthode de transfert des trames entre les nœuds du réseau. Elle est composée de connexions virtuelles entre les nœuds. Les chemins sont définis par les protocoles de la couche liaison [22].

La topologie logique d'un réseau peut avoir une influence sur la façon dont l'arbitrage d'accès est réalisé. Le choix de cette dernière dépendra de la topologie logique du réseau, de la bande passante disponible, du nombre de nœuds et de la nature de la ressource partagée.

Voici les principales topologies logiques de réseaux :

- **Ethernet :** c'est une technologie de réseau local qui utilise la topologie en bus, en anneau ou en étoile pour connecter les ordinateurs. Les ordinateurs communiquent entre eux en envoyant des paquets de données sur le réseau, qui sont acheminés d'un nœud à l'autre

jusqu'à leur destination. Ethernet utilise l'arbitrage CSMA/CD pour contrôler l'accès au réseau, ce qui signifie que les nœuds écoutent le réseau pour éviter les collisions avant de transmettre des données.

- **Token Ring :** c'est une technologie de réseau local qui utilise la topologie en anneau pour connecter les ordinateurs. Dans un réseau Token Ring, chaque nœud transmet un jeton spécial appelé jeton de transmission autour de l'anneau. Seul le nœud en possession du jeton est autorisé à transmettre des données sur le réseau, ce qui garantit une allocation équitable de la bande passante. Les nœuds peuvent également recevoir des données en écoutant l'anneau pour les paquets de données qui leur sont destinés.

I.5 Les modèles de réseau

Les modèles de réseau sont des modèles conceptuels qui définissent la structure, les fonctions et les interactions des différentes couches du réseau informatique. Les modèles de réseau les plus couramment utilisés sont le modèle OSI et TCP/IP.

I.5.1 Le modèle OSI (Open Systems Interconnection)

Développé par l'ISO (Organisation internationale de normalisation), ce modèle est basé sur une architecture en sept couches. Chaque couche est responsable de fonctions spécifiques, telles que la transmission des données, le routage et la gestion des erreurs [23].

L'ensemble du processus est ainsi découpé en sept couches hiérarchiques :

- **Couche physique :** cette couche est responsable de la transmission physique des données sur le support de communication, tels que les câbles ou les ondes radio.
- **Couche liaison de données :** cette couche organise les données en trames et gère la transmission des trames sur le support de communication. Elle détecte et corrige les erreurs de transmission.
- **Couche réseau :** cette couche gère les adresses logiques et les itinéraires pour les paquets de données entre les différents réseaux.
- **Couche transport :** cette couche fournit des services de transport de bout en bout, telle que la segmentation et la reconstitution des données, le contrôle de flux et la correction des erreurs.
- **Couche session :** cette couche gère les connexions et les sessions entre les applications distantes.
- **Couche présentation :** cette couche assure la conversion, le codage et le chiffrement des données pour la transmission sur le réseau.
- **Couche application :** cette couche fournit des services de réseau aux applications utilisateur, tels que l'envoi et la réception de courriers électroniques, la navigation sur le Web et le transfert de fichiers.

I.5.2 Le modèle TCP/IP (Transmission Control Protocol/Internet Protocol)

C'est un modèle de réseau en quatre couches qui est largement utilisé dans les réseaux informatiques modernes, en particulier sur Internet. Voici les quatre couches du modèle TCP/IP avec une brève description de leur fonction [24] :

- **Couche application :** Cette couche fournit des services de réseau aux applications utilisateur, tels que la messagerie électronique, la navigation sur le Web et le transfert de fichiers. Les protocoles courants à cette couche incluent HTTPs, FTP, SMTP et DNS.

- **Couche transport :** Cette couche fournit des services de transport de bout en bout, tels que la segmentation et la reconstitution des données, le contrôle de flux et la correction d'erreurs. Les protocoles courants à cette couche sont TCP (Transmission Control Protocol) et UDP (User Datagram Protocol).

- **Couche réseau :** Cette couche gère les adresses logiques et les itinéraires pour les paquets de données entre les différents réseaux. Les protocoles courants à cette couche incluent IP (Internet Protocol) et ICMP (Internet Control Message Protocol).

- **Couche accès au réseau :** Cette couche est responsable de la transmission physique des données sur le support de communication, tels que les câbles ou les ondes radio. Cette couche est souvent spécifique au type de réseau, tels qu'Ethernet, Wi-Fi ou ATM.

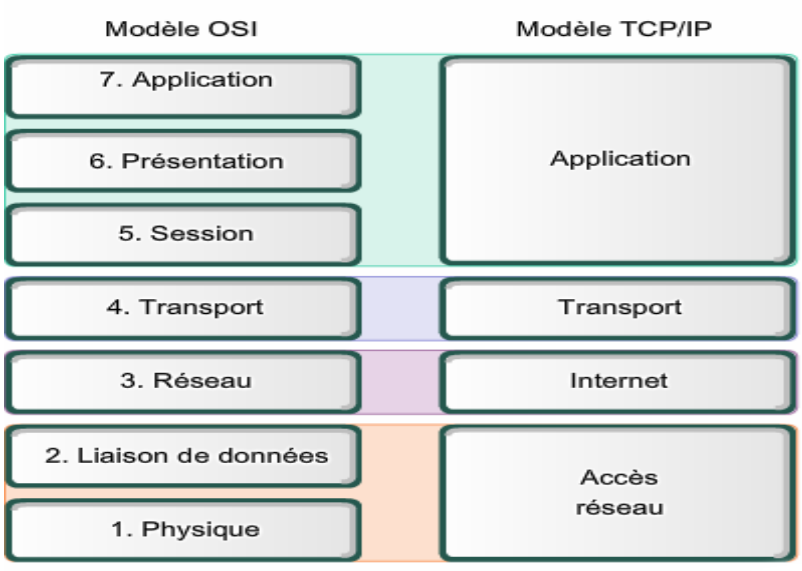


Figure 16: Le modèle OSI et TCP/IP [16].

I.6 Les protocoles réseau

Un protocole de communication c'est un ensemble de règles qui rendent les communications possibles. Les protocoles définissent une sorte de langage commun que les intervenants utilisent pour se retrouver, se connecter l'un à l'autre et y transporter des informations [25].

I.6.1 Le protocole IP (Internet Protocol)

IP est un protocole qui se charge de l'acheminement des paquets pour tous les autres protocoles de la famille TCP/IP. Il fournit un système de remise de données optimisé sans connexion. Le terme « optimisé » souligne le fait qu'il ne garantit pas que les paquets transportés parviennent à leurs destinations, ni qu'ils ne soient reçus dans leurs ordre d'envoi. Ainsi seuls, les protocoles de niveau supérieur sont responsables des données contenues dans les paquets IP et de leurs ordres de réception. Le protocole travaille en mode non-connecté, c'est-à-dire que les paquets émis sont acheminés de manière autonome, sans garantie de livraison [26].

I.6.2 Le Protocole TCP (Transmission Control Protocol)

TCP est le protocole IP de niveau supérieur, il fournit un service sécurisé de remise des paquets. TCP est un protocole fiable, orienté connexion, au-dessus d'IP qui garantit l'ordre et la remise des paquets, il vérifie l'intégrité de l'en-tête et les données qu'ils contiennent.

TCP fonctionne en établissant une connexion entre deux ordinateurs, puis en échangeant des données sous forme de segments. Chaque segment est numéroté et contient des informations de contrôle pour permettre au protocole de garantir la fiabilité de la transmission. Une fois la transmission de données terminée, la connexion est fermée [26].

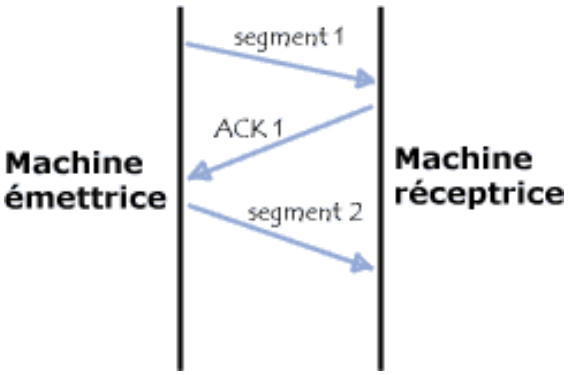


Figure 17: Protocole TCP [17].

I.6.3 Le protocole UDP (User Datagram Protocol)

C'est un protocole non-orienté connexion de la couche transport du modèle TCP/IP. Contrairement au protocole TCP, qui garantit la livraison des données dans l'ordre et sans perte, le protocole UDP est considéré comme un protocole non fiable car il ne garantit pas la livraison des données ni l'ordre dans lequel elles sont reçues.

Les datagrammes UDP sont généralement plus courts que les paquets TCP, ce qui les rend plus rapides à transmettre sur le réseau. Cependant, cela signifie également que les datagrammes UDP sont plus sujets à la fragmentation et peuvent nécessiter des transmissions plus fréquentes en cas de perte de données [27].

I.6.4 Le protocole ICMP (Internet Control Message Protocol)

C'est un protocole réseau qui permet de communiquer des messages d'erreur et de contrôle entre les équipements de réseau. Il est utilisé principalement pour signaler des erreurs dans la transmission des données, par exemple des paquets perdus ou des problèmes de routage.Le protocole ICMP est généralement utilisé en conjonction avec le protocole IP.

Les messages ICMP sont générés par les routeurs ou les hôtes lorsqu'ils rencontrent des problèmes de communication. Ces messages sont ensuite transmis à l'équipement source, qui peut prendre des mesures pour résoudre le problème. Parmi les messages ICMP les plus courants, on peut citer le Ping qui permet de vérifier la disponibilité d'un hôte sur le réseau [28].

I.6.5 Le protocole ARP (Address Resolution Protocol)

C'est un protocole de couche réseau utilisé pour résoudre les adresses MAC (Media Access Control) en adresses IP sur un réseau local.

Lorsqu'un ordinateur souhaite envoyer des données à un autre ordinateur sur le même réseau, il doit connaître l'adresse MAC de cet ordinateur. Pour obtenir cette adresse, l'ordinateur envoie une requête ARP à tous les ordinateurs du réseau en demandant « qui possède cette adresse IP ?». L'ordinateur qui possède cette adresse IP répond avec son adresse MAC et l'ordinateur qui a envoyé la requête ARP enregistre cette correspondance dans sa table ARP [29].

I.6.6 Le protocole DHCP (Dynamic Host Configuration Protocol)

C'est un protocole de réseau qui permet à un serveur DHCP de fournir automatiquement des adresses et d'autres informations de configuration réseau à des clients DHCP.

Lorsqu'un ordinateur ou un périphérique est connecté à un réseau, il envoie une demande DHCP broadcast pour demander une adresse IP auprès d'un serveur DHCP. Le serveur DHCP répond à la demande en attribuant une adresse IP disponible dans sa plage d'adresses IP, ainsi que d'autres informations de configuration telles que le masque de sous-réseau, la passerelle par défaut et les serveurs DNS. Le DHCP a pour but principal la simplification de l'administration d'un réseau [30].

I.6.7 Le protocole DNS (Domain Name System)

Le DNS est un service permettant de traduire un nom de domaine en adresse IP. Il est utilisé afin d'éviter aux utilisateurs d'entrer une adresse IP numérique manuellement en associant à cette dernière sous la forme d'une chaîne de caractères. Apprendre un nom d'un site est plus facile qu'apprendre son adresse IP [31].

I.6.8 Les virtuel LAN (VLAN)

I.6.8.1 Définition

C'est un réseau local virtuel qui permet de segmenter un réseau physique en plusieurs sous-

réseaux logiques. Les VLAN sont largement utilisés dans les réseaux informatiques d'entreprise pour améliorer la sécurité, la gestion des ressources et la performance.

Un VLAN permet de créer des groupes logiques de machines, indépendamment de leur position physique dans le réseau. Ainsi, des machines connectées à des ports différents d'un même commutateur peuvent appartenir à des VLAN différents et ne pas communiquer entre elles, même si elles sont physiquement connectées au même équipement et inversement.

En somme, les VLAN sont une technique importante pour la gestion efficace des réseaux informatiques d'entreprise, en permettant une segmentation du réseau pour améliorer la sécurité, la gestion des ressources et la performance [32].

I.6.8.2 Avantage des VLAN

Les VLANs (Virtual LAN) présentent de nombreux avantages pour la gestion d'un réseau local. Voici les principaux avantages des VLAN [33] :

- **Réduction des diffusions de broadcast :** les VLAN permettent de limiter les diffusions de broadcast en isolant les groupes d'utilisateurs dans des réseaux logiques distincts. Chaque groupe d'utilisateur ne peut communiquer qu'avec les utilisateurs du même VLAN, ce qui réduit considérablement les diffusions de broadcast sur l'ensemble du réseau.
- **Optimisation de la bande passante :** en limitant les diffusions de broadcast, les VLAN permettent d'optimiser la bande passante du réseau. Cela permet d'améliorer les performances et de réduire les temps de latence, en particulier dans les réseaux à forte charge.
- **Gestion des utilisateurs par fonction ou département :** les VLAN permettent de regrouper les utilisateurs par fonction ou département, ce qui facilite la gestion du réseau. Les administrateurs peuvent définir des politiques de sécurité, de qualité de service ou de bande passante pour chaque VLAN, en fonction des besoins des utilisateurs.
- **Amélioration de la sécurité** : les VLAN permettent également d'améliorer la sécurité en limitant l'accès aux ressources du réseau. Chaque VLAN est considéré comme un réseau distinct, ce qui permet de définir des politiques de sécurité spécifiques par groupe d'utilisateurs.

I.6.8.3 Agrégation de VLAN

Une agrégation est une liaison point à point entre deux périphériques réseau qui porte plusieurs VLAN à l'ensemble d'un réseau. Une agrégation de VLAN n'appartient pas à un VLAN spécifique, mais constitue plutôt un conduit pour les VLAN entre les commutateurs et les routeurs [34].

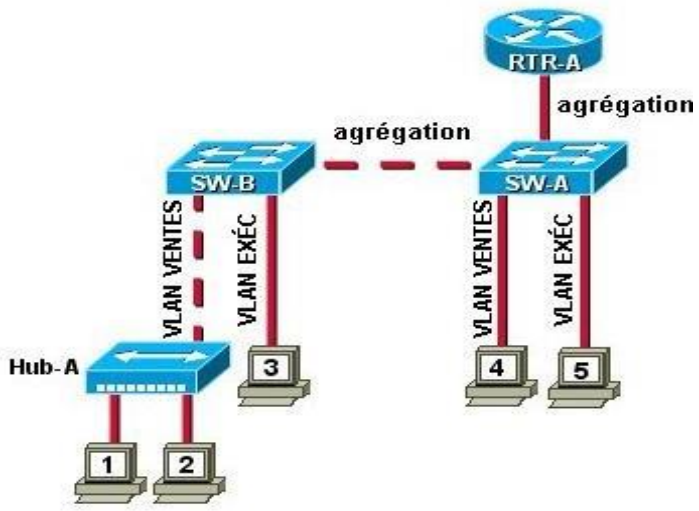


Figure 18: Agrégation de VLAN [18].

I.7 Adressage IP (Internet Protocol)

I.7.1 Définition d'une adresse IPV4

L'adresse IP est un numéro unique qui permet d'identifier chaque ordinateur connecté sur un réseau. Ce numéro est réparti en quatre fois 8 bits allant de 0 jusqu'à 255 séparées par des points. On distingue deux parties dans une adresse IP, la partie réseau et la partie hôte. La première identifie le réseau sur lequel est connectée la machine et la deuxième identifie les machines connectées à ce réseau [35].

I.7.2 Les classes d'adresse

Chaque adresse IP appartient à une classe qui correspond à une plage d'adresses IP. Ces classes d'adresses sont au nombre de 5 c'est-à-dire les classes A, B, C, D et E. Le fait d'avoir des classes d'adresses permet d'adapter l'adressage selon la taille du réseau c'est-à-dire le besoin en termes d'adresses IP [36].

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

I.7.3 Masque réseau

Le masque est un séparateur entre la partie réseau et la partie machine d'une adresse IP. Le masque, comme l'adresse IP, est une suite de 4 octets, soit 32 bits. Chacun de ces bits peut prendre la valeur 1 ou 0. Pour définir le masque, il nous suffit de dire que les bits à 1 représenteront la partie réseau (Net-ID) de l'adresse, et les bits à 0 la partie machine (Host-ID). Ainsi, on fera une association entre une adresse IP et un masque pour savoir, dans cette adresse IP, quelle est la partie réseau et quelle est la partie machine de l'adresse [37].

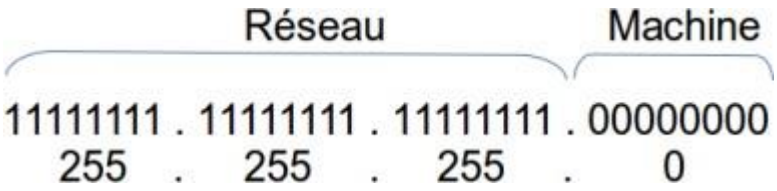


Figure 19: Exemple d'un masque réseau [19].

Ainsi, dans l'exemple illustré par Figure 19, 8 bits du masque du sous-réseau sont à 0 (partie hôte), on aura donc la possibilité d'avoir 2^8 -2 machines disponibles dans ce sous-réseau, machines qui pourront dialoguer entre-elles.

I.7.4 Un masque générique (wildcard mask)

Un masque générique est une séquence de bits binaires qui aide à rationaliser le routage des paquets au sein d'un sous-réseau. Il est affiché avec l'adresse de sous-réseau, fournissant au routeur des informations sur les parties d'adresse de sous-réseau sur lesquelles se concentrer. L'utilisation de la marque générique aide le routeur à se concentrer uniquement sur les chiffres choisis par le masque plutôt que sur l'intégralité de l'adresse IP. Les masques génériques sont normalement utilisés pour spécifier quelles adresses IP peuvent être autorisées ou refusées dans les listes de contrôle d'accès et avec des protocoles de routage tels que Open Shortest Path First (OSPF) [38].

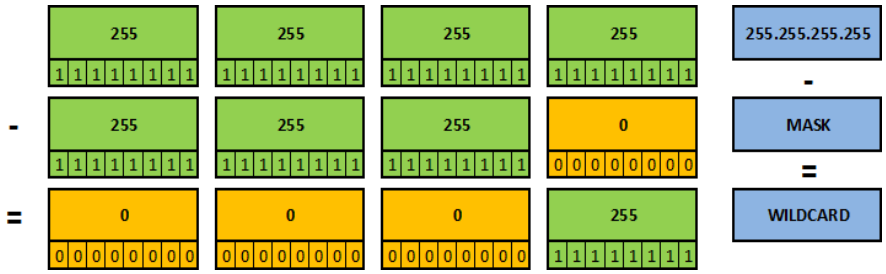


Figure 20 : Exemple d'un wildcard mask [20].

I.7.5 Adresse de diffusion

Broadcast est une connexion multipoint dans les réseaux IP qui atteint automatiquement tous les participants du réseau sans connaître les adresses des destinataires. Il existe pour cela dans chaque réseau ou sous-réseau une adresse de broadcast qui est en permanence réservée.

Dans l'adresse IP de broadcast, tous les bits de l'hôte sont définis sur la valeur binaire « 1», il s'agit de l'adresse de broadcast [39].

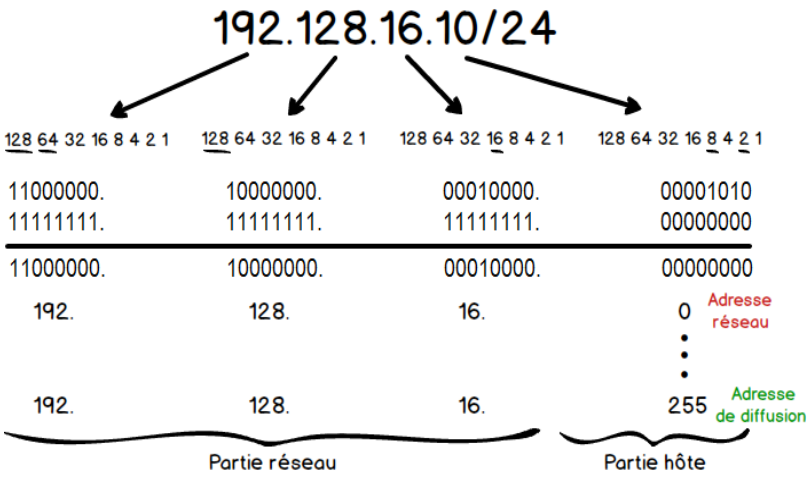


Figure 21: Exemple du calcul d'une adresse de diffusion [21].

I.7.6 Les sous-réseaux

Un sous-réseau est une portion d'un réseau informatique qui est créée en divisant un réseau plus grand en plusieurs parties plus petites, appelées sous-réseaux. Chaque sous-réseau a une adresse IP unique et peut contenir plusieurs ordinateurs, périphériques ou équipements de réseau connectés ensemble. Les sous-réseaux sont souvent utilisés pour optimiser les performances et la sécurité du réseau en réduisant le trafic sur le réseau global [40].

I.8 Conclusion

Ce chapitre nous a permis de comprendre les principes fondamentaux des réseaux informatiques, dont la structure, les différentes topologies et les composants d'un réseau, ainsi que les protocoles de communication utilisés pour assurer les interconnexions entre les différents périphériques.

En somme, le chapitre des généralités est une introduction complète et essentielle à la compréhension des réseaux informatiques et des technologies de communication modernes.

Chapitre II. Présentation de l'organisme d'accueil et des techniques de redondance réseaux.

II.1 Introduction

Dans le monde des affaires d'aujourd'hui, les réseaux informatiques sont un élément essentiel de l'infrastructure de l'entreprise. La perte de connectivité réseau peut avoir des conséquences graves, allant des temps d'arrêt coûteux à la perte de données critiques. Pour éviter ces problèmes, les entreprises investissent souvent dans des architectures réseau redondantes.

Dans ce chapitre, nous allons examiner les différentes techniques de redondance de réseau d'entreprise, y compris les protocoles de routage redondants, les connexions réseau en double, les équipements en double, et les technologies de tolérance aux pannes. Nous allons également discuter des avantages et des inconvénients de ces techniques, et des facteurs à prendre en compte lors de la conception d'un réseau redondant.

Ce chapitre se compose de deux parties, la première présente notre entreprise d'accueil et la deuxième décrit l'ensemble des techniques de redondance réseau.

II.2 Présentation de l'organisme d'accueil

II.2.1 Présentation de l'entreprise et son histoire

Figure 22:Logo Cevital .

Cevital est un conglomérat industriel algérien, fondé en 1998 par Issad Rebrab. L'entreprise est devenue un acteur majeur de l'économie algérienne et un important employeur dans le pays.

L'histoire de Cevital remonte à 1988, lorsqu'Issad Rebrab, un entrepreneur algérien, a créé une petite entreprise. Au départ, elle était spécialisée dans la production de sucre et d'huile végétale, en 1998 elle a diversifié ses activités dans d'autres secteurs, notamment l'industrie automobile avec la création de la marque automobile "Cevital Motors".

Cevital opère dans une variété de secteurs, notamment l'agroalimentaire, l'automobile, l'électronique, la sidérurgie, l'énergie, l'immobilier et la grande distribution. Comme elle contribue largement au développement de l'industrie agroalimentaire nationale, elle offre des produits de haute qualité aux consommateurs, mais aussi aux industriels, et ce grâce à ses prix compétitifs, son savoir-faire, la modernité de ses unités de production, le contrôle strict en ce qui concerne la qualité, mais aussi et surtout un réseau de distribution très développé.

Au fil des années, Cevital a connu une croissance rapide et est devenue l'une des plus grandes entreprises d'Algérie. Elle a également étendu ses activités à l'étranger, avec des projets en Europe, en Afrique et en Amérique du Nord [41].

II.2.2 Valeurs du groupe Cevital

Les quatre règles d'or (IRIS) à respecter :

- ✓ **Initiative :** Le collaborateur anticipe les problèmes potentiels, et propose des solutions innovantes grâce à sa connaissance métier.
- ✓ **Respect :** Un principe prime entre collaborateurs, et avec les partenaires internes et externes.
- ✓ **Intégrité :** Une valeur fondamentale, les collaborateurs par leurs actes doivent adopter une éthique professionnelle irréprochable.
- ✓ **Solidarité :** Les collaborateurs doivent s'entraider mutuellement, et partager leur expérience et savoir.

II.2.3 Infrastructure de l'entreprise

CEVITAL Agro-industrie dispose de plusieurs unités de production ultra modernes qui se présentent comme suit :

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

II.2.4 Situation géographique

Cevital agro-industrie est le plus grand complexe privé en Algérie, il s'étend sur une superficie de 45000 m² avec un siège social situé à Béjaïa, au nouveau quai du port, à proximité de la route nationale 26 soit à 280 km d'Alger, ce qui fait que cet emplacement géographique lui est bénéfique, car elle se trouve pas loin de l'aéroport, du port de Bejaia, et dela zone industrielle d'Akbou ce qui lui permet de posséder un quai privé.

Le groupe possède également des installations et des bureaux dans d'autres villes algériennes telles qu'Alger, Oran, Tizi-Ouzou et Constantine. Le complexe qui a fait l'objet de notre cas d'étude est situé au nouveau quai de l'arrière-port de Bejaïa.

Cevital a également étendu ses activités à l'étranger, avec des bureaux et des installations dans plusieurs pays, notamment la France, les Émirats Arabes Unis, le Portugal, l'Italie, les États-Unis, l'Espagne et le Brésil. Ces filiales étrangères sont principalement axées sur la distributionet la commercialisation de produits Cevital dans ces pays.

Figure 23: Vue satellitaire du complexe Cevital.

II.2.5 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.

- **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.

- **La direction des ressources humaines :** cette direction a pour mission d'assurer un support administratif à l'ensemble du personnel de CEVITAL, de piloter les activités du social et d'assister à la direction générale ainsi que tous les managers sur tous les aspects de la gestion des ressources humaines.

- **La direction industrielle :** elle est chargée de l'évolution industrielle des sites de production et définit, avec la direction générale, les objectifs et le budget de chaque site. Elle analyse les dysfonctionnements sur chaque site (équipements, organisations, etc.) et recherche des solutions techniques ou humaines pour améliorer en permanence la productivité, la qualité des produits et des conditions de travail. Elle anticipe aussi les besoins en matériels et supervise leurs achats.

- **La direction des systèmes d'informations :** elle assure la mise en place des moyens des technologies de l'information nécessaire pour supporter et améliorer l'activité, la stratégie et la performance de l'entreprise. Elle doit ainsi veiller à la cohérence des moyens d'informatique de communication mis à la disposition des utilisateurs, à leurs mises à niveau, à leurs maîtrises techniques, disponibilité et opérationnalité permanente en toute sécurité.

L'ensemble des directions de l'entreprise sont schématisées dans la figure suivante :

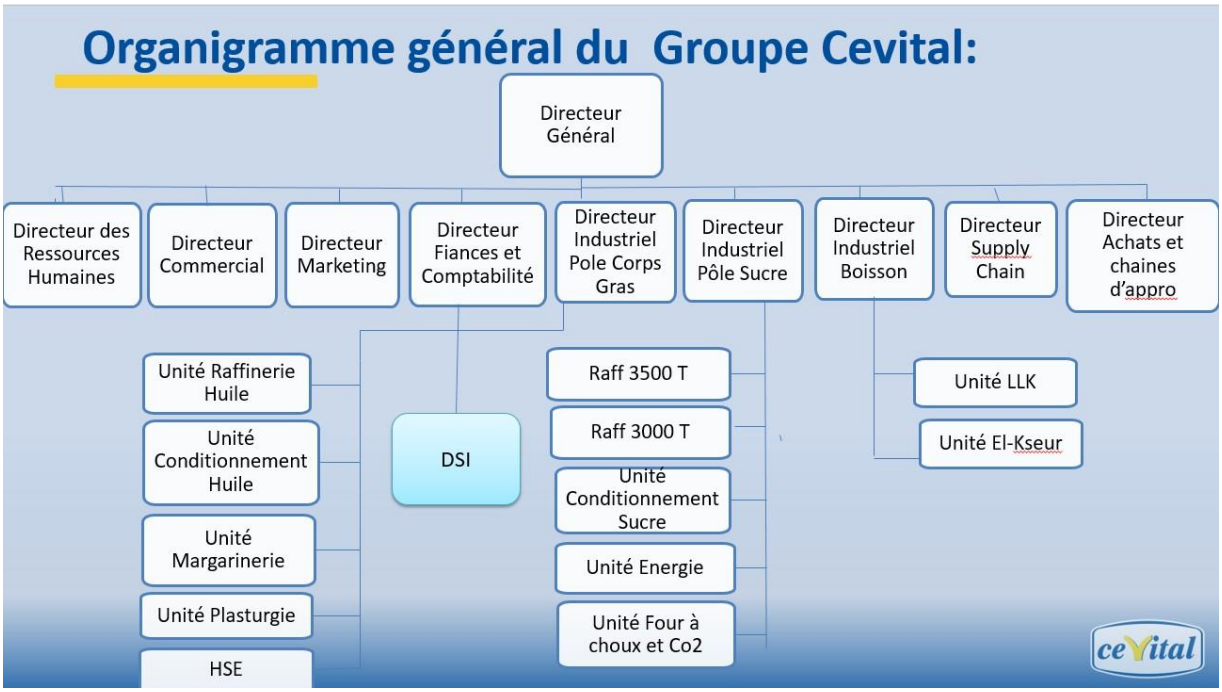


Figure 24:Organigramme général du groupe Cevital.

II.2.6 Organigramme de la direction du système d'information

Dans le cadre de ce stage pratique, nous avons eu l'opportunité d'effectuer notre stage au sein de la direction des systèmes informatiques (DSI).

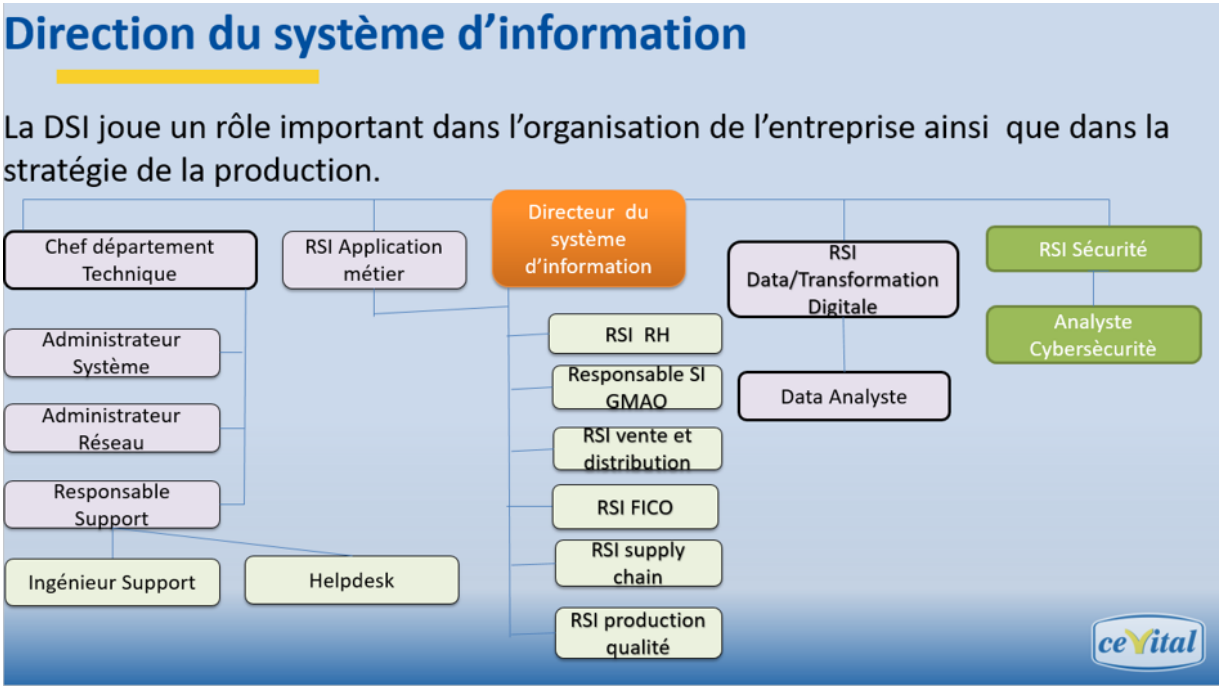


Figure 25:Organigramme de la DSI.

Le service informatique est suivi par des responsables spécialistes cités ci-dessous :

- **Directeur du système d'information :** Il est chargé de régler les problèmes à moindre coût et dans les plus brefs délais et opter pour des solutions informatiques améliorant la

productivité de l'entreprise.

- **Administrateur système :** Il conçoit, installe et veille au bon fonctionnement d'une infrastructure informatique et réseau d'une entreprise, il assure également la gestion et la maintenance de système opérant sur le réseau.

- **Administrateur réseau :** Il permet d'administrer le réseau et d'assurer la bonne circulation de l'information dans l'entreprise en veillant à la qualité, continuité et la performance des équipements et du réseau, tout en répondant aux besoins des utilisateurs.

- **Responsable support :** Il permet d'assurer un contrôle à distance des postes, apporter aux utilisateurs une aide pour la prise en main de leur équipement et assurer un support téléphonique interne.

II.2.7 Architecture réseau de Cevital

CEVITAL dispose d'un réseau interne assez vaste permettant de relier les différents bâtiments, unités de production et direction de complexe. Nous pouvons le décomposer en plusieurs parties : le backbone du réseau, un pare-feu et un DMZ (zone démilitarisée), une couverture wifi, un routeur et un data-center (où sont placés les serveurs de l'entreprise). Le réseau est composé de plusieurs équipements dont la plupart sont de marque Cisco interconnectés entre eux grâce à la fibre optique ou câbles en cuivre. (Voir figure 26)

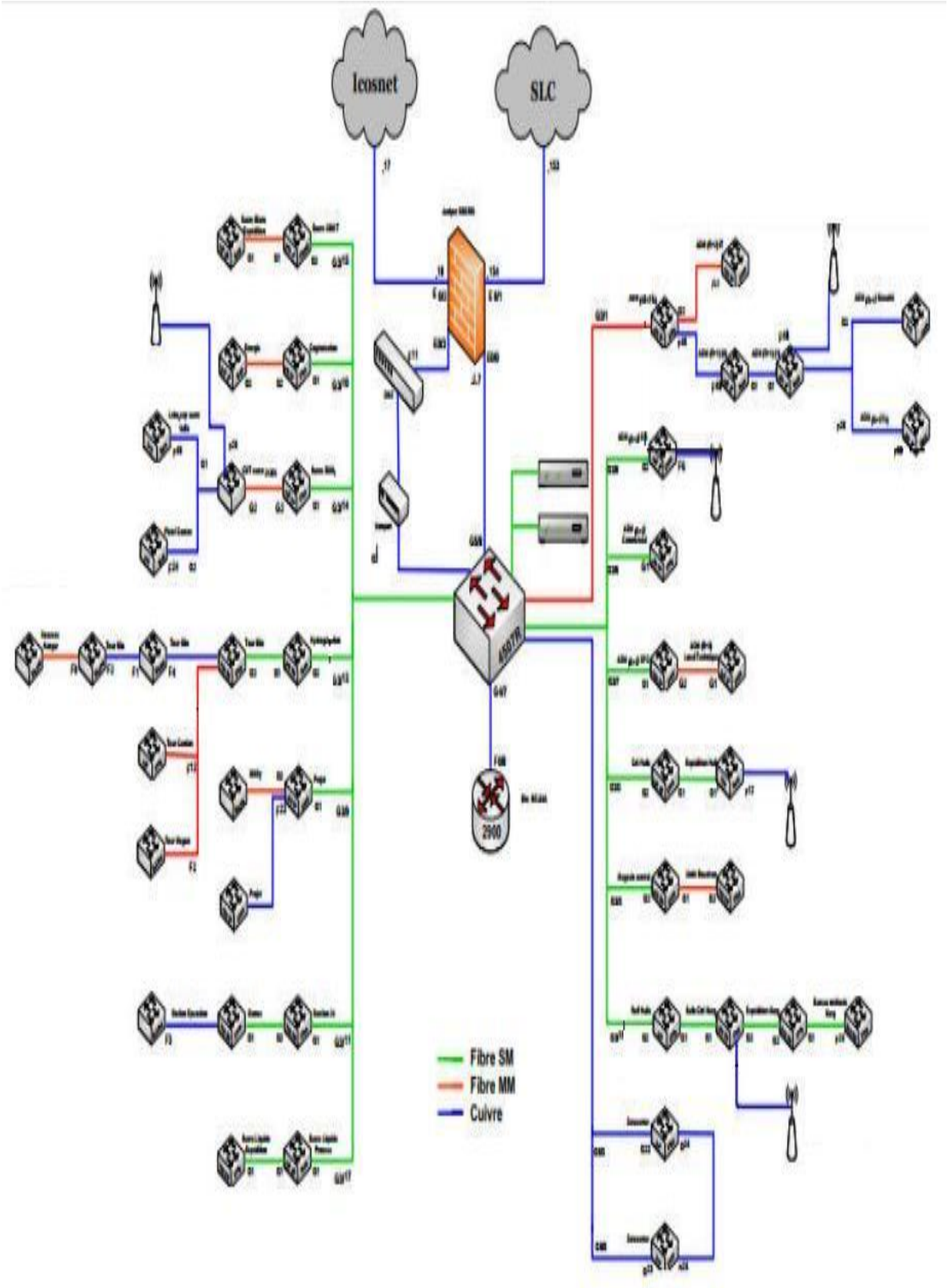


Figure 26:Architecture réseau de Cevital.

.

Le réseau local du complexe se compose de trois couches, couche Core qui représente aussi la couche distribution (backbone), la couche accès et la couche en cascade.

- **Couche Core (Distribution) :** le Backbone est composé d'un Switch Catalyst placé au data center du bâtiment, qui est relié aussi bien au pare feu et au routeur à l'aide des câble RJ45, qu'aux Switches d'accès à l'aide de la fibre optique offrant ainsi un meilleur débit aux différents postes. Cette partie est la plus sensible parce qu'elle est reliée à tous les équipements réseau.

- **Couche d'accès :** cette couche se compose des switches qui sont distribués sur les différents sites locaux du bâtiment. Les responsables du réseau de CEVITAL utilisent des VLANs pour partager l'accès aux utilisateurs d'une façon que chaque site local (étage des bâtiments) comprend un ou plusieurs VLANs.

- **Couche en cascade :** dans cette couche les switches sont reliés entre eux et aux switches d'accès (ils ne sont pas directement reliés au backbone) et fournissent un accès aux utilisateurs, au sein de ses switches des VLANs permettent de définir plusieurs sous-réseaux en fonction des départements de l'entreprise.

II.2.8 Liaison inter-sites (architecture WAN)

Afin d'assurer le partage des ressources et de la communication interne de l'entreprise, CEVITAL dispose des connexions qui permettent de relier le site Bejaïa aux différentes annexes de l'entreprise telles que :

- Liaison par VPN (RMS) entre Bejaïa et les sites d'El-kseur (Cojek), site de TiziOuzou (Lala Khadija) et site El Kheroub (Constantine).

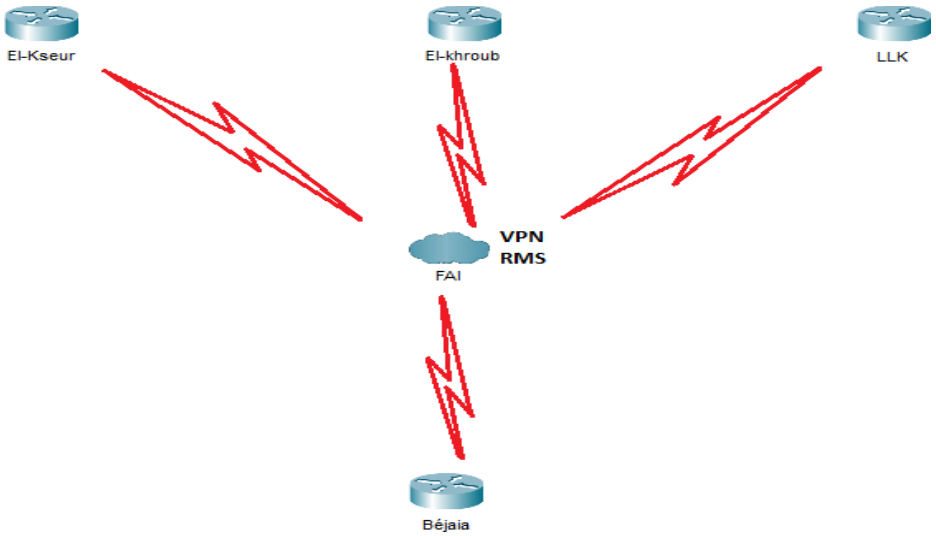


Figure 27:Lisaison inter-sites du groupe Cevital.

✓ **VPN(RMS)**

La solution proposée afin d'interconnecter les différents sites, consiste en la création de réseaux privés virtuels (VPN) [42].

Afin d'assurer un accès aisé et peu coûteux aux entreprises, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils mettent en œuvre en réalité une infrastructure d'accès partagé, tel que le RMS.

✓ **RMS (Remote Monitoring System)**

La Liaison spécialisée est une liaison permanente réservée à l'usage exclusif d'un utilisateur. Elle offre la possibilité de transmission entre deux points de terminaison déterminés du réseau public.

✓ **Qu'est-ce qu'un VPN RMS ?**

RMS VPN est un service conçu pour une gestion à distance efficace et peu coûteuse de réseaux à grande échelle. Contrairement au service VPN point à point, le VPN RMS permet de créer des tunnels VPN cryptés pour un accès sécurisé à plusieurs points de terminaison en quelques secondes. Il est très utile dans le secteur des entreprises, nous le montrons dans un exemple particulièrement pertinent. Imaginez que les employés de l'entreprise doivent soudainement passer à un scénario de travail à domicile en raison d'une pandémie. Cependant, tous les systèmes et bases de données de l'entreprise ne sont disponibles que sur site via LAN. Par conséquent, les possibilités d'accomplir leurs tâches professionnelles deviennent très limitées. Voici donc le service VPN RMS, permettant d'ajouter les ordinateurs des employés à un réseau virtuel et leur permettant d'accéder aux systèmes et applications internes depuis leur domicile.

II.2.9 Equipements utilisés dans l'architecture

L'architecture réseau du Cevital est composée de :

- **Distributeur (Backbone) Cisco Catalyst 4507R :** c'est la partie centrale du réseau, Il supporte le trafic de données le plus important du réseau de l'entreprise avec une bande passante très large, sur lequel les commutateurs d'accès, le pare-feu, serveurs et routeurs de l'entreprise y sont connectés. Il s'occupe du routage inter-Vlan (Virtual Lan) et il permet l'accès à internet via le pare-feu, il peut jouer le rôle d'un serveur DHCP. Il est aussi appelé un switch fédérateur.

Figure 28: Switch distributeur Cisco Catalyst 4507R [22].

- **Switch d'accès et en cascade Cisco Catalyst 2960 et 2950 :** Ils sont connectés au backbone et installés dans les différents bâtiments de l'entreprise.

Figure 29:Switch Cisco Catalyst 2960 [23].

- **Routeur de type Cisco 2900 :** Il permet de gérer le routage entre les différents sites del'entreprise.

Figure 30:Routeur Cisco 2900 [24].

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

Figure 31:Point d'accès WIFI Ruckus [25].

- **Pare-feu :** quatre pare-feu sont reliés en redondance et permettant de sécuriser le réseau, d'isoler certaines parties de celui-ci, d'encadrer et de sécuriser l'accès internet.

Figure 32:Pare feu Fortinet [26].

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

Figure 33:Data Center [27].

- **Câblage informatique :** le système de câblage informatique installé est conçu pour fonctionner de façon idéale pour permettre des améliorations futures. Tout dispositif informatique existant dans l'entreprise est interconnecté via le câblage de type fibre optique. Les boîtiers des prises muraux sont repérés par des étiquettes portant un numéro unique sur le réseau et qui est repéré facilement dans le panneau de brassage pour l'interconnexion avec les commutateurs.

II.2.10 Modèle et nombre des équipements

L'ensemble des équipements utilisés sur l'architecture réseau sera résumé en ce tableau suivant :

Equipement		Le hardware			Le software
		Nombre	Marque		
Ordinateurs personnels		1400	80% HP 15% Lenovo		Windows 1022H2 Windows 1122H2
Imprimantes		150	90% Canon		
Téléphones	Numériques	700	Alcatel-Lucent	4019,4029,4039	
	Analogiques			/	
	IP			4018,4028,8028s	
	Dect			8232s	
Routeur		02	Cisco		
Switch		55	Cisco		
Serveur	Physique	40	HP		
	Virtuelle	22			
Pare-feu		04	Fortinet		
Point d'accès		26	Ruckus, zoneFlex R500		
PDA		---------	Motorola		
Caméras		473	Samsung, pelco, dahua		

Tableau 1: Modèle et nombre des équipements du Cevital.

II.2.11 Nombre et modèle des Switches

Modèle	Nombre
WS-C2960X-48FPS-L	07
WS-C2960X-24PS-L	07
WS-C2960X-24PS-L V03	04
WS-C2960X-24PS-L V06	02
WS-C2960-48PST-L	04
WS-C2960-48TC-L	07
WS-C2960-24TC-L	03
WS-C2960-24TC-S	01
WS-C2960-24PC-L	03
WS-C2960C-12PC-L V05	02
WS-C2960-24LT-L	02
WS-C2960C-12PC	02
WS-C2960-8TC-L	01
C2950-I6K2L2Q4-M	01
WS-C2950G-12-EI	02
WS-C3850-24S	02
C6807-XL	02
Nexus 3048	03

Tableau 2 : Nombre et modèle des Switch.

Cevital possède plusieurs modèles de switches qui sont en EOL et EOS, pour y remédier elle vient de recevoir 10 nouveaux switches du modèle Cisco C9200L 48 ports qui vont remplacer les switches en EOL et EOS dans les prochains jours, et vient aussi de lancer l'achat

de 20 nouveaux autres switches de la même gamme (17 qui auront 24 ports et 3 qui auront 48 ports).

II.2.12 Modèles des Serveurs

Cevital possède 62 serveurs dont 40 sont physiques tandis que 22 sont logiques, parmi eux :

- Serveur WSUS pour les mises à jour des machines.
- Sage x3 pour la facturation et la comptabilité.
- Coswin pour la gestion des stocks et maintenance
- Kelio pour le suivi des pointages.
- Skeeper pour la traçabilité.
- 2 Exchange comme serveurs de messagerie.
- GLPI présente la plateforme pour recevoir les tickets des utilisateurs en cas de problèmes informatiques.

II.2.13 Codification des équipements de Cevital

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

II.2.14 VLANs de l'entreprise

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

Direction	VLAN	Adresse réseau	Passerelle
DRH	VLAN10	10.10.10.0/24	10.10.10.254
Direction des Appro	VLAN11	10.10.11.0/24	10.10.11.254
DSI	VLAN12	10.10.12.0/24	10.10.12.254
Raff Huile	VLAN13	10.10.13.0/24	10.10.13.254
Raff sucre 3000T	VLAN14	10.10.14.0/24	10.10.14.254
Division utilités	VLAN15	10.10.15.0/24	10.10.15.254
Supply-chain	VLAN16	10.10.16.0/24	10.10.16.254
Unité margarinerie	VLAN17	10.10.17.0/24	10.10.17.254
Printer	VLAN18	10.10.18.0/24	10.10.18.254
Téléphone	VLAN20	10.10.20.0/24	10.10.20.254
Voice	VLAN21	10.10.21.0/24	10.10.21.254

Direction R&D	VLAN22	10.10.22.0/24	10.10.22.254
Performance industriel	VLAN23	10.10.23.0/24	10.10.23.254
Unité Cdt Huile	VLAN24	10.10.24.0/24	10.10.24.254
Management switch	VLAN25	10.10.25.0/24	10.10.25.254
DFC	VLAN26	10.10.26.0/24	10.10.26.254
Commercial	VLAN27	10.10.27.0/24	10.10.27.254
Direction générale	VLAN28	10.10.28.0/24	10.10.28.254
Direction qualité et management système	VLAN29	10.10.29.0/24	10.10.29.254
Raff sucre 3500T	VLAN30	10.10.30.0/24	10.10.30.254
Cdt sucre	VLAN31	10.10.31.0/24	10.10.31.254
Caméra	VLAN32	10.10.32.0/24	10.10.32.254
Projets	VLAN33	10.10.33.0/24	10.10.33.254
Trituration	VLAN36	10.10.36.0/24	10.10.36.254

Tableau 2:Vlan de l'entreprise.

II.2.15 Analyse et critique de l'existant

Après avoir décortiqué le réseau de CEVITAL, en l'occurrence le réseau informatique existant, de nombreuses insuffisances ont été découvertes. Ceci nous a permis de définir un nombre important de contraintes fonctionnelles, cependant celles-ci peuvent réduire significativement les performances du réseau existant, voire même des dysfonctionnements fréquents. Les constats résultants de notre étude par rapport au réseau existant sont les suivants:

- Un seul backbone centralise le réseau, ce qui implique la surcharge de ce dernier.
- Les switches sont reliés en cascade, ce type de liaison est problématique car :
  - Il provoque une limitation de la bande passante ce qui ralentit par conséquent les applications et les ressources.
  - Il entraîne une panne dans plusieurs bâtiments si une défaillance de l'un des switches survient.
  - Il a un impact significatif sur les coûts de l'entreprise.
- L'absence d'équipements en redondance qui assurera la tolérance aux pannes et garantira des liaisons de secours aux équipements, d'ailleurs cela induit plusieurs points de défaillances dans l'architecture du réseau.

II.2.16 Problématique et solutions

La disponibilité du réseau est cruciale pour le bon fonctionnement d'une entreprise. Cependant, les défaillances d'équipements ou de liaisons peuvent survenir à tout moment, ce qui peut entraîner une interruption de service et une perte de productivité.

Par conséquent, la problématique suivante se pose : Comment assurer une disponibilité maximale du réseau de l'entreprise en cas de défaillance d'un équipement ou d'une liaison ?

Cette problématique est d'autant plus importante que les entreprises dépendent de plus en

plus des technologies de l'information pour leur fonctionnement quotidien. Les perturbations dans le réseau peuvent avoir des conséquences importantes sur la productivité des employés, la satisfaction des clients et la rentabilité de l'entreprise.

Pour assurer une disponibilité maximale du réseau de l'entreprise en cas de défaillance d'un équipement ou d'une liaison, il est nécessaire de mettre en place des stratégies de redondance et de résilience. Cela peut inclure :

- **Division du réseau en couches distinctes :** le modèle de conception se divise en trois couches: la couche d'accès, la couche de distribution et la couche cœur de réseau, ce qui rend la conception modulaire et évolutive. La couche de distribution est ajoutée pour assurer la double connectivité avec les switches d'accès, ce qui limitera la taille des câbles et réduira les coûts de l'entreprise.

- **La mise en place de systèmes de redondance :** les entreprises peuvent utiliser des équipements réseau de secours pour prendre le relais en cas de défaillance d'un équipement principal. La redondance peut se présenter sous différentes formes. Par exemple, doubler les connexions réseau entre les périphériques, ou bien doubler les périphériques eux-mêmes. L'implémentation de liaisons redondantes peut être coûteuse. Il serait improbable d'implémenter une redondance sur la couche d'accès, en raison du coût et des fonctionnalités limitées des périphériques finaux. Cependant, la redondance sera implémentée au niveau des couches de distribution et cœur de réseau en utilisant des protocoles de redondance.
- **Diamètre du réseau :** lors de la conception d'une topologie de réseau hiérarchique, le premier élément dont il faut tenir compte est le diamètre du réseau. Le diamètre correspond généralement à une mesure de distance, mais dans ce cas, ce terme est utilisé pour mesurer le nombre de périphériques. Il correspond également au nombre de périphériques que doit traverser un paquet avant d'atteindre sa destination. Lorsque vous maintenez un faible diamètre de réseau, cela garantit une latence faible et prévisible entre les périphériques.

- **La mise en place de tests de diagnostic réguliers :** les entreprises peuvent effectuer des tests réguliers sur leurs équipements et leurs liaisons pour détecter les problèmes potentiels avant qu'ils ne deviennent graves. Les tests de diagnostic peuvent aider à identifier les équipements défectueux ou les liaisons défaillantes et à les remplacer avantqu'ils ne causent des perturbations.

II.3 La haute disponibilité d'un réseau informatique

La haute disponibilité des réseaux informatiques est un enjeu majeur pour assurer la continuité des activités des entreprises et des organisations en dépit de pannes, de coupures de courant, d'attaques de cybercriminels ou d'autres événements imprévus. Une infrastructure réseau haute disponibilité garantit une connectivité constante et une disponibilité des services informatiques essentiels, ce qui permet aux entreprises de maintenir leur productivité et leur compétitivité. Dans cette optique, différentes techniques et technologies sont utilisées pour assurer un accès ininterrompu aux services réseau, telles que la redondance, la répartition de charge, la virtualisation et la surveillance proactive.

II.3.1 Définition de la haute disponibilité

La haute disponibilité est la capacité d'un système informatique ou d'un réseau à fournir un accès continu et ininterrompu à ses services, données et applications essentiels, même en cas de panne ou de défaillance d'un composant. Cela implique l'utilisation de technologies et de stratégies de redondance, de résilience et de reprise après sinistre pour minimiser les temps d'arrêt et garantir une disponibilité maximale des services.

Ces techniques permettent d'assurer la continuité de service en cas de panne ou de défaillance d'un composant en redirigeant automatiquement les utilisateurs vers une instance fonctionnelle de l'application ou du service. Ainsi, la haute disponibilité est une exigence critique pour les entreprises qui dépendent de la disponibilité des systèmes informatiques pour leur activité quotidienne.

II.3.2 Evaluation des risques

La panne d'un système informatique peut causer une perte de productivité et d'argent, voir des pertes matérielles ou humaines dans certains cas critiques. Il est ainsi essentiel d'évaluer les risques liés à un dysfonctionnement d'une des composantes du système d'information et de prévoir des moyens et mesures permettant d'éviter ou de rétablir dans des temps acceptables tout incident. Les risques de pannes d'un système informatique en réseau sont nombreux, on peut les classer selon leurs origines comme suit :

- **Origines physiques :**

  Elles peuvent être d'origine naturelle ou humaine :

  - Désastre naturel (inondation, séisme, incendie).
  - Environnement (intempéries, taux d'humidité de l'air, température).
  - Panne matérielle.
  - Panne du réseau.
  - Coupure électrique.

- **Origines humaines :**

  Elles peuvent être soit intentionnelles soit fortuites :

  - Erreur de conception (bogue logiciel, mauvais dimensionnement du réseau).
  - Porte dérobée.
  - Sabotage.
  - Piratage.

- **Origines opérationnelles :**

  Elles sont liées à un état du système à un moment donné :

  - Bogue logiciel.
  - Dysfonctionnement logiciel.

Pour assurer la haute disponibilité et le bon fonctionnement du réseau, on fait appel aux techniques de redondance.

II.3.3 La redondance

La redondance des réseaux informatiques est une technique qui consiste à ajouter des chemins de communication supplémentaires pour garantir une disponibilité continue des réseaux, en minimisant les temps d'arrêt. Elle permet d'assurer la continuité de service en cas de défaillance d'un composant du réseau, tel qu'un routeur, un commutateur ou un câble. Elle permet également d'améliorer la performance et la capacité des réseaux, en tolérant la répartition de la charge de travail entre plusieurs chemins de communication. Elle est particulièrement importante dans les environnements où la disponibilité du réseau est critique, comme centres de données ou les systèmes de contrôle de processus industriels [43].

La redondance des réseaux informatiques peut être mise en place de différentes manières, en fonction des besoins et des contraintes du réseau. Parmi les techniques courantes, on peut citer :

- **Au niveau des connexions réseau :** en utilisant plusieurs connexions physiques pour assurer une redondance, comme l'agrégation de liens ou la redondance de liens. Si une connexion tombe en panne, le trafic est automatiquement redirigé vers les autres connexions.
- **Au niveau des commutateurs :** en utilisant des commutateurs redondants pour permettre un basculement automatique en cas de panne d'un commutateur.
- **Au niveau des routeurs :** en utilisant des protocoles de redondance tels que HSRP et VRRP pour assurer un basculement transparent en cas de défaillance d'un routeur.
- **Au niveau des serveurs :** en configurant des serveurs en cluster pour permettre à un serveur de prendre le relais en cas de défaillance d'un autre serveur.

II.3.4 Les protocoles de redondance

Les protocoles réseaux transportent les données des applications à travers le réseau de l'entreprise. Ces protocoles comptent sur une architecture réseau qui fournit la hiérarchie, les adresses et les informations de la topologie aux machines clientes. Une passerelle ou un routeur multi protocole approvisionne toutes ces informations. Les stations de travail, routeurs, et serveurs de fichiers doivent communiquer entre eux, et c'est dans ce but que les protocoles ont implémenté des méthodes de recherche pour trouver et conserver l'adresse de la passerelle.

II.3.5 Le protocol FHRP (First Hop Redundancy Protocol)

Le protocole FHRP est une technologie importante pour garantir la disponibilité et la fiabilité des réseaux d'entreprise, il assure la redondance des équipements réseau, et des passerelles par défaut. L'objectif principal du FHRP est de permettre aux équipements du réseau de fournir une adresse IP de passerelle par défaut virtuelle (ou adresse VIP) pour les hôtes connectés au

réseau. Cette adresse VIP est partagée entre les équipements réseau qui fournissent la redondance pour la passerelle par défaut.

Lorsqu'un routeur de passerelle par défaut tombe en panne, le protocole FHRP permet à un autre routeur de prendre le relais et de fournir la passerelle par défaut aux hôtes connectés. Cela permet d'assurer la continuité de service pour les utilisateurs du réseau, même en cas de panne d'un équipement [44].

Il existe plusieurs types de FHRP, notamment HSRP (Hot Standby Router Protocol), VRRP (Virtual Router Redundancy Protocol) et GLBP (Gateway Load Balancing Protocol).

II.3.5.1 Le protocole VRRP (Virtual Router Redundancy Protocol)

Le protocole VRRP (Virtual Router Redundancy Protocol) est un protocole de routage de niveau 3 qui permet de configurer un groupe de routeurs pour qu'ils partagent une adresse IP virtuelle, appelée adresse IP de passerelle par défaut. VRRP permet à un routeur de prendre le relais d'un autre routeur en cas de défaillance, assurant ainsi la redondance et la haute disponibilité de la passerelle par défaut [45].

- **Fonctionnement du protocole VRRP**

Le fonctionnement de VRRP est basé sur la notion de routeur virtuel (VR). Les routeurs du groupe VRRP élit un routeur virtuel qui est chargé de répondre aux requêtes ARP pour l'adresseIP virtuelle. Les autres routeurs du groupe VRRP servent de routeurs de sauvegarde et surveillent en permanence le routeur virtuel.

Si le routeur virtuel devient indisponible, le routeur de sauvegarde qui possède la priorité la plus élevée prend en charge l'adresse IP virtuelle et devient le nouveau routeur virtuel. Ce processus se produit de manière transparente pour les hôtes du réseau, qui continuent d'utiliser la même adresse IP de passerelle par défaut.

II.3.5.2 Le protocole HSRP (Hot Standby Router Protocol)

Le protocole HSRP (Hot Standby Routing Protocol) est un protocole de niveau 3 propriétaire de "continuité de service" implémenté dans les routeurs Cisco pour la gestion des "liens de secours". Il sert à augmenter la tolérance de panne sur le réseau en créant un routeur virtuel à partir de 2 (ou plus) routeurs physiques : un "**actif**" et l'autre (ou les autres) "**en attente**" (ou "standby") en fonction des priorités accordées à chacun de ces routeurs [46].

- **Fonctionnement du protocole HSRP**

Le protocole HSRP permettra aux routeurs situés dans un même groupe de former un routeur virtuel qui sera l'unique passerelle des hôtes du réseau local, en se cachant derrière ce routeur virtuel aux yeux des hôtes. Les routeurs garantissent en fait qu'il y est toujours un routeur qui assure le travail de l'ensemble du groupe. Un routeur dans ce groupe est donc désigné comme actif et ce sera lui qui fera passer les requêtes d'un réseau à un autre.

Pendant que le routeur actif travaille, il envoie également des messages aux autres routeurs indiquant qu'il est toujours vivant et opérationnel. Si le routeur principal (élu actif) vient à tomber, il sera automatiquement remplacé par un routeur qui était jusque-là passif et lui aussi membre du groupe HSRP. Aux yeux des utilisateurs toutefois, cette réélection et ce

changement de passerelle seront totalement invisibles, car ils auront toujours pour unique passerelle le routeur virtuel que forment les routeurs membres du groupe HSRP. Le routeur virtuel aura donc toujours la même adresse IP et adresse MAC aux yeux des hôtes du réseau même si en réalité il y a un changement du chemin par lequel transitent les paquets.

- **Le protocole HSRP vue d'un hôte d'un réseau :**

Un seul routeur qui fait office de passerelle est toujours disponible sur la même IP.

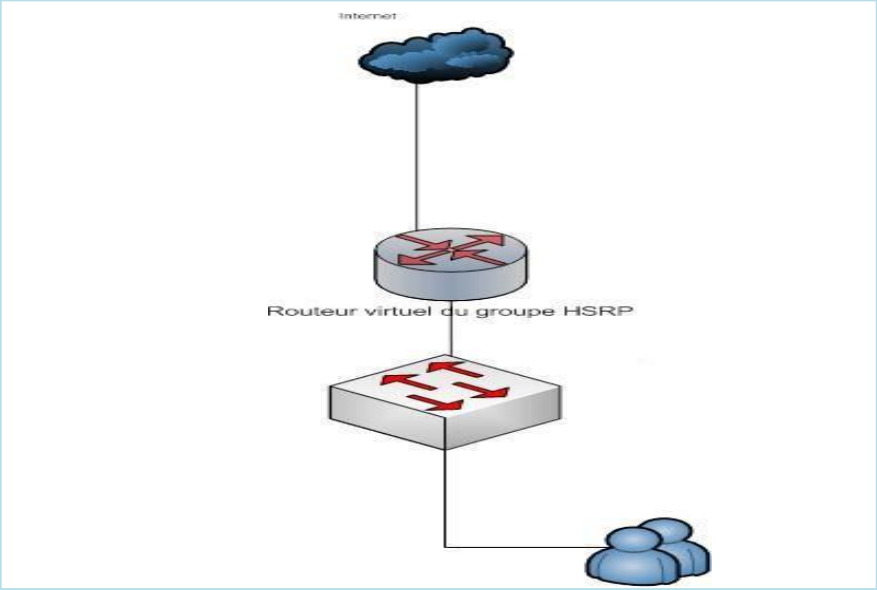


Figure 34: Schéma illustre le protocole HSRP vue d'un hôte d'un réseau [28].

- **L'état réel du réseau :**

Les routeurs physiques forment un routeur virtuel. Un des routeurs est en état actif et transmet les échanges alors que l'autre est en état passif et reste à l'écoute de l'état de routeur actif prêt à prendre la relève.

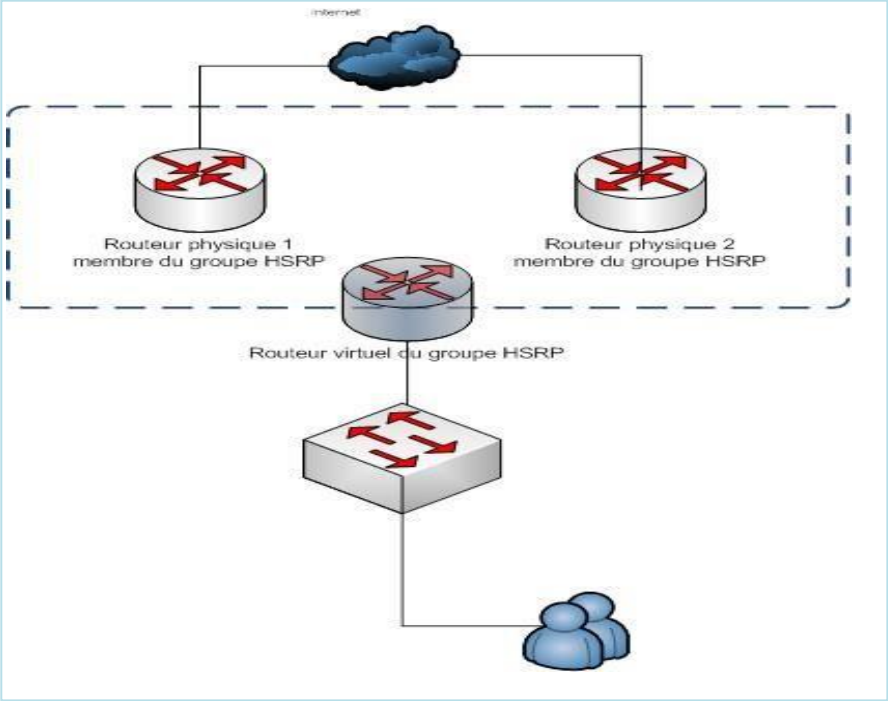


Figure 35: Schéma physique et virtuel d'un réseau HSRP [28].

HSRP possède trois types de messages multicast envoyés entre les appareils **:**

- **Hello** : c'est un type de message périodique utilisé par les routeurs pour maintenir leur état de synchronisation dans un groupe HSRP, il contient des informations importantes, telles que le numéro de groupe et le numéro de version HSRP. Chaque routeur envoie des messages "Hello" à intervalles réguliers (par défaut toutes les 3 secondes), indiquant qu'il est toujours en vie et qu'il participe toujours au groupe, par ailleurs s'il ne reçoit pas de message "Hello" d'un autre routeur pendant un certain temps (par défaut 10 secondes), il considère que ce dernier a échoué et prend des mesures pour assumer le rôle du routeur actif.

- **Démissionner** : il est envoyé par le périphérique HSRP actif lorsqu'il se prépare à se déconnecter ou à abandonner le rôle actif pour une autre raison. Ce message indique au routeur de secours d'être prêt et de reprendre le rôle actif.

- **Coup** : il est utilisé lorsqu'un routeur de secours veut assumer le rôle actif (préemption).

Lorsqu'un routeur rejoint le groupe HSRP pour la première fois, il passe par une séquence d'états avant de pouvoir assumer un rôle actif ou de secours dans le groupe. La séquence d'états est la suivante:

Initial	Indique un état de démarrage, le protocole n'est pas encore en cours d'exécution. Des interfaces sont disponibles.
Learn	Etat temporaire dans lequel un routeur HSRP écoute les messages "Hello" des autres routeurs du groupe et apprend leurs informations.

Listen	Indique que le routeur connaît l'adresse IP virtuelle, il n'a pas été choisi comme veille ou actif.
Speak	Le routeur participe activement à l'élection Actif/Veille en envoyant des messages Hello.
Standby	Agit en tant que sauvegarde. Surveille et envoie des messages Hello.
Active	Acceptation et transfert du trafic utilisateur.

Tableau 3: Les états d'un routeur HSRP.

Voici un tableau des commandes couramment utilisé pour la configuration du protocole HSRP sur routeur Cisco :

Commande	Description
`Standby <numéro de groupe> IP <adresse IP virtuelle>`	Configure l'adresse IP virtuelle pour le groupe HSRP spécifié.
`Standby <numéro de groupe> priority <priorité>`	Définit la priorité du routeur HSRP, par défaut 100.
`standby <numéro de groupe> preempt`	Active la fonctionnalité de préemption sur le routeur HSRP.
`Standby <numéro de groupe> authentication <mot de passe>`	Configure un mot de passe pour l'authentification HSRP.
`Standby<numéro de groupe> preempt [delay minimum_seconds]`	Configurer le délai de préemption.
`show standby`	Vérifier l'état HSRP.

Tableau 4:Commandes utilisées pour la configuration de l'HSRP.

II.3.5.3 Le protocole GLBP (Gateway Load Blancing Protocol)

GLBP est un protocole de niveau 3 propriétaire Cisco, qui fournit une redondance ainsi que de la répartition de charge sur plusieurs routeurs utilisant une seule adresse IP virtuelle, mais plusieurs adresses MAC virtuelles**,** Il protège les données de toutes failles d'un routeur ou d'un circuit, tout en permettant le partage de charge de paquets entre plusieurs routeurs redondants.

Contrairement au protocole HSRP, qui permet à un seul routeur de servir de passerelle par défaut, GLBP permet à plusieurs routeurs de servir de passerelle en même temps, ce qui améliore les performances et la disponibilité du réseau en distribuant les tâches de traitement des requêtes ARP entre plusieurs routeurs [47].

- **Fonctionnement du protocole GLBP**

Le fonctionnement du protocole GLBP peut être décrit en quatre étapes :

1. Les routeurs du groupe GLBP élisent un routeur actif en utilisant le même

mécanisme que celui utilisé dans HSRP. Le routeur actif assume la responsabilité de la passerelle par défaut et répond aux requêtes ARP pour l'adresse IP virtuelle associée au groupe GLBP.

2. Chaque routeur du groupe GLBP se voit attribuer un ou plusieurs membres du groupe GLBP, appelés propriétaires virtuels (VG, Virtual Gateway). Les propriétaires virtuels sont responsables de répondre aux requêtes ARP pour les adresses IP virtuelles associées au groupe GLBP.

3. Les routeurs du groupe GLBP utilisent une technique de round-robin pour distribuer les requêtes ARP entrantes entre les propriétaires virtuels. Cela permet de répartir la charge de trafic sur plusieurs routeurs, ce qui peut améliorer les performances et la disponibilité du réseau.

4. En cas de défaillance d'un routeur, les autres routeurs du groupe GLBPdétectent rapidement la panne et redistribuent les propriétaires virtuels en conséquence. Cela garantit que les requêtes ARP continuent à être traitées même en cas de défaillance d'un routeur.

II.3.6 Le protocole STP (Spanning-Tree Protocol)

Le protocole Spanning-tree (STP) est un protocole de niveau 2 conçu pour les commutateurs. Il permet de créer un chemin sans boucle dans un environnement commuté et physiquement redondant. STP détecte et désactive ces boucles et fournit un mécanisme de liens de sauvegarde.

Toutefois, si les commutateurs acheminent le trafic de diffusion et multicast par tous les ports sauf celui d'origine et si les trames Ethernet ne disposent pas de durée de vie(TTL), divers problèmes peuvent alors apparaître [48].

- **Fonctionnement du protocole STP**

Le fonctionnement du protocole STP se déroule en 4 étapes :

1. **Élection du Bridge Root :** tous les commutateurs du réseau envoient des messages BPDU (Bridge Protocol Data Unit) pour élire un commutateur qui servira de racine de l'arbre de couverture. Le commutateur ayant l'ID de pont le plus bas sera choisi comme racine.

2. **Établissement de chemins de redondance :** le protocole STP sélectionne un chemin de transmission vers la racine de l'arbre pour chaque commutateur du réseau. Les chemins alternatifs sont mis en état de blocage pour éviter les boucles. Les ports des commutateurs rencontrent cinq états dont le "Blocking" qui ne transfère pas de trames de données et le "Forwarding" qui les transfère.

3. **Détection de changement de topologie :** le protocole STP surveille constamment le réseau pour détecter les changements de topologie, tels que la défaillance d'un commutateur ou la mise en place d'une nouvelle connexion.

Lorsqu'un changement est détecté, le protocole STP recalcule l'arbre de couverture pour s'adapter à la nouvelle topologie.

4. **Rétablissement du réseau** : lorsqu'un commutateur ou une liaison échoue, le protocole STP active un chemin alternatif en débloquant le port correspondant. Egalement, le protocole STP surveille constamment le réseau pour détecter si le problème est résolu et si le chemin principal peut être rétabli.

- **Les fonctionnalités du STP**

❖ **PortFast**

La commande PortFast est une amélioration de Cisco qui permet à un switch de commencer la communication beaucoup plus rapidement. Il se configure uniquement sur les ports du commutateur qui sont en mode accès. Lorsque la fonction PortFast est activée sur un port en mode accès, il contournera les différents états du spanning tree. En gros il passe directement de l'état de blocage à celui de forwarding. Cette option est à utiliser sur les ports connectés à des postes de travail ou à des serveurs pour qu'ils puissent accéder immédiatement au réseau sans avoir à attendre la convergence du spanning tree (50 secondes).

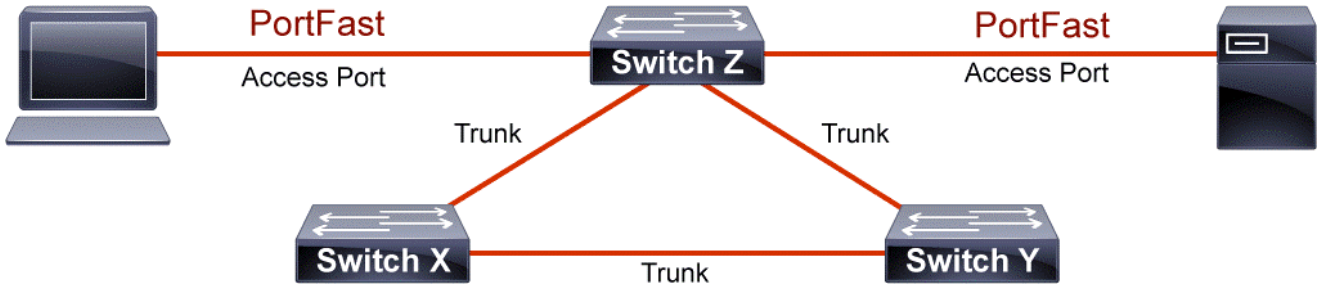


Figure 36: Schéma illustrant le fonctionnement de PortFast [29].

❖ **BPDU Guard**

L'unité de donnée de protocole de pont (Bridge Protocol Data Unit, BPDU) est un paquet de données, envoyé sur les réseaux locaux, qui travaille pour détecter les boucles dans un réseau. Les boucles peuvent provoquer des paquets de données en double pour être envoyés, ce qui peut prendre de la bande passante sur un réseau. BPDU Guard protège les ordinateurs de la réception de paquets de données non autorisées qui pourraient contenir des virus.

Cette fonction doit être activée sur un port qui ne doit jamais recevoir de BPDU de son appareil connecté. Les périphériques finaux ne sont pas censés générer de BPDU, car dans un environnement réseau normal, les messages BPDU sont échangés par des commutateurs réseau. Lorsqu'un port activé par BPDU Guard reçoit BPDU du périphérique connecté, BPDU Guard désactive le port et l'état du port passe à l'état Disabled (down/down, même état qu'en cas de violation de Port-Security).

II.3.7 Le protocole VTP (Vlan trunking Protocol)

C'est un protocole de niveau 2 qui permet d'ajouter, renommer ou supprimer un ou plusieurs réseaux locaux virtuels sur un seul commutateur (le serveur) qui propagera cette nouvelle

configuration à l'ensemble des autres commutateurs du réseau (clients). Le VTP permet ainsi d'éviter toute incohérence de configuration des VLAN sur l'ensemble d'un réseau local [49].

- **Fonctionnement du protocole VTP**

Le VTP possède trois modes de fonctionnement :

❖ **Serveur**

Il est associé à un domaine VTP. La déclaration des VLANs s'effectue sur le serveur. Lorsqu'on modifie la configuration VLAN sur un serveur VTP, que ce soit un ajout, une suppression ou bien une simple modification, elle est propagée sur tous les switches du domaine VTP. Il tient à jour la liste des VLANs déclarés et la diffuse à l'ensemble des clients.

❖ **Client**

Il est associé à un domaine VTP. Il n'est pas possible de modifier la configuration des VLAN. Il reçoit la liste des VLANs, il la propage aux autres clients auxquels il est connecté et met à jour sa propre liste.

❖ **Transparent**

Il n'est associé à aucun domaine VTP. Sa liste de VLAN est locale et n'est pas mise à jour lorsqu'il reçoit une trame VTP. Cependant il propage les listes de VLAN qu'il reçoit.

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

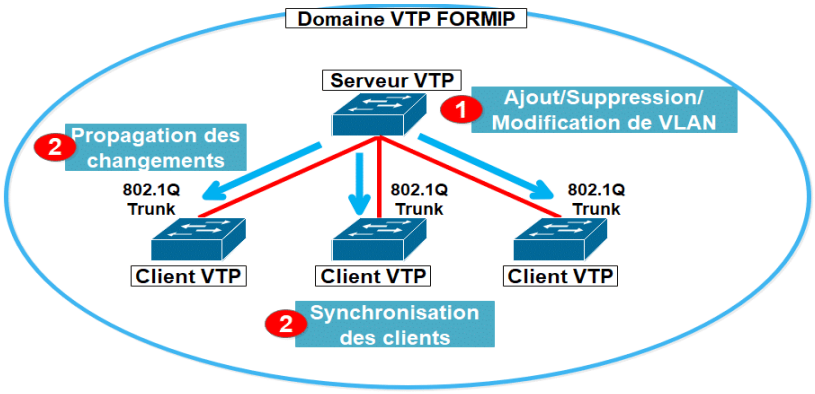


Figure 37: Représentation de fonctionnement de VTP [30].

II.3.8 EtherChannel

La technologie EtherChannel a initialement été développée par Cisco comme une technique de réseau local entre deux commutateurs permettant d'assembler plusieurs liens physiques

Ethernet identiques en un seul lien logique. Cette technologie a pour but d'augmenter la bande passante et d'améliorer la tolérance aux pannes entre les commutateurs, les routeurs et les serveurs [50].

- **Unité de l'EtherChannel**

L'EtherChannel est défini par une agrégation de lien qui a pour principe de combiner plusieurs liens pour avoir un seul lien virtuel de meilleure capacité. Nous allons expliquer son utilité à travers l'exemple suivant :

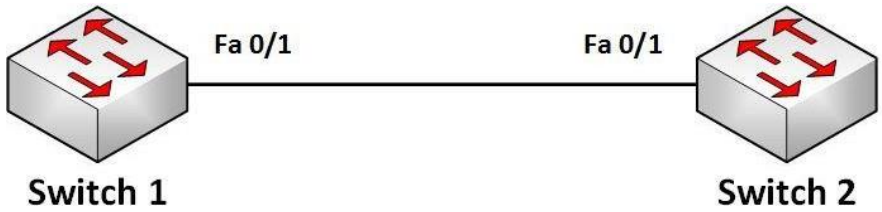


Figure 38: Schéma illustrant l'interconnexion de deux commutateurs sans EtherChannel [31].

Figure 38 montre deux switchers reliés par un seul lien qui communique à une vitesse de 100 Mbit/s. Pour bénéficier d'une meilleure bande passante, une agrégation de lien est mise en place ce qui augmente la capacité à 200 Mbit/s. Néanmoins, sans aucune configuration, STP se chargerait de désactiver l'un des liens. En configurant l'EtherChannel, les deux switches ne représentant plus qu'un seul lien virtuel.

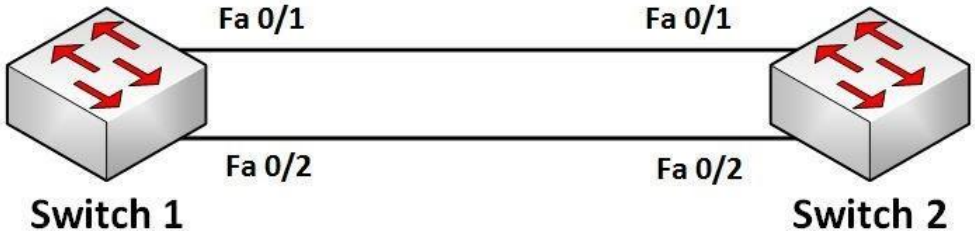


Figure 39:Schéma illustre l'interconnexion de deux commutateurs avec EtherChannel [31].

- **Protocoles d'agrégation de canaux**

Il existe deux protocoles d'agrégation de lien pour configurer un EtherChannel, dits protocoles de négociation :

- **PAgP :** c'est un protocole propriétaire de Cisco, il facilite la création automatique d'une liaison EtherChannel. Les modes PagP sont : on, PagP désirable et PagP auto.

- **LACP :** il fait partie d'une spécification IEEE qui permet également de regrouper plusieurs ports physiques dans un seul canal logique. Les modes LacP sont on, LacP active et LacP passive.

PAgP et LACP ne fonctionnent pas ensemble. Le mode **ON** existe pour PAgP et LACP pour réaliser un EtherChannel de manière inconditionnelle, sans leurs utilisations par défaut, aucun mode n'est configuré.

- **Avantages de l'EtherChannel**

- La plupart des tâches de configuration peuvent être effectuées sur l'interface EtherChannel plutôt que sur chaque port individuel, ce qui assure la cohérence de la configuration à travers les liens.
- L'EtherChannel s'appuie sur les ports de commutation existants afin d'augmenter la bande passante. Aucune mise à niveau matérielle n'est nécessaire.
- L'équilibrage de charge est possible entre les liaisons qui font partie d'un même Etherchannel.
- L'EtherChannel crée une agrégation que STP reconnaît comme une seule liaison logique.
- L'EtherChannel garantit la redondance et la perte d'un lien physique ne génère pas de changement dans la topologie.

II.3.9 Les protocoles de routage

Le routage est le processus qui permet de diriger les paquets de données à travers un réseau de manière efficace et en fonction de leur destination. C'est un élément clé des réseaux informatiques, car il permet d'acheminer les données de manière fiable et rapide d'un point à un autre tout en évitant les congestions ou les temps d'arrêt. Il est utilisé pour connecter des réseaux locaux (LAN) ou des réseaux étendus (WAN) entre eux, et pour permettre à des utilisateurs distants de se connecter aux ressources du réseau.

Le routage consiste à prendre une décision de transmission en fonction des informations de destination contenues dans les en-têtes de paquets de données. Les routeurs sont les équipements du réseau qui effectuent cette tâche. Ils analysent les en-têtes de paquets de données et les transmettent au prochain routeur en fonction des informations de destination [51].

Le routage peut être classé en deux catégories principales :

- **Routage statique :** dans le routage statique, les routes sont configurées manuellement sur chaque routeur. Cette méthode est souvent utilisée pour les réseaux simples ou lorsque la topologie du réseau est stable et ne change pas fréquemment.

- **Routage dynamique :** dans le routage dynamique, les routes sont calculées automatiquement par les routeurs en utilisant des protocoles de routage. Cette méthode est utilisée pour les réseaux complexes ou lorsque la topologie du réseau est susceptible de changer fréquemment.

Il existe plusieurs protocoles de routage, chacun ayant des caractéristiques et des fonctionnalités spécifiques. Les protocoles de routage dynamiques peuvent être classés en deux catégories principales:

II.3.9.1 Protocoles de routage dynamique à vecteur de distance :

Sont des protocoles de routage utilisés pour déterminer les meilleures routes vers les destinations à travers un réseau. Ces protocoles utilisent des informations de distance pour décider du meilleur chemin. Les protocoles de routage à vecteur de distance les plus couramment utilisés sont RIP (Routing Information Protocol) et EIGRP (Enhanced Interior

Gateway Routing Protocol).

➢ **Le protocole EIGRP (Enhanced Interior Gateway Routing Protocol)**

C'est un protocole de routage de niveau 3 utilisé pour échanger des informations de routage entre les routeurs. Il utilise un algorithme de routage à vecteur de distance amélioré pour déterminer les meilleurs chemins vers les réseaux de destination.

EIGRP offre des fonctionnalités de redondance telles que l'équilibrage de charge, la redondance de lien, la redondance de routeurs et l'agrégation des liens pour améliorer la disponibilité et la redondance du réseau. Ces fonctionnalités lui permettent de fournir une haute disponibilité et une faible latence pour les applications critiques [52].

- **Fonctionnement du protocole EIGRP**

1. Les routeurs qui participent au protocole EIGRP échangent des informations de routage entre eux en utilisant des messages de protocole EIGRP.
2. Chaque routeur qui participe au protocole EIGRP maintient une table de routage qui contient des informations sur les réseaux accessibles et les chemins les plus courts pour y accéder.
3. Les routeurs échangent des mises à jour périodiques pour maintenir à jour leur table de routage.
4. EIGRP utilise un algorithme appelé DUAL (Diffusing Update Algorithm) pour calculer les chemins les plus courts vers toutes les destinations.
5. Les chemins les plus courts sont ensuite transmis aux autres routeurs de sorte que chaque routeur dispose d'une vue cohérente de la topologie du réseau.

➢ **Le protocole RIP (Routing Information Protocol)**

Est un protocole de routage à vecteur de distance qui utilise le nombre de sauts comme métrique pour déterminer les chemins de routage les plus courts dans un réseau.

RIP fonctionne en envoyant périodiquement des messages de mise à jour à tous les routeurs voisins, annonçant les réseaux auxquels le routeur est connecté et le nombre de sauts nécessaire pour atteindre chaque réseau. Chaque routeur utilise ces informations pour construire une table de routage et déterminer les meilleurs chemins vers les réseaux de destination.

Bien que RIP soit facile à configurer et à utiliser, il présente quelques limites importantes, notamment une convergence lente, une faible capacité de mise à l'échelle et une faible sécurité. Pour cette raison, RIP est généralement utilisé dans des réseaux de petite taille ou des réseaux privés, et est souvent remplacé par des protocoles de routage plus sophistiqués, tels qu'OSPF et BGP, dans les réseaux plus importants et complexes.

II.3.9.2 Protocoles de routage dynamique à état de lien

Sont l'un des deux principaux types de protocoles de routage dynamique. Contrairement aux protocoles de routage de vecteur de distance, qui ne connaissent que les informations sur les routes directement connectées, les protocoles de routage d'état de lien maintiennent une vue complète de la topologie du réseau. Chaque nœud du réseau (routeur) collecte des informations sur ses voisins et les partage avec les autres nœuds du réseau en diffusant des messages de mise

à jour d'état de lien. Les exemples de protocoles de routage d'état de lien comprennent OSPF.

- **Le protocole OSPF (Open Shortest Patch First)**

C'est un protocole de routage d'état de lien qui est largement utilisé dans les réseaux IP. Il a été développé pour remplacer le protocole de routage de passerelle intérieure (IGRP), qui étaitun protocole de routage propriétaire de Cisco. De plus, OSPF utilise un algorithme de Dijkstra pour trouver la meilleure route de destination et maintenir une table de routage optimisée. Ce qui le rend plus adapté aux réseaux de plus grande taille.

OSPF est conçu pour prendre en charge les réseaux de grandes envergures et complexes. Il fonctionne en collectant des informations sur l'état des liens de tous les nœuds du réseau et en les utilisant pour construire une carte complète de la topologie du réseau permettant une redondance de route et une meilleure résilience du réseau en cas de défaillance [53].

- **Fonctionnement du protocole OSPF**

1. Les routeurs qui participent au protocole OSPF échangent des informations de routage entre eux en utilisant des messages de protocole OSPF.
2. Chaque routeur qui participe au protocole OSPF maintient une base de données topologique qui décrit l'état du réseau.
3. Les routeurs échangent des mises à jour périodiques pour maintenir à jour leur base de données topologique.
4. Les routeurs calculent ensuite les routes les plus courtes vers toutes les destinations enutilisant l'algorithme Dijkstra.
5. Les routes les plus courtes sont ensuite transmises aux autres routeurs de sorte quechaque routeur dispose d'une vue cohérente de la topologie du réseau.

- **Les airs de l'OSPF**

OSPF est un protocole de routage qui utilise la notion d'aires (ou zones) pour organiser les réseaux en fonction de leur taille et de leur topologie. Les interfaces OSPF sont les interfaces de réseau qui sont configurées pour participer au processus OSPF.

Voici une description de chaque type d'aire OSPF :

- **Area 0 :** Aussi connue sous le nom d'aire dorsale ou backbone, cette aire est obligatoirepour tous les réseaux OSPF et relie toutes les autres aires entre elles. Les routeurs dansl'aire 0 ont une vue complète de la topologie de l'ensemble du domaine OSPF.

- **Aire standard :** Une aire standard est une zone qui est connectée à l'aire 0 ou à une autreaire standard. Les routeurs dans une aire standard ne voient que les informations sur lesréseaux de l'aire à laquelle ils sont connectés directement, ainsi que les résumés d'itinéraire envoyés depuis l'aire 0 ou l'aire backbone.

- **Aire sans sommaire (ou aire stub) :** Une aire sans sommaire est une zone qui est connectée à l'aire 0 ou à une autre aire standard, mais qui ne reçoit pas les

résumés d'itinéraire depuis l'aire backbone. Au lieu de cela, un routeur de bordure d'aire (ABR) envoie une route par défaut à tous les routeurs dans l'aire sans sommaire.

- **Aire sans sortie (ou aire totally stubby) :** Une aire sans sortie est une zone qui est connectée à l'aire 0 ou à une autre aire standard, mais qui ne reçoit pas les résumés d'itinéraire depuis l'aire backbone et ne peut pas avoir de routeur de bordure d'aire (ABR) interne. Un ABR externe peut encore envoyer une route par défaut vers l'aire sans sortie.

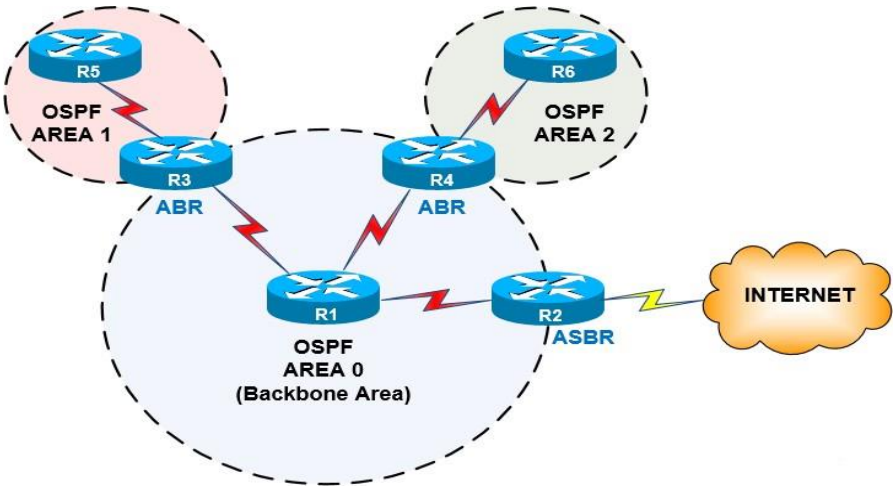


Figure 40: Les aires de l'OSPF [32].

II.4 Conclusion

Dans ce chapitre, nous avons présenté l'organisme d'accueil ainsi que les techniques de redondance réseaux. Tout d'abord, nous avons présenté l'entreprise et ses activités. Ensuite, nous avons discuté des équipements réseau utilisés dans l'entreprise et de leur fonctionnement. Nous avons également souligné l'importance de la disponibilité du réseau pour le bon fonctionnement de l'entreprise.

Nous avons ensuite abordé la question de la redondance des équipements et des liaisons réseau. Nous avons expliqué que la redondance consiste à fournir une solution de secours en cas de défaillance d'un équipement ou d'une liaison. Nous avons décrit les techniques de redondance les plus utilisées, notamment les systèmes de redondance, les liaisons redondantes.

CHAPITRE III. CONCEPTION ET REALISATION

III.1 Introduction

Dans ce chapitre, nous allons explorer la réalisation et la conception d'une simulation d'un réseau informatique redondant sous le simulateur Cisco Packet Tracer.

Ce chapitre se compose de deux parties, la première partie sera consacrée à la mise en œuvre de la redondance au niveau LAN, et la deuxième partie sera consacrée à la redondance au niveau WAN.

Nous allons nous concentrer sur la création d'un réseau redondant qui utilise les technologies VTP, STP, l'EtherChannel, HSRP et enfin l'OSPF, tout en explorant la configuration de VLAN pour isoler le trafic sur le réseau, et à la fin nous allons tester la fiabilité de la solution optée.

III.2 Présentation du simulateur Cisco Packet Tracer

Cisco Packet Tracer est un simulateur de matériel réseau très puissant permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibres optiques). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, pour finalement tester le réseau créé. (Voir annexe 1)

En fin de compte, le simulateur Cisco est un outil précieux qui permet de créer, configurer et tester des configurations réseau avant de les implémenter sur un réseau de production [54].

Figure 41: Simulateur Cisco Packet Tracer [33].

III.3 La mise en place d'un réseau LAN redondant

III.3.1 Optimisation de la conception

Afin de tester la solution proposée, nous avons apporté des améliorations à l'ancienne architecture du Cevital, que nous allons simuler sous Cisco Packet Tracer.

Nous avons apporté des modifications sur les deux couches existantes dans le réseau de l'entreprise, la couche cœur et la couche d'accès, de plus nous avons créé une couche de distribution. Nous avons ajouté deux backbones pour la partie Core celle qui reliera le réseau vers les autres sites et comprendra en elle avec la partie distribution le protocole de routage choisi (OSPF), nous avons aussi mis en œuvre deux backbones dans la partie distribution afin de configurer le protocole de la haute disponibilité HSRP sur ces deux backbones qui eux-mêmes sont reliés en EtherChannel pour une meilleure connectivité et un débit élevé. Pour que cette architecture soit hautement disponible, on doit aussi brancher tous les switches d'accès au premier backbone que nous avons nommé SWD1 ainsi qu'au deuxième que nous avons nommé SWD2. Comme suit :

- **Niveau de la couche cœur :** au niveau de cette couche, nous avons ajouté un Switch cœur SWC2, qui va partager le trafic avec le SWC1, et en cas de panne de l'un des deuxswitches, le trafic sera acheminé par l'autre.

- **Création de la couche distribution :** cette couche ne figure pas sur la topologie du réseau de l'entreprise, nous avons ajouté deux commutateurs entre la couche cœur et la couche accès pour rendre le réseau plus efficace, et avec la redondance, on a doublé les commutateurs avec une double liaison entre les deux pour permettre la fluidité du trafic.

- **Niveau de la couche accès :** Au niveau de cette couche, nous avons repris les switches qui sont reliés en série afin de maintenir un faible diamètre du réseau.

III.3.2 Nouvelle architecture du réseau Cevital

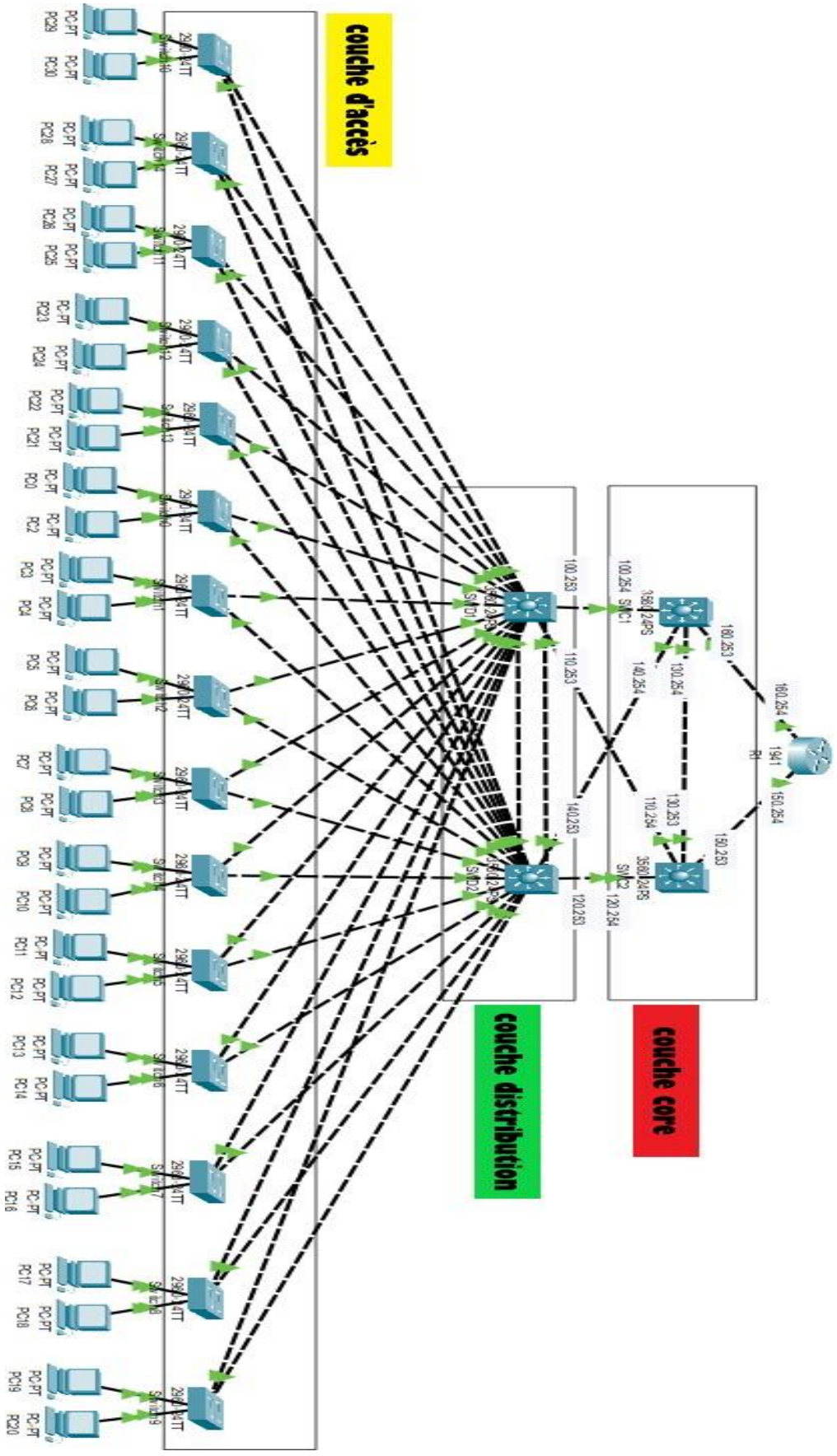


Figure 42: Topologie de la nouvelle architecture du réseau Cevital.

La nouvelle architecture est composée de trois couches : une couche cœur contenant deux commutateurs de niveau 3, une couche distribution composée de deux commutateurs de niveau 3, et une couche d'accès composée de plusieurs commutateurs de niveau 2.

Les deux commutateurs de la couche distribution sont interconnectés par une liaison EtherChannel. Toutes les liaisons de niveau 2 sont en mode trunk (distribution-accès) (Accès-distribution) (distribution-distribution x2), ainsi que l'interface de l'EtherChannel.

Sur la couche distribution on va configurer les protocoles VTP, STP et HSRP qui assurent la bonne gestion et la haute disponibilité du service. Un protocole OSPF sera configuré entre la partie Core et distribution qui vas assurer le bon routage du réseau, et tout ça sera un mi-travaille sans que les périphériques de la couche accès soient interconnectés aux deux switches en redondance pour qu'ils assurent la haute disponibilité dans le cas où l'un des switches de distribution subit un dysfonctionnement ou une coupure d'un des liens d'interconnexion.

III.3.3 Présentation des équipements utilisés

Couche	Equipement du modèle type	Nombre	Nomination
Couche core	Switch Core (Cisco CatalystC6807-XL)	2	SWC1 SWC2
Couche distribution	Switch distribution (Cisco Catalyst C3850-24S)	2	SWD1 SWD2
Couche d'accès	Switch d'accès (Cisco Catalyst C2960)	15	Switch(n)
PC	PC	30	PC(n)
Routeur	Router ISR4331	1	Router

Tableau 5: Les équipements utilisés sur la topologie.

III.3.4 Désignation des interfaces

Equipment local	Equipment distant	Interface(s) local(s)	Interface(s) distante(s)
Router	Core 1	Gig0/0/0	Fa0/4
Router	Core 2	Gig0/0/1	Fa0/4
Core 1	Core 2	Fa0/3	Fa0/3
Core 1	SWD1	Fa0/1	Fa0/18
Core 1	SWD2	Fa0/2	Fa0/19
Core 2	SWD1	Fa0/1	Fa0/19
Core 2	SWD2	Fa0/2	Fa0/18
SWD1	Core 1	Fa0/18	Fa0/1
SWD1	Core 2	Fa0/19	Fa0/1
SWD1	SWD2	Fa0/16-Fa0/17	Fa0/16-Fa0/17
SWD1	Switch0	Fa0/01	Fa0/1
SWD1	Switch1	Fa0/2	Fa0/1
SWD1	Switch2	Fa0/3	Fa0/1
SWD1	Switch3	Fa0/4	Fa0/1
SWD1	Switch4	Fa0/5	Fa0/1
SWD1	Switch5	Fa0/6	Fa0/1
SWD1	Switch6	Fa0/7	Fa0/1
SWD1	Switch7	Fa0/8	Fa0/1
SWD1	Switch8	Fa0/9	Fa0/1

SWD1	Switch9	Fa0/10	Fa0/1
SWD1	Switch10	Fa0/11	Fa0/1
SWD1	Switch11	Fa0/12	Fa0/1
SWD1	Switch12	Fa0/13	Fa0/1
SWD1	Switch13	Fa0/14	Fa0/1
SWD1	Switch14	Fa0/15	Fa0/1
SWD2	Switch0	Fa0/1	Fa0/2
SWD2	Switch1	Fa0/2	Fa0/2
SWD2	Switch2	Fa0/3	Fa0/2
SWD2	Switch3	Fa0/4	Fa0/2
SWD2	Switch4	Fa0/5	Fa0/2
SWD2	Switch5	Fa0/6	Fa0/2
SWD2	Switch6	Fa0/7	Fa0/2
SWD2	Switch7	Fa0/8	Fa0/2
SWD2	Switch8	Fa0/9	Fa0/2
SWD2	Switch9	Fa0/10	Fa0/2
SWD2	Switch10	Fa0/11	Fa0/2
SWD2	Switch11	Fa0/12	Fa0/2
SWD2	Switch12	Fa0/13	Fa0/2
SWD2	Switch13	Fa0/14	Fa0/2
SWD2	Switch14	Fa0/15	Fa0/2

Tableau 6: Désignation des interfaces.

III.3.5 Vlans de l'entreprise

Direction	VLAN	DHCP	Root	IP SWD1	IP SWD2	Passerelle
DRH	VLAN10	Dynamique	SWD1	10.10.10.252	10.10.10.253	10.10.10.254
Direction des Appro	VLAN11	Dynamique	SWD1	10.10.11.252	10.10.11.253	10.10.11.254
DSI	VLAN12	Dynamique	SWD1	10.10.12.252	10.10.12.253	10.10.12.254
Raff Huile	VLAN13	Dynamique	SWD1	10.10.13.252	10.10.13.253	10.10.13.254
Raff sucre 3000T	VLAN14	Dynamique	SWD1	10.10.14.252	10.10.14.253	10.10.14.254
Division utilités	VLAN15	Dynamique	SWD1	10.10.15.252	10.10.15.253	10.10.15.254
Supply-chain	VLAN16	Dynamique	SWD1	10.10.16.252	10.10.16.253	10.10.16.254
Unité margarinerie	VLAN17	Dynamique	SWD1	10.10.17.252	10.10.17.253	10.10.17.254
Printer	VLAN18	Statique	SWD1	10.10.18.252	10.10.18.253	10.10.18.254
Téléphone	VLAN20	Dynamique	SWD1	10.10.20.252	10.10.20.253	10.10.20.254
Voice	VLAN21	Dynamique	SWD1	10.10.21.252	10.10.21.253	10.10.21.254
Direction R&D	VLAN22	Dynamique	SWD1	10.10.22.252	10.10.22.253	10.10.22.254
Performance industriel	VLAN23	Dynamique	SWD2	10.10.23.252	10.10.23.253	10.10.23.254
Unité Cdt Huile	VLAN24	Dynamique	SWD2	10.10.24.252	10.10.24.253	10.10.24.254
Managemen t switch	VLAN25	Statique	SWD2	10.10.25.252	10.10.25.253	10.10.25.254
DFC	VLAN26	Dynamique	SWD2	10.10.26.252	10.10.26.253	10.10.26.254

Commercial	VLAN27	Dynamique	SWD2	10.10.27.252	10.10.27.253	10.10.27.254
Direction générale	VLAN28	Dynamique	SWD2	10.10.28.252	10.10.28.253	10.10.28.254
Direction qualité et management système	VLAN 29	Dynamique	SWD2	10.10.29.252	10.10.29.253	10.10.29.254
Raff sucre 3500T	VLAN 30	Dynamique	SWD2	10.10.30.252	10.10.30.253	10.10.30.254
Cdt sucre	VLAN 31	Dynamique	SWD2	10.10.31.252	10.10.31.253	10.10.31.254
Caméra	VLAN 32	Statique	SWD2	10.10.32.252	10.10.32.253	10.10.32.254
Projets	VLAN 33	Dynamique	SWD2	10.10.33.252	10.10.33.253	10.10.33.254
Trituration	VLAN 36	Dynamique	SWD2	10.10.36.252	10.10.36.253	10.10.36.254

Tableau 7: Les Vlans de l'entreprise.

III.3.6 Adresses IP des interfaces du niveau 3

Equipement	Interface	Adresse IP
SWD1	Fa0/18	10.10.100.253/30
SWD1	Fa0/19	10.10.110.253/30
SWD2	Fa0/18	10.10.120.253/30
SWD2	Fa0/19	10.10.140.253/30
SWC1	Fa0/1	10.10.100.254/30
SWC1	Fa0/2	10.10.140.254/30
SWC1	Fa0/3	10.10.130.254/30
SWC1	Fa0/4	10.10.160.253/30
SWC2	Fa0/1	10.10.110.254/30
SWC2	Fa0/2	10.10.120.254/30
SWC2	Fa0/3	10.10.130.253/30
SWC2	Fa0/4	10.10.150.253/30
R1	gig0/0/0	10.10.160.254/30
R1	gig0/0/1	10.10.150.254/30

Tableau 8: Adresses IP des interfaces du niveau 3.

III.3.7 Configuration des équipements utilisés

Une fois les équipements sont interconnectés, nous allons appliquer une série de configuration sur tous les périphériques afin de réaliser un réseau redondant. Pour sauvegarder les configurations appliquées nous allons utiliser la commande « **copy running-config startup-config».**

III.3.7.1 Configuration de base

La même configuration de base sera effectuée sur le routeur, les Switches Cores, les Switches de distribution SWD1 et SWD2.

III.3.7.1.1 Hostname

Pour reconnaître nos équipements, nous commençons par attribuer des noms significatifs avec la commande **« hostname ».**

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch (config) #hostname SWD1
```

Listing 1:Attribution du nom SWD1 au switch distribution1.

III.3.7.1.2 Configuration de la ligne Console

Pour sécuriser l'accès aux périphériques nous avons attribué un mot de passe « Cevital » pour la ligne console de chaque commutateur de niveau 2 et 3.

```
SWD1 (config)#line con 0
SWD1 (config-line)#password cevital
SWDI (config-line) #login
SWD1 (config-line)#exit
```

Listing 2: Configuration de ligne console.

III.3.7.1.3 Sécurisation du mode privilégié

Nous avons attribué un mot de passe « Cevital » pour l'accès au mode privilégié.

```
SWD1 (config)#enable password Cevital
```

Listing 3: Attribution d'un mot de passe pour l'accès au mode privilégié

III.3.7.1.4 Sécurisation des mots de passe

Les mots de passe apparaissent en clair lors de l'affichage du fichier de configuration. Nous allons donc activer le service **password-encryption** afin de sécuriser les équipements.

```
SWD1 (config) #service password encryption
```

Listing 4: Sécurisation des mots de passe.

III.3.7.1.5 Configuration d'une bannière

Nous avons utilisé une bannière de type « banner motd » qui indique que cet accès est interdit aux utilisateurs non autorisés (Hackers).

```
SWD1 (config) #banner mot " Acces aux personnes autorisees "
```

Listing 5:Configuration d'une bannière motd.

- **Vérification des configurations de base**

La commande **« show running-config »** nous permet de vérifier l'ensemble des configurations effectuées sur l'équipement**.**

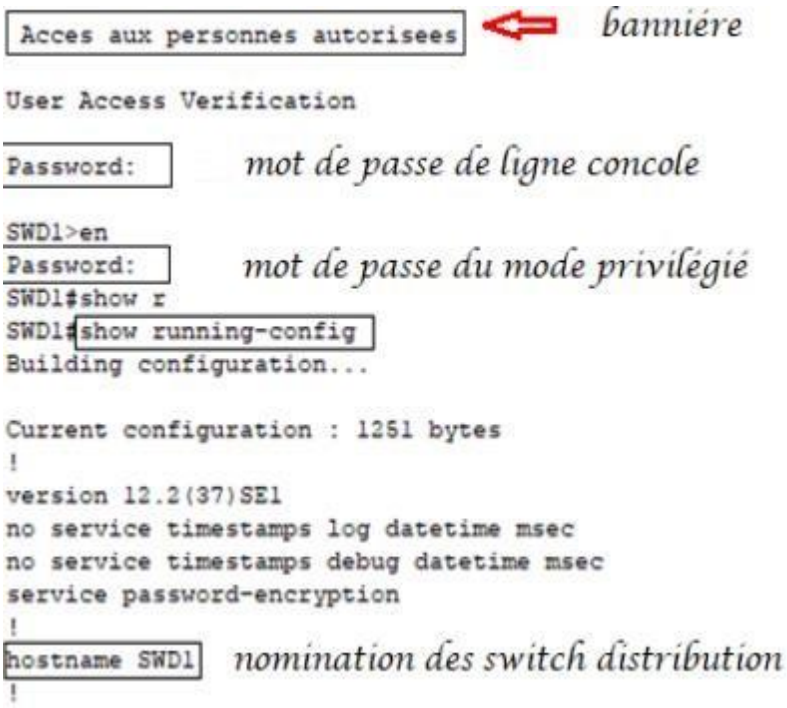


Figure 43:Vérification des configurations de base.

III.3.7.1.6 Sécurisation d'accès à distance avec SSH (Secure Socket Shell)

SSH est largement utilisé par les administrateurs réseau pour gérer à distance les systèmes et les applications en toute sécurité, car il leur permet de se connecter à un autre ordinateur sur un réseau, d'exécuter des commandes et de déplacer des fichiers d'un ordinateur à un autre.

Nous allons activer le SSH sur les commutateurs de la couche cœur et distribution. Voici un exemple des étapes de configuration sur le switch SWD1.

```
SWD1 (config) #username Admin password cevitalAgro
SWD1 (config)#ip domain-name cisco.com
SWD1 (config)#crypto key generate rsa
The name for the keys will be: SWD1.cisco.com
Choose the size of the key modulus in the range of 360 to 2048
for your General Purpose Keys. Choosing a key modulus greater
than 512 may take a few minutes.
How many bits in the modulus [512]: 1024
%Generating 1024 bit RSA keys, keys will be non-exportable.
.. [OK]
SWD1 (config)#line vty 04
*Mar 1 0:4:12.236: ASSH-5-ENABLED: SSH 1.99 has been enabled
SWD1 (config-line) #transport input ssh
SWD1 (config-line) #login
```

Listing 6:Configuration du SSH sur SWD1.

III.3.7.2 Configuration des liaisons Trunk

Dans cette section nous allons configurer les liaisons entre les switches de distribution et les switches d'accès (Niveau 2) en mode trunk afin que ces derniers communiquent et transmettent

entre eux les Vlans configurés dans les switches de distribution. La commande **« interface range »** va nous permettre de regrouper les interfaces de chaque switch.

- **Sur SWD1 :**

```
SWD1#configure terminal
Enter configuration commands, one per line. End with CNIL/Z.
SWD1 (config) #interface range fa0/1-17
SWD1 (config-if-range)#switchport trunk encapsulation dot1q
SWD1 (config-if-range)#switchport mode trunk
```

Listing 7:Configuration du trunk sur SWD1.

- **Sur SWD2 :**

```
SWD2#configure terminal
Enter configuration commands, one per line. End with CNIL/Z.
SWD2 (config) #interface range fa0/1-17
SWD2 (config-if-range)#switchport trunk encapsulation dot1q
SWD2 (config-if-range) #switchport mode trunk
```

Listing 8:Configuration du Trunk sur SWD2.

- **Sur les switches d'accès :**

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNIL/Z.
Switch (config)#interface range fa0/1-2
Switch (config-if-range) #switchport mode trunk
Switch (config-if-range)#exit
```

Listing 9:Configuration du Trunk sur switch d'accès.

- **Vérification des liaisons Trunk**

Avec la commande **« show running-config »** sur SWD1 et SWD2 :

```
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

Figure 44:Vérification des liens Trunks.

III.3.7.3 Configuration des liens EtherChannel

Dans l'architecture, nous avons opté pour une agrégation des liens FastEthernet entre les deux switches de distribution SWD1 et SWD2, on a donc mis les deux ports fastEthernet dans un groupe en précisant le mode ON, ensuite on les a mis en mode trunk comme la figure ci-dessous le montre :

La même configuration sera réalisée sur SWD1 et SWD2.

```
SWD1 (config)#interface range fa0/16-17
SWD1 (config-if-range)#channel-group 1 mode on
Creating a port-channel interface Port-channel 1 §LINK-5-
CHANGED: Interface Port-channell, changed state to up
§LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1,
changed state to up
SWD1 (config-if-range)#exit
SWD1 (config) #interface port-channel 1
SWD1 (config-if)#switchport trunk encapsulation dot1q
SWD1 (config-if)#switchport mode trunk
```

Listing 10:Configuration de l'Etherchannel.

- **Vérification de l'EtherChannel**

Avec la commande **« show etherchannel summary »** :

```
SWD1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)           -      Fa0/16(P) Fa0/17(P)
```

Figure 45:Vérification de l'EtherChannel.

III.3.7.4 Configuration des VLANs

- **Création des Vlans de l'entreprise**

Nous allons créer tous les VLANs de l'entreprise sur le switch distribution 1 (SWD1). Prenons exemple pour le Vlan 10 et 11comme sur la figure suivante :

```
SWD1#configure terminal
Enter configuration commands, one per line. End with CNIL/Z.
SWD1 (config) #vlan 10
SWD1 (config-vlan) #name DRH
SWD1 (config-vlan)#exit
SWD1 (config) #vlan 11
SWD1 (config-vlan) #name Direction-Appro
SWD1 (config-vlan) #exit
```

Listing 11:Création des Vlans sur SWD1.

- **Vérification de la création des Vlans**

Avec la commande **« show vlan brief »**

```
SWD1#show vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                   Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                   Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                   Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   DRH                                 active
11   Direction-Appro                     active
12   DSI                                 active
13   Raff-Huille                         active
14   Raff-sucre-300T                     active
15   Division-Utilites                   active
16   Supply-chain                        active
17   Unite-margarinerie                  active
18   Printer                             active
20   telephone                           active
21   voice                               active
22   Direction-RD                        active
23   performance-industriel              active
24   Unite-Cdt-Huile                     active
25   Management-Switch                   active
26   DFC                                 active
27   Commercial                          active
28   Direction-generale                  active
29   Direction-qualite-et-management-systeme active
30   Raff-sucre-3500T                    active
31   Cdt-sucre                           active
32   camera                              active
33   projets                             active
36   Trituration                         active
```

Figure 46:Vérification de la création des Vlans sur SWD1.

III.3.7.5 Configuration du VTP (Vlan Trunking Protocol)

Afin de profiter des services VTP (création, suppression, modification des Vlans), Nous allons donc configurer le switch de distribution « SWD1 » en mode Serveur et lui attribué un nom de domaine ainsi un mot de passe, et le reste des switches en mode Client afin que les Vlans se propagent du SDW1 vers les autres switches. Pour cela nous allons procéder comme suit :

- Configurer le SWD1 en VTP serveur :

```
SWD1 (config) #vtp mode server
Device mode already VTP SERVER.
SWD1 (config) #vtp version 2
SWD1 (config) #vtp domain cevital.com
Changing VIP domain name from NULL to cevital.com
SWD1 (config) #vtp password cisco
Setting device VAN database password to cisco
```

Listing 12:configuration du VTP server sur SWD1.

- Configurer tous les switches restants en mode VTP client :

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNIL/Z.
Switch (config)#vtp mode client
```

```
Setting device to VTP CLIENT mode.
Switch (config)#vtp domain cevital.com
Domain name already set to cevital.com.
Switch (config)#Vtp password cisco
Setting device VLAN database password to cisco
```

Listing 13:configuration du VTP client.

- **Vérification du VTP**

Avec la commande **« show vtp status »** :

```
SWD1#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : cevital.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0005.5E31.ED00
Configuration last modified by 0.0.0.0 at 3-1-93 01:57:54
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          : 29
Configuration Revision            : 0
MD5 digest                        : 0x9B 0xBC 0x74 0x85 0x1C 0xA5 0x58 0x69
                                    0xC2 0x4B 0xF2 0xCC 0x50 0x05 0xC4 0x36
```

Figure 47:vérification du VTP sur SWD1.

```
Switch#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : cevital.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0002.1681.2C00
Configuration last modified by 0.0.0.0 at 3-1-93 01:57:54

Feature VLAN :
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 29
Configuration Revision            : 0
MD5 digest                        : 0x9B 0xBC 0x74 0x85 0x1C 0xA5 0x58 0x69
                                    0xC2 0x4B 0xF2 0xCC 0x50 0x05 0xC4 0x36
```

Figure 48:vérification du VTP client sur switch d'accès.

- **Vérification de la propagation des Vlans sur les switches clients**

Avec la commande « show vlan brief » :

```
SWD2#show vlan brief

VLAN Name                                Status
---- ----------------------------------- -------
1    default                             active

10   DRH                                 active
11   direction-des-appro                 active
12   DSI                                 active
13   raff-huile                          active
14   raff-sucre-3000T                    active
15   division-utilits                    active
16   supply-chain                        active
17   unite-margarinerie                  active
18   printer                             active
20   telephone                           active
21   voice                               active
22   direction-R&D                       active
23   performance-industriel              active
24   unite-Cdt-huile                     active
25   management-switch                   active
26   DFC                                 active
27   commercial                          active
28   direction-generale                  active
29   direction-qualit-management         active
30   Raff-sucre-3500T                    active
31   Cdt-sucre                           active
32   camera                              active
33   projets                             active
36   trituration                         active
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active
```

```
Switch#show vlan brief

VLAN Name                                Status
---- ----------------------------------- -------
1    default                             active

10   DRH                                 active
11   Direction-Appro                     active
12   DSI                                 active
13   Raff-Huille                         active
14   Raff-sucre-300T                     active
15   Division-Utilites                   active
16   Supply-chain                        active
17   Unite-margarinerie                  active
18   Printer                             active
20   telephone                           active
21   voice                               active
22   Direction-RD                        active
23   performance-industriel              active
24   Unite-Cdt-Huile                     active
25   Management-Switch                   active
26   DFC                                 active
27   Commercial                          active
28   Direction-generale                  active
29   Direction-qualite-et-management-systeme
30   Raff-sucre-3500T                    active
31   Cdt-sucre                           active
32   camera                              active
33   projets                             active
36   Trituration                         active
```

Figure 49: Propagation des Vlans sur SWD2 et switch d'accès.

III.3.7.6 Configuration du STP

Pour faciliter la mise en place d'un chemin logique sans boucle sur l'ensemble du domaine de diffusion et assurer la redondance entre la couche distribution et la couche d'accès, nous allons configurer le protocole STP.

Nous allons configurer la moitié des Vlans (10-22) en Root Bridge sur SWD1 et l'autre moitié des Vlans (23-36) en Root Bridge sur SWD2.

- **Sur SWD1 :**

```
SWD1>enable
SWD1#configure terminal
Enter configuration commands, one per line. End with CNIL/Z.
SWD2 (config) #spanning-tree mode pvst
SWD1 (config) #spanning-tree vlan 10-22 root primary
SWD1 (config) #spanning-tree vlan 23-36 root secondary
```

Listing 14: Configuration du STP sur SWD1.

- **Sur SWD2 :**

```
SWD2>enable
SWD2#configure terminal
Enter configuration commands, one per line.
End with CNIL/Z.
SWD2 (config) #spanning-tree mode pvst
SWD2 (config) #spanning-tree vlan 23-36 root primary
SWD2 (config) #spanning-tree vlan 10-22 root secondary
```

Listing 15: Configuration du STP sur SWD2.

➢ **Vérification du STP**

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

- **Sur SWD1 :**

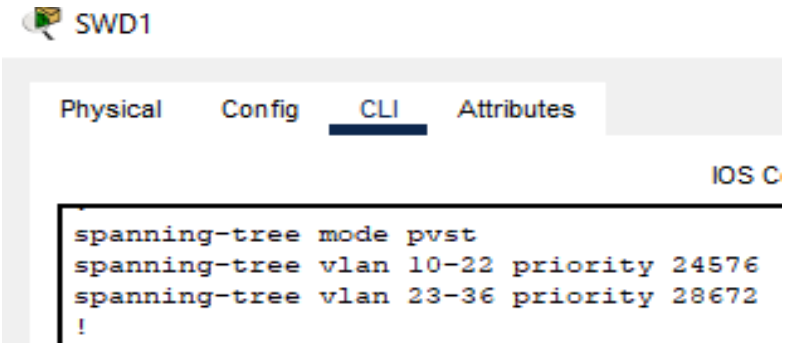


Figure 50: Vérification du STP sur SWD1.

- **Sur SWD2 :**

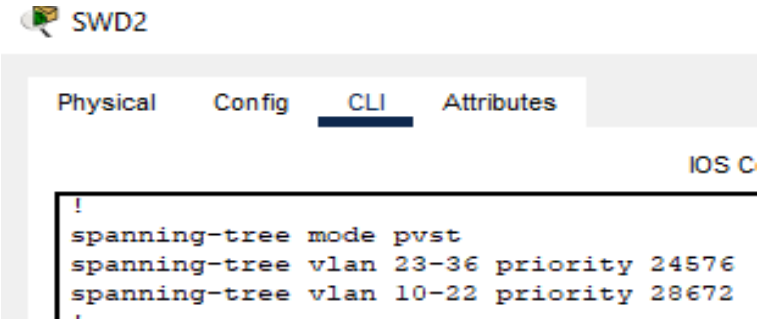


Figure 51: Vérification du STP sur SWD2.

III.3.7.7 Configuration des SVI (Switch Virtual Interface)

Nous allons configurer les SVI de chaque vlan, autrement dit, nous allons attribuer une adresses IP virtuel pour chaque vlan sur les deux switches de distribution SWD1 avec 252 sur la partie machine de chaque vlan et SWD2 avec 253 sur la partie machine de chaque vlan.

- **Sur SWD1 :**

```
SWD1#configure terminal
Enter configuration commands, one per line.
End with CNIL/Z.
SWD1 (config) #interface vlan10
SWD1 (config-if) #
ELINK-5-CHANGED: Interface Vlan10, changed state to up
$LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed
state to up
SWD1 (config-if)#ip address 10.10.10.252 255.255.255.0
SWD1 (config-if)#no shutdown
SWD1 (config-if)#exit
```

Listing 16: Configuration des SVI sur SWD1.

- **Sur SWD2 :**

```
SWD2>enable
SWD2#configure terminal
Enter configuration commands, one per line.
End with CNIL/Z.
SWD2 (config)#interface vlan10
SWD2 (config-if)#ip address 10.10.10.253 255.255.255.0
SWD2 (config-if)#no shutdown
SWD2 (config-if)#exit
```

Listing 17: Configuration des SVI sur SWD2.

- **Vérification des SVI sur SW1 et SW2**

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

```
interface Vlan10
 mac-address 0060.5ca5.5401
 ip address 10.10.10.252 255.255.255.0
!
interface Vlan11
 mac-address 0060.5ca5.5402
 ip address 10.10.11.252 255.255.255.0
!
interface Vlan12
 mac-address 0060.5ca5.5403
 ip address 10.10.12.252 255.255.255.0
!
interface Vlan13
 mac-address 0060.5ca5.5404
 ip address 10.10.13.252 255.255.255.0
!
interface Vlan14
 mac-address 0060.5ca5.5405
 ip address 10.10.14.252 255.255.255.0
!
interface Vlan15
 mac-address 0060.5ca5.5406
 ip address 10.10.15.252 255.255.255.0
!
interface Vlan16
 mac-address 0060.5ca5.5407
 ip address 10.10.16.252 255.255.255.0
!
interface Vlan17
 mac-address 0060.5ca5.5408
 ip address 10.10.17.252 255.255.255.0
```

```
interface Vlan18
 mac-address 0007.ec60.c909
 ip address 10.10.18.253 255.255.255.0
!
interface Vlan20
 mac-address 0007.ec60.c90a
 ip address 10.10.20.253 255.255.255.0
!
interface Vlan21
 mac-address 0007.ec60.c90b
 ip address 10.10.21.253 255.255.255.0
!
interface Vlan22
 mac-address 0007.ec60.c90c
 ip address 10.10.22.253 255.255.255.0
!
interface Vlan23
 mac-address 0007.ec60.c90d
 ip address 10.10.23.253 255.255.255.0
!
interface Vlan24
 mac-address 0007.ec60.c90e
 ip address 10.10.24.253 255.255.255.0
!
interface Vlan25
 mac-address 0007.ec60.c90f
 ip address 10.10.25.253 255.255.255.0
!
interface Vlan26
 mac-address 0007.ec60.c910
 ip address 10.10.26.253 255.255.255.0
```

Figure 52: Vérification des SVI sur SWD1 et SWD2.

III.3.7.8 Configuration du DHCP

III.3.7.8.1 Exclusion des adresses IP

Pour faciliter la gestion et l'attribution des adresses IP pour chaque hôte du réseau, nous allons utiliser le protocole DHCP, ce dernier permet de configurer les paramètres de chaque hôte et le laissera profiter d'un adressage dynamique. La configuration se fera au niveau des switches de distribution SWD1 et SWD2. Afin de réussir ce protocole, et de permettre aux deux switches de distribution d'attribuer des adresses au même temps sans conflit, nous allons exclure les adresses de 128 à 254 sur le SWD1, c'est-à-dire le SWD1 va attribuer les adresses allant de 1 jusqu'à 127 et nous allons exclure les adresses de 1 à 127 et de 252 à 254 sur SWD2 c'est-à-dire le SWD2 va attribuer les adresses allant de 128 à 251.

- **Sur SWD1, exclusion des adresses IP de 128 à 254 :**

```
SWD1>enable
SWD1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWD1 (config)#ip dhcp excluded-address 10.10.10.128 10.10.10.254
SWD1 (config)#ip dhcp excluded-address 10.10.11.128 10.10.11.254
SWD1 (config)#ip dhcp excluded-address 10.10.12.128 10.10.12.254
SWD1 (config)#ip dhcp excluded-address 10.10.13.128 10.10.13.254
SWD1 (config)#ip dhcp excluded-address 10.10.14.128 10.10.14.254
SWD1 (config)#ip dhcp excluded-address 10.10.15.128 10.10.15.254
SWD1 (config)#ip dhcp excluded-address 10.10.16.128 10.10.16.254
SWD1 (config)#ip dhcp excluded-address 10.10.17.128 10.10.17.254
SWD1 (config)#ip dhcp excluded-address 10.10.18.128 10.10.18.254
SWD1 (config)#ip dhcp excluded-address 10.10.18.128 10.10.18.254
SWD1 (config)#ip dhcp excluded-address 10.10.20.128 10.10.20.254
SWD1 (config)#ip dhcp excluded-address 10.10.21.128 10.10.21.254
SWD1 (config)#ip dhcp excluded-address 10.10.22.128 10.10.22.254
SWD1 (config)#ip dhcp excluded-address 10.10.23.128 10.10.23.254
SWD1 (config)#ip dhcp excluded-address 10.10.24.128 10.10.24.254
SWD1 (config)#ip dhcp excluded-address 10.10.25.128 10.10.25.254
SWD1 (config)#ip dhcp excluded-address 10.10.26.128 10.10.26.254
SWD1 (config)#ip dhcp excluded-address 10.10.27.128 10.10.27.254
SWD1 (config)#ip dhcp excluded-address 10.10.28.128 10.10.28.254
SWD1 (config)#ip dhcp excluded-address 10.10.29.128 10.10.29.254
SWD1 (config)#ip dhcp excluded-address 10.10.30.128 10.10.30.254
SWD1 (config)#ip dhcp excluded-address 10.10.31.128 10.10.31.254
SWD1 (config)#ip dhcp excluded-address 10.10.32.128 10.10.32.254
SWD1 (config)#ip dhcp excluded-address 10.10.33.128 10.10.33.254
SWD1 (config)#ip dhcp excluded-address 10.10.36.128 10.10.36.254
```

Listing 18: Exclusion des adresses DHCP sur SWD1.

- **Sur SWD2, exclusion des adresses IP de 1 à 127 :**

```
SWD2#configure terminal
Enter configuration commands, one per line. End with NIL/Z.
 SWD2 (config)#ip dhcp excluded-address 10.10.10.1 10.10.10.127
 SWD2 (config)#ip dhcp excluded-address 10.10.11.1 10.10.11.127
 SWD2 (config)#ip dhcp excluded-address 10.10.12.1 10.10.12.127
```

```
SWD2 (config)#ip dhcp excluded-address 10.10.13.1 10.10.13.127
SWD2 (config)#ip dhcp excluded-address 10.10.14.1 10.10.14.127
SWD2 (config)#ip dhcp excluded-address 10.10.15.1 10.10.15.127
SWD2 (config)#ip dhcp excluded-address 10.10.16.1 10.10.16.127
SWD2 (config)#ip dhcp excluded-address 10.10.17.1 10.10.17.127
SWD2 (config)#ip dhcp excluded-address 10.10.18.1 10.10.18.127
SWD2 (config)#ip dhcp excluded-address 10.10.20.1 10.10.20.127
SWD2 (config)#ip dhcp excluded-address 10.10.21.1 10.10.21.127
SWD2 (config)#ip dhcp excluded-address 10.10.22.1 10.10.22.127
SWD2 (config)#ip dhcp excluded-address 10.10.23.1 10.10.23.127
SWD2 (config)#ip dhcp excluded-address 10.10.24.1 10.10.24.127
SWD2 (config)#ip hhcp excluded-address 10.10.25.1 10.10.25.127
SWD2 (config)#ip dhcp excluded-address 10.10.26.1 10.10.26.127
SWD2 (config)#ip dhcp excluded-address 10.10.27.1 10.10.27.127
SWD2 (config)#ip dhcp excluded-address 10.10.28.1 10.10.28.127
SWD2 (config)#ip dhcp excluded-address 10.10.29.1 10.10.29.127
SWD2 (config)#ip dhcp excluded-address 10.10.30.1 10.10.30.127
SWD2 (config)#ip dhcp excluded-address 10.10.31.1 10.10.31.127
SWD2 (config)#ip dhcp excluded-address 10.10.32.1 10.10.32.127
SWD2 (config)#ip dhcp excluded-address 10.10.33.1 10.10.33.127
SWD2 (config)#ip dhcp excluded-address 10.10.36.1 10.10.36.127
```

Listing 19: Exclusion des adresses DHCP de 1 à 127 sur SWD2.

- **Sur SWD2, exclusion des adresses IP de 252 à 254 :**

```
SWD2 (config)#ip dhcp excluded-address 10.10.10.252 10.10.10.254
SWD2 (config)#ip dhcp excluded-address 10.10.11.252 10.10.11.254
SWD2 (config)#ip dhcp excluded-address 10.10.12.252 10.10.12.254
SWD2 (config)#ip dhcp excluded-address 10.10.13.252 10.10.13.254
SWD2 (config)#ip dhcp excluded-address 10.10.14.252 10.10.14.254
SWD2 (config)#ip dhcp excluded-address 10.10.15.252 10.10.15.254
SWD2 (config)#ip dhcp excluded-address 10.10.16.252 10.10.16.254
SWD2 (config)#ip dhcp excluded-address 10.10.17.252 10.10.17.254
SWD2 (config)#ip dhcp excluded-address 10.10.18.252 10.10.18.254
SWD2 (config)#ip dhcp excluded-address 10.10.20.252 10.10.20.254
SWD2 (config)#ip dhcp excluded-address 10.10.21.252 10.10.21.254
SWD2 (config)#ip dhcp excluded-address 10.10.22.252 10.10.22.254
SWD2 (config)#ip dhcp excluded-address 10.10.23.252 10.10.23.254
SWD2 (config)#ip dhcp excluded-address 10.10.24.252 10.10.24.254
SWD2 (config)#ip dhcp excluded-address 10.10.25.252 10.10.25.254
SWD2 (config)#ip dhcp excluded-address 10.10.26.252 10.10.26.254
SWD2 (config)#ip dhcp excluded-address 10.10.27.252 10.10.27.254
SWD2 (config)#ip dhcp excluded-address 10.10.28.252 10.10.28.254
SWD2 (config)#ip dhcp excluded-address 10.10.29.252 10.10.29.254
SWD2 (config)#ip dhcp excluded-address 10.10.30.252 10.10.30.254
SWD2 (config)#ip dhcp excluded-address 10.10.31.252 10.10.31.254
SWD2 (config)#ip dhcp excluded-address 10.10.32.252 10.10.32.254
SWD2 (config)#ip dhcp excluded-address 10.10.33.252 10.10.33.254
SWD2 (config)#ip dhcp excluded-address 10.10.36.252 10.10.36.254
```

Listing 20: Exclusion des adresses DHCP de 252 à 254 sur SWD2.

➢ **Vérification des adresses exclues**

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

- **Sur SWD1 :**

```
ip dhcp excluded-address 10.10.10.128 10.10.10.254
ip dhcp excluded-address 10.10.11.128 10.10.11.254
ip dhcp excluded-address 10.10.12.128 10.10.12.254
ip dhcp excluded-address 10.10.13.128 10.10.13.254
ip dhcp excluded-address 10.10.14.128 10.10.14.254
ip dhcp excluded-address 10.10.15.128 10.10.15.254
ip dhcp excluded-address 10.10.16.128 10.10.16.254
ip dhcp excluded-address 10.10.17.128 10.10.17.254
ip dhcp excluded-address 10.10.18.128 10.10.18.254
ip dhcp excluded-address 10.10.20.128 10.10.20.254
ip dhcp excluded-address 10.10.21.128 10.10.21.254
ip dhcp excluded-address 10.10.22.128 10.10.22.254
ip dhcp excluded-address 10.10.23.128 10.10.23.254
ip dhcp excluded-address 10.10.24.128 10.10.24.254
ip dhcp excluded-address 10.10.25.128 10.10.25.254
ip dhcp excluded-address 10.10.26.128 10.10.26.254
ip dhcp excluded-address 10.10.27.128 10.10.27.254
ip dhcp excluded-address 10.10.28.128 10.10.28.254
ip dhcp excluded-address 10.10.29.128 10.10.29.254
ip dhcp excluded-address 10.10.30.128 10.10.30.254
ip dhcp excluded-address 10.10.31.128 10.10.31.254
ip dhcp excluded-address 10.10.32.128 10.10.32.254
ip dhcp excluded-address 10.10.33.128 10.10.33.254
ip dhcp excluded-address 10.10.36.128 10.10.36.254
```

Figure 53: Vérification des adresses exclues sur SWD1.

- **Sur SWD2 :**

```
ip dhcp excluded-address 10.10.10.1 10.10.10.127
ip dhcp excluded-address 10.10.11.1 10.10.11.127
ip dhcp excluded-address 10.10.12.1 10.10.12.127
ip dhcp excluded-address 10.10.13.1 10.10.13.127
ip dhcp excluded-address 10.10.14.1 10.10.14.127
ip dhcp excluded-address 10.10.15.1 10.10.15.127
ip dhcp excluded-address 10.10.16.1 10.10.16.127
ip dhcp excluded-address 10.10.17.1 10.10.17.127
ip dhcp excluded-address 10.10.18.1 10.10.18.127
ip dhcp excluded-address 10.10.20.1 10.10.20.127
ip dhcp excluded-address 10.10.21.1 10.10.21.127
ip dhcp excluded-address 10.10.22.1 10.10.22.127
ip dhcp excluded-address 10.10.23.1 10.10.23.127
ip dhcp excluded-address 10.10.24.1 10.10.24.127
ip dhcp excluded-address 10.10.25.1 10.10.25.127
ip dhcp excluded-address 10.10.26.1 10.10.26.127
ip dhcp excluded-address 10.10.27.1 10.10.27.127
ip dhcp excluded-address 10.10.28.1 10.10.28.127
ip dhcp excluded-address 10.10.29.1 10.10.29.127
ip dhcp excluded-address 10.10.30.1 10.10.30.127
ip dhcp excluded-address 10.10.31.1 10.10.31.127
ip dhcp excluded-address 10.10.32.1 10.10.32.127
ip dhcp excluded-address 10.10.33.1 10.10.33.127
ip dhcp excluded-address 10.10.36.1 10.10.36.127
ip dhcp excluded-address 10.10.10.252 10.10.10.254
ip dhcp excluded-address 10.10.11.252 10.10.11.254
ip dhcp excluded-address 10.10.12.252 10.10.12.254
ip dhcp excluded-address 10.10.13.252 10.10.13.254
ip dhcp excluded-address 10.10.14.252 10.10.14.254
ip dhcp excluded-address 10.10.15.252 10.10.15.254
ip dhcp excluded-address 10.10.16.252 10.10.16.254
ip dhcp excluded-address 10.10.17.252 10.10.17.254
ip dhcp excluded-address 10.10.18.252 10.10.18.254
ip dhcp excluded-address 10.10.20.252 10.10.20.254
ip dhcp excluded-address 10.10.21.252 10.10.21.254
ip dhcp excluded-address 10.10.22.252 10.10.22.254
ip dhcp excluded-address 10.10.23.252 10.10.23.254
ip dhcp excluded-address 10.10.24.252 10.10.24.254
ip dhcp excluded-address 10.10.25.252 10.10.25.254
ip dhcp excluded-address 10.10.26.252 10.10.26.254
ip dhcp excluded-address 10.10.27.252 10.10.27.254
ip dhcp excluded-address 10.10.28.252 10.10.28.254
ip dhcp excluded-address 10.10.29.252 10.10.29.254
ip dhcp excluded-address 10.10.30.252 10.10.30.254
ip dhcp excluded-address 10.10.31.252 10.10.31.254
ip dhcp excluded-address 10.10.32.252 10.10.32.254
ip dhcp excluded-address 10.10.33.252 10.10.33.254
ip dhcp excluded-address 10.10.36.252 10.10.36.254
```

Figure 54:Vérification des adresses exclues sur SWD2.

III.3.7.8.2 Création des pools d'adresse DHCP

Nous allons créer maintenant un pool d'adresse pour chaque vlan à l'exception du vlan 18 (printer), vlan 25 (Management), et vlan 32 (Camera), par la suite on définira la passerelle par défaut du sous réseau.

- Sur SWD1 :

```
SWD1#configure terminal
Enter configuration commands, one per line. End with CNIL/Z.
SWD1 (config)#ip dhcp pool vlan10
SWD1 (dhep-config)#network 10.10.10.0 255.255.255.0
SWD1 (dhep-config)#default-router 10.10.10.254
SWD1 (dhep-config)#exit
```

Listing 21: Exemple de création d'un pool pour le Vlan 10 sur le SWD1.

➢ **Vérification de la création des pools DHCP**

Avec la commande **« show run ».**

- Sur SWD1 :

```
ip dhcp pool vlan10
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.254
ip dhcp pool vlan11
 network 10.10.11.0 255.255.255.0
 default-router 10.10.11.254
ip dhcp pool vlan12
 network 10.10.12.0 255.255.255.0
 default-router 10.10.12.254
ip dhcp pool vlan13
 network 10.10.13.0 255.255.255.0
 default-router 10.10.13.254
ip dhcp pool vlan14
 network 10.10.14.0 255.255.255.0
 default-router 10.10.14.254
ip dhcp pool vlan15
 network 10.10.15.0 255.255.255.0
 default-router 10.10.15.254
ip dhcp pool vlan16
 network 10.10.16.0 255.255.255.0
 default-router 10.10.16.254
ip dhcp pool vlan17
 network 10.10.17.0 255.255.255.0
 default-router 10.10.17.254
ip dhcp pool vlan20
 network 10.10.20.0 255.255.255.0
 default-router 10.10.20.254
ip dhcp pool vlan21
 network 10.10.21.0 255.255.255.0
 default-router 10.10.21.254
ip dhcp pool vlan22
 network 10.10.22.0 255.255.255.0
 default-router 10.10.22.254
ip dhcp pool vlan23
 network 10.10.23.0 255.255.255.0
 default-router 10.10.23.254
ip dhcp pool vlan24
 network 10.10.24.0 255.255.255.0
 default-router 10.10.24.254
ip dhcp pool vlan26
 network 10.10.26.0 255.255.255.0
 default-router 10.10.26.254
ip dhcp pool vlan27
 network 10.10.27.0 255.255.255.0
 default-router 10.10.27.254
ip dhcp pool vlan28
 network 10.10.28.0 255.255.255.0
 default-router 10.10.28.254
ip dhcp pool vlan29
 network 10.10.29.0 255.255.255.0
 default-router 10.10.29.254
ip dhcp pool vlan30
 network 10.10.30.0 255.255.255.0
 default-router 10.10.30.254
ip dhcp pool vlan31
 network 10.10.31.0 255.255.255.0
 default-router 10.10.31.254
ip dhcp pool vlan33
 network 10.10.33.0 255.255.255.0
 default-router 10.10.33.254
ip dhcp pool vlan36
 network 10.10.36.0 255.255.255.0
 default-router 10.10.36.254
```

Figure 55: Vérification de la création des pools sur SWD1.

III.3.7.9 Attribution des ports aux Vlans sur les switchs d'accès

Dans cette étape nous allons assigner des ports aux Vlans au niveau des switchs d'accès avec les commandes citées dans le listing ci-dessous :

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNIL/2.
Switch (config)#interface fa0/3
Switch (config-if)#switchport mode access
Switch (config-if)#switchport access vlan 10
Switch (config-if)#exit
Switch (config)#interface fa0/4
Switch (config-if)#switchport mode access
Switch (config-if)#switchport access vlan 23
Switch (config-if)#exit
```

Listing 22: Exemple d'attribution des ports aux Vlans sur un switch d'accès.

- **Vérification des ports attribués aux Vlans**

```
interface FastEthernet0/3          interface FastEthernet0/4
 switchport access vlan 10          switchport access vlan 23
 switchport mode access             switchport mode access
```

Figure 56: Vérification des ports attribués aux Vlans 10 et 23 sur un switch d'accès.

III.3.7.10 Configurations de PortFast et BPDUGUARD

Au démarrage d'un Switch, la recherche de la meilleure topologie prend un peu de temps. Pour optimiser la configuration du STP, nous allons activer le PortFast en utilisant la commande « **Spanning-tree portfast** » qui fait passer directement le port de l'état blocking à l'état forwarding, le démarrage de l'interface est donc plus rapide et le BPDGUARD avec La commande « **Spanning-tree bpduguard enable** » pour sécuriser les ports des Switches de façon à empêcher tous intrus de brancher un Switch externe à l'un des Switches de l'entreprise (bloquer les ports non utilisés). Ces commandes sont applicables uniquement sur les ports d'accès (couche d'accès) reliés à des machines terminales.

```
Switch (config)#interface range fa0/3-4
Switch (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
§Portfast has been configured on FastEthernet0/3 but will only
   have effect when the interface is in a non-trunking mode.
  §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
{Portfast has been configured on FastEthernet0/4 but will only
   have effect when the interface is in a non-trunking mode.
Switch (config-if-range)#spanning-tree bpduguard enable
```

Listing 23:configuration du PortFast et BPDU.

III.3.7.11 Sécurisation des ports des switchs d'accès

Pour une sécurité plus élevée, nous allons activer le « port-security » aux interfaces qui autorise qu'un seul port soit lié à une machine tout en sauvegardant l'adresse Mac de cette dernière avec la commande « port-security mac-address sticky » pour une reconnaissance ultime de la machine au démarrage des prochaines sessions.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNIL/Z.
Switch (config)#interface fa0/3
```

```
Switch (config-if)#switchport nonegotiate
Switch (config-if)#switchport port-security
Switch (config-if)#switchport port-security maximum 1
Switch (config-if)#switchport port-security mac-address sticky
Switch (config-if)#switchport port-security violation restrict
```

Listing 24: Exemple de sécurisation d'une interface.

III.3.7.12 Configuration du DHCP sur les PCs

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

- **Sur le PC0 interconnecté au Vlan10 :**

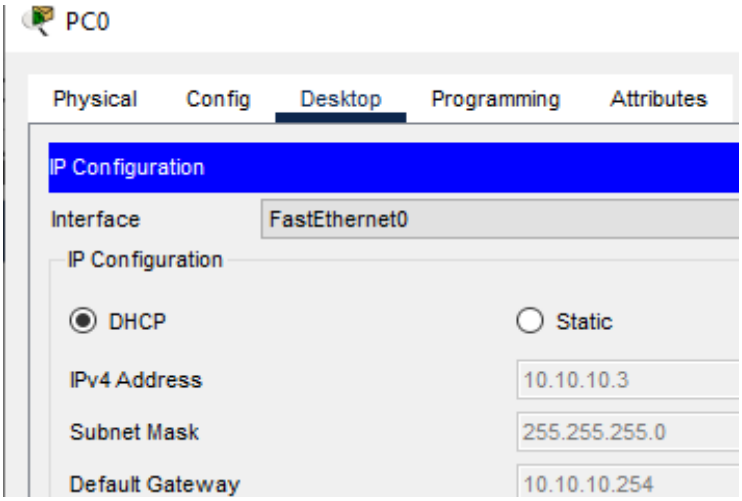


Figure 57:vérification du DHCP sur le PC0.

- **Sur le PC1 interconnecté au Vlan23 :**

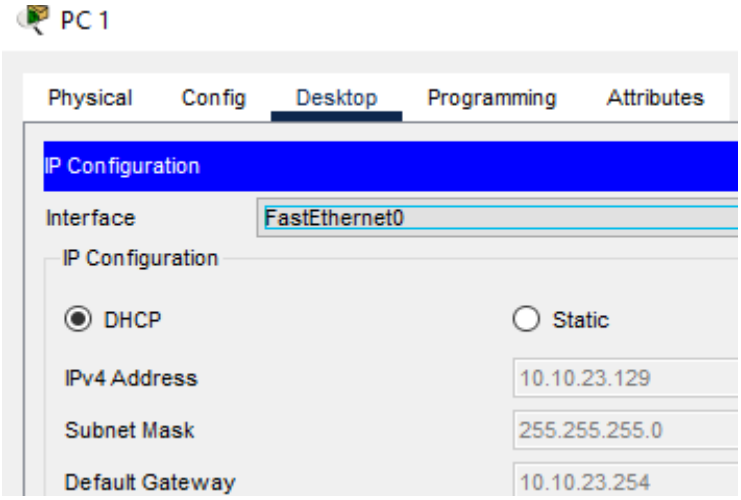


Figure 58:Vérification du DHCP sur le PC1.

III.3.7.13 Configuration de l'HSRP

Maintenant nous allons configurer le protocole HSRP au niveau des deux switches de distribution SWD1 et SWD2, au niveau de chaque interface de Vlan sur SWD1, nous allons mettre la moitié des Vlans avec la priorité 200 pour les Vlans actifs, et 150 pour ceux en standby (les mêmes moitiés que celle utilisées sur le STP), et inversement au niveau de SWD2, tout en définissant les numéros de groupe HSRP comme étant le numéro du Vlan.

Exemple : Vlan 10 / standby 10

- **Sur SWD1 :**

```
SWD1#configure terminal
Enter configuration commands, one per line.
SWD1 (config)#Interface vlan 10
SWD1 (config-if)#Standby 10 ip 10.10.10.254
SWD1 (config-if)#Standby 10 priority 200
SWD1 (config-if)#Standby 10 preempt
SWD1 (config-if)#Exit
```

Listing 25: Exemple de configuration du HSRP au Vlan10 sur SWD1.

```
SWD1>enable
SWD1#configure terminal
Enter configuration commands, one per line. End with CNIL/2
SWD1 (config)#interface vlan23
SWD1 (config-if)#standby 23 ip 10.10.23.254
SWD1 (config-if)#standby 23 priority 150
SWD1 (config-if)#standby 23 preempt
SWD1 (config-if)#exit
```

Listing 26: Exemple de configuration du HSRP au Vlan23 sur SWD1.

- **Sur SWD2 :**

```
SWD2#configure terminal
Enter configuration commands, one per line. End with CNIL/Z.
SWD2 (config) #Interface vlan 10
SWD2 (config-if)#Standby 10 ip 10.10.10.254
SWD2 (config-if)#Standby 10 priority 150
SWD2 (config-if)#Standby 10 preempt
SWD2 (config-if)#exit
```

Listing 27: Exemple de configuration du HSRP au Vlan10 sur SWD2.

```
SWD2 (config)#Interface vlan 23
SWD2 (config-if)#Standby 23 ip 10.10.23.254
SWD2 (config-if)#Standby 23 priority 200
SWD2 (config-if)#Standby 23 preempt
SWD2 (config-if)#exit
```

Listing 28: Exemple de configuration du HSRP au Vlan23 sur SWD2.

➢ **Vérification du HSRP**

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

- **Sur SWD1 :**

```
SWD1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   200 P Active   local           10.10.10.253    10.10.10.254
Vl11        11   200 P Active   local           10.10.11.253    10.10.11.254
Vl12        12   200 P Active   local           10.10.12.253    10.10.12.254
Vl13        13   200 P Active   local           10.10.13.253    10.10.13.254
Vl14        14   200 P Active   local           10.10.14.253    10.10.14.254
Vl15        15   200 P Active   local           10.10.15.253    10.10.15.254
Vl16        16   200 P Active   local           10.10.16.253    10.10.16.254
Vl17        17   200 P Active   local           10.10.17.253    10.10.17.254
Vl18        18   200 P Active   local           10.10.18.253    10.10.18.254
Vl20        20   200 P Active   local           10.10.20.253    10.10.20.254
Vl21        21   200 P Active   local           10.10.21.253    10.10.21.254
Vl22        22   200 P Active   local           10.10.22.253    10.10.22.254
Vl23        23   150 P Standby  10.10.23.253    local           10.10.23.254
Vl24        24   150 P Standby  10.10.24.253    local           10.10.24.254
Vl25        25   150 P Standby  10.10.25.253    local           10.10.25.254
Vl26        26   150 P Standby  10.10.26.253    local           10.10.26.254
Vl27        27   150 P Standby  10.10.27.253    local           10.10.27.254
Vl28        28   150 P Standby  10.10.28.253    local           10.10.28.254
Vl29        29   150 P Standby  10.10.29.253    local           10.10.29.254
Vl30        30   150 P Standby  10.10.30.253    local           10.10.30.254
Vl31        31   150 P Standby  10.10.31.253    local           10.10.31.254
Vl32        32   150 P Standby  10.10.32.253    local           10.10.32.254
Vl33        33   150 P Standby  10.10.33.253    local           10.10.33.254
Vl36        36   150 P Standby  10.10.36.253    local           10.10.36.254
```

Figure 59: Vérification du HSRP sur SWD1.

- **Sur SWD2 :**

```
SWD2#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
V110        10   150 P Standby  10.10.10.252    local           10.10.10.254
V111        11   150 P Standby  10.10.11.252    local           10.10.11.254
V112        12   150 P Standby  10.10.12.252    local           10.10.12.254
V113        13   150 P Standby  10.10.13.252    local           10.10.13.254
V114        14   150 P Standby  10.10.14.252    local           10.10.14.254
V115        15   150 P Standby  10.10.15.252    local           10.10.15.254
V116        16   150 P Standby  10.10.16.252    local           10.10.16.254
V117        17   150 P Standby  10.10.17.252    local           10.10.17.254
V118        18   150 P Standby  10.10.18.252    local           10.10.18.254
V120        20   150 P Standby  10.10.20.252    local           10.10.20.254
V121        21   150 P Standby  10.10.21.252    local           10.10.21.254
V122        22   150 P Standby  10.10.22.252    local           10.10.22.254
V123        23   200 P Active   local           10.10.23.252    10.10.23.254
V124        24   200 P Active   local           10.10.24.252    10.10.24.254
V125        25   200 P Active   local           10.10.25.252    10.10.25.254
V126        26   200 P Active   local           10.10.26.252    10.10.26.254
V127        27   200 P Active   local           10.10.27.252    10.10.27.254
V128        28   200 P Active   local           10.10.28.252    10.10.28.254
V129        29   200 P Active   local           10.10.29.252    10.10.29.254
V130        30   200 P Active   local           10.10.30.252    10.10.30.254
V131        31   200 P Active   local           10.10.31.252    10.10.31.254
V132        32   200 P Active   local           10.10.32.252    10.10.32.254
V133        33   200 P Active   local           10.10.33.252    10.10.33.254
V136        36   200   Active   local           10.10.36.252    10.10.36.254
```

Figure 60: Vérification du HSRP sur SWD2.

III.3.7.14 Configuration du niveau 3

Nous allons faire passer les ports montants des switchs de distribution vers les switchs cœurs du niveau 2 au niveau 3 avec la commande « no switchport » pour les faire fonctionner comme des interfaces de routeur plutôt que comme des ports de commutateur.

- **Pour l'interface reliant SWD1 (0/18) à SWC1 :**

```
SWD1#configure terminal
Enter configuration commands, one per line. End with CNIL/2.
SWD1 (config)#interface fa0/18
SWD1 (config-if)#no switchport
```

Listing 29:exemple de configuration du niveau3 sur l'interface du SWD1.

III.3.7.15 Configuration des ports routés

Nous allons attribuer une adresse IP/30 et un masque de réseau pour chacun des ports routés suivant Tableau 04.

- **Sur SWD1 :**

```
SWD1 (config)#interface fa0/18
SWD1 (config-if)#ip address 10.10.100.253 255.255.255.252
SWD1 (config-if)#exit
SWD1 (config)#interface fa0/19
```

```
SWD1 (config-if)#ip address 10.10.110.253 255.255.255.252
```

Listing 30:Configuration des ports routés sur SWD1

III.3.7.16 Configuration de l'OSPF

Nous allons configurer le protocole de routage OSPF au niveau des switches de distribution (SWD1, SWD2) et ceux du Core (SWC1, SWC2). Nous allons activer le routage OSPF avec lacommande « **ip routing** » et attribuer un groupe OSPF 1, puis nous allons déclarer tous les sous-réseaux dans chaque switch de distribution et routeur.

Pour les Vlans, nous allons saisir le réseau 10.10.X.0 avec un masque inversé 0.0.0.255.

- **Sur SWD1 :**

```
SWDI (config)#Ip routing
SWD1 (config) #Router ospf 1
SWD1 (config-router)#Network 10.10.10.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.11.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.12.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.13.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.14.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.15.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.16.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.17.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.18.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.20.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.21.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.22.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.23.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.24.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.25.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.26.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.27.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.28.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.29.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.30.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.31.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.32.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.33.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.36.0 0.0.0.255 area 0
SWD1 (config-router)#Network 10.10.100.252 0.0.0.3 area 0
SWD1 (config-router)#Network 10.10.110.252 0.0.0.3 area 0
```

Listing 31:Configuration de l'OSPF sur SWD1.

- **Sur SWD2 :**

```
SWD2 (config-router)#Network 10.10.10.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.11.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.12.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.13.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.14.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.15.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.16.0 0.0.0.255 area 0
```

```
SWD2 (config-router)#Network 10.10.17.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.18.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.20.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.21.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.22.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.23.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.24.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.25.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.26.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.27.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.28.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.29.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.30.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.31.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.32.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.33.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.36.0 0.0.0.255 area 0
SWD2 (config-router)#Network 10.10.120.252 0.0.0.3 area 0
SWD2 (config-router)#Network 10.10.140.252 0.0.0.3 area 0
```

Listing 32: Configuration de l'OSPF sur SWD2.

Nous allons procéder à la même chose sur les deux switches Cores et sur le routeur.

- **Vérification de l'OSPF**

Avec la commande **« show run »** Sur SWD1 et SWD2 :

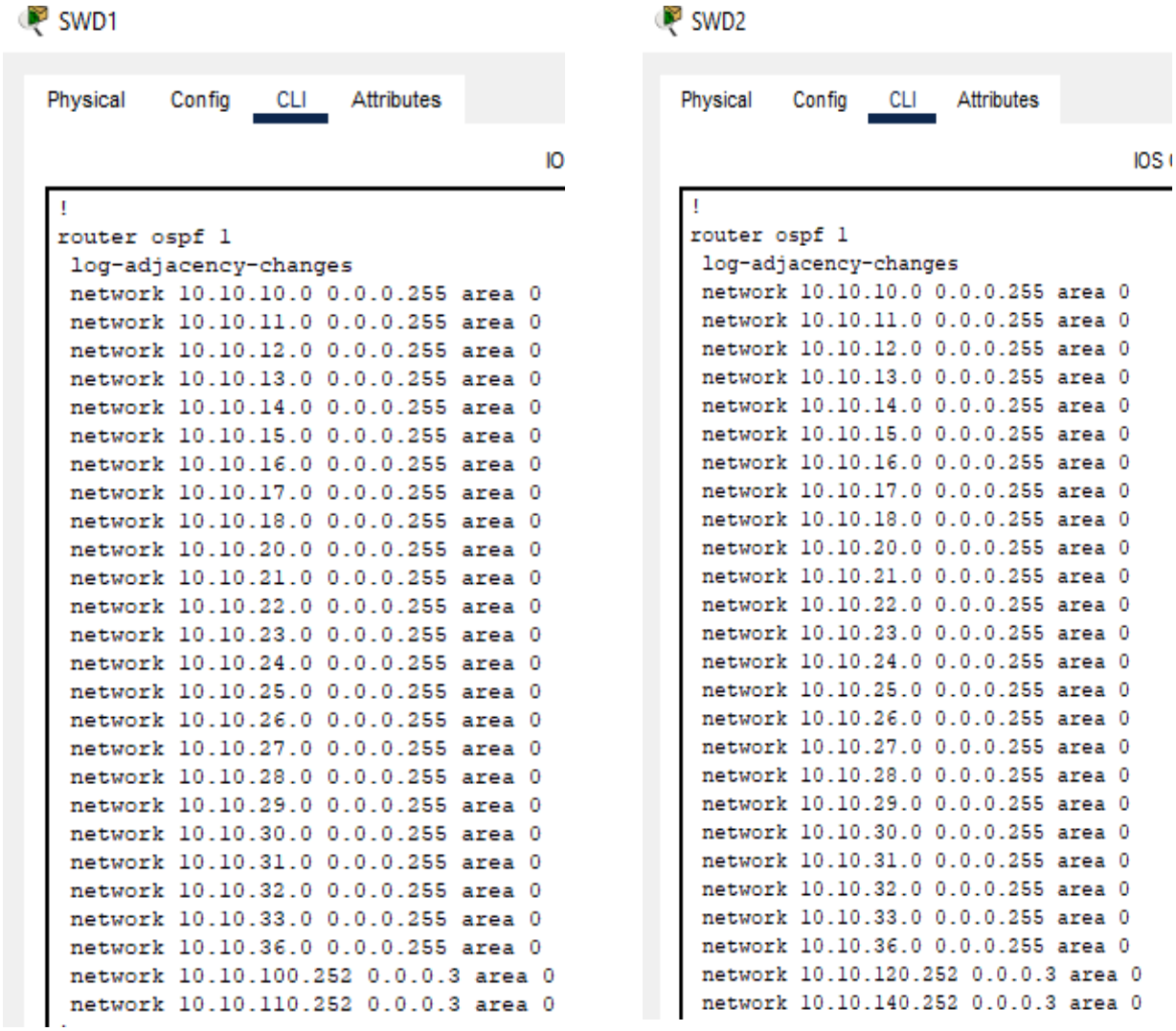


Figure 61:Vérificaton de l'OSPF sur SWD1 et SWD2.

- **Sur SWC1 et SWC2 :**

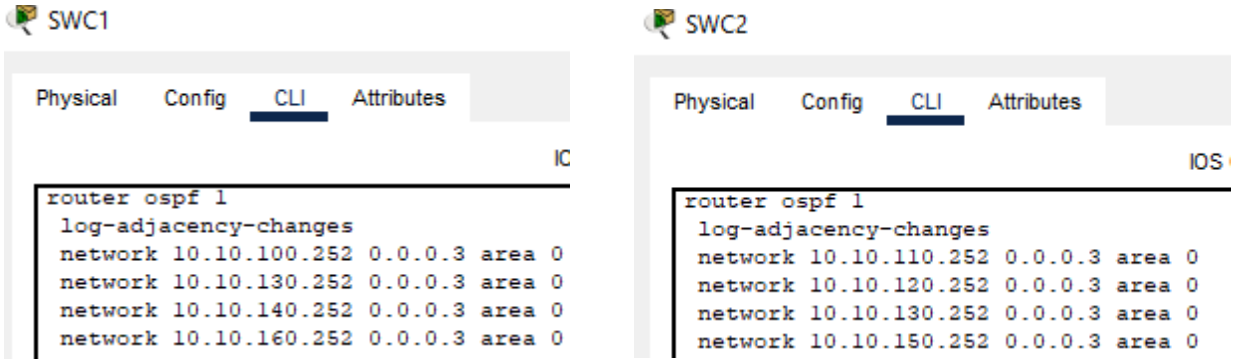


Figure 62: Vérification de l'OSPF sur SWC1 et SWC2.

- Sur le routeur :

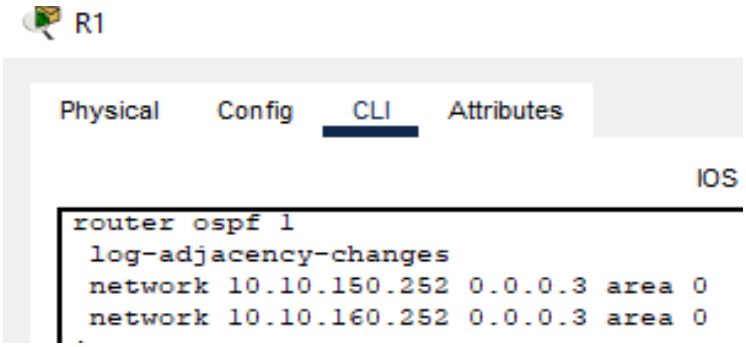


Figure 63: Vérification de l'OSPF sur R1.

III.3.8 Teste de la haute disponibilité du réseau

Afin de tester le bon fonctionnement de notre réseau LAN et de s'assurer qu'il est opérationnel, nous allons simuler un ping continu entre deux PCs du même Vlan, puis nous allons simuler une panne sur leur switch Root Bridge en éteignant les ports de ce dernier, et on vérifie que le ping repart après un arrêt d'une dizaine de secondes, et ensuite nous allons à nouveau rallumer la route principale afin de vérifier le « preempt » du HSRP qui va à nouveau reprendre sa route principale.

- **Test de haute disponibilité entre PCs du même Vlan**

Premièrement nous avons pris un PC du Vlan 10 (10.10.10.128) et nous allons faire un Ping continu vers un PC du même Vlan (10.10.10.2), En premier lieu nous avons constaté que le Ping fonctionne parfaitement et sans problème, comme illustré dans Figure 64 :

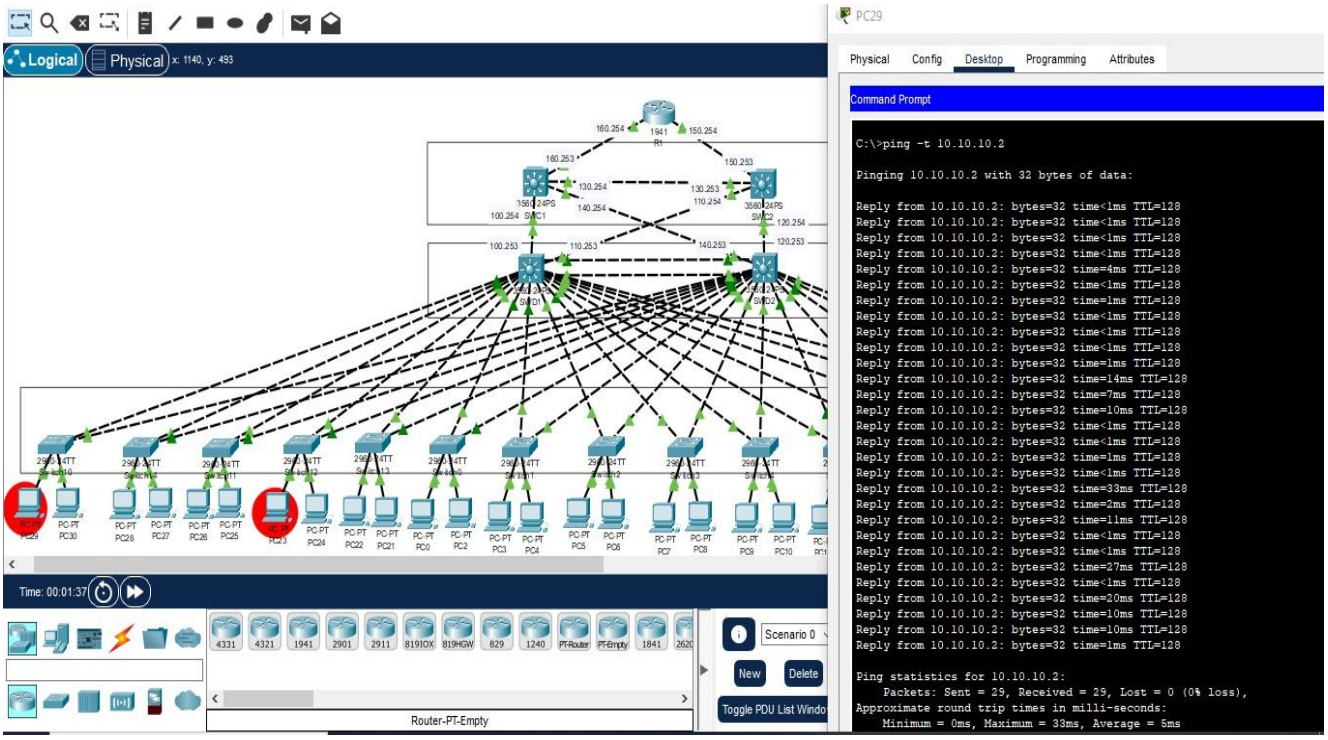


Figure 64: Ping continu entre deux PC du même Vlan.

Maintenant nous allons simuler une panne, celle d'éteindre la route principale de ce vlan,

nous allons constater directement que le Ping s'arrête pour quelques paquets, le temps que le protocole HSRP discute avec le SWD2 pour activer la route secondaire, puis le Ping reprend, ce qui prouve que la route a bien été basculé vers le SWD2, comme l'explique Figure 65:

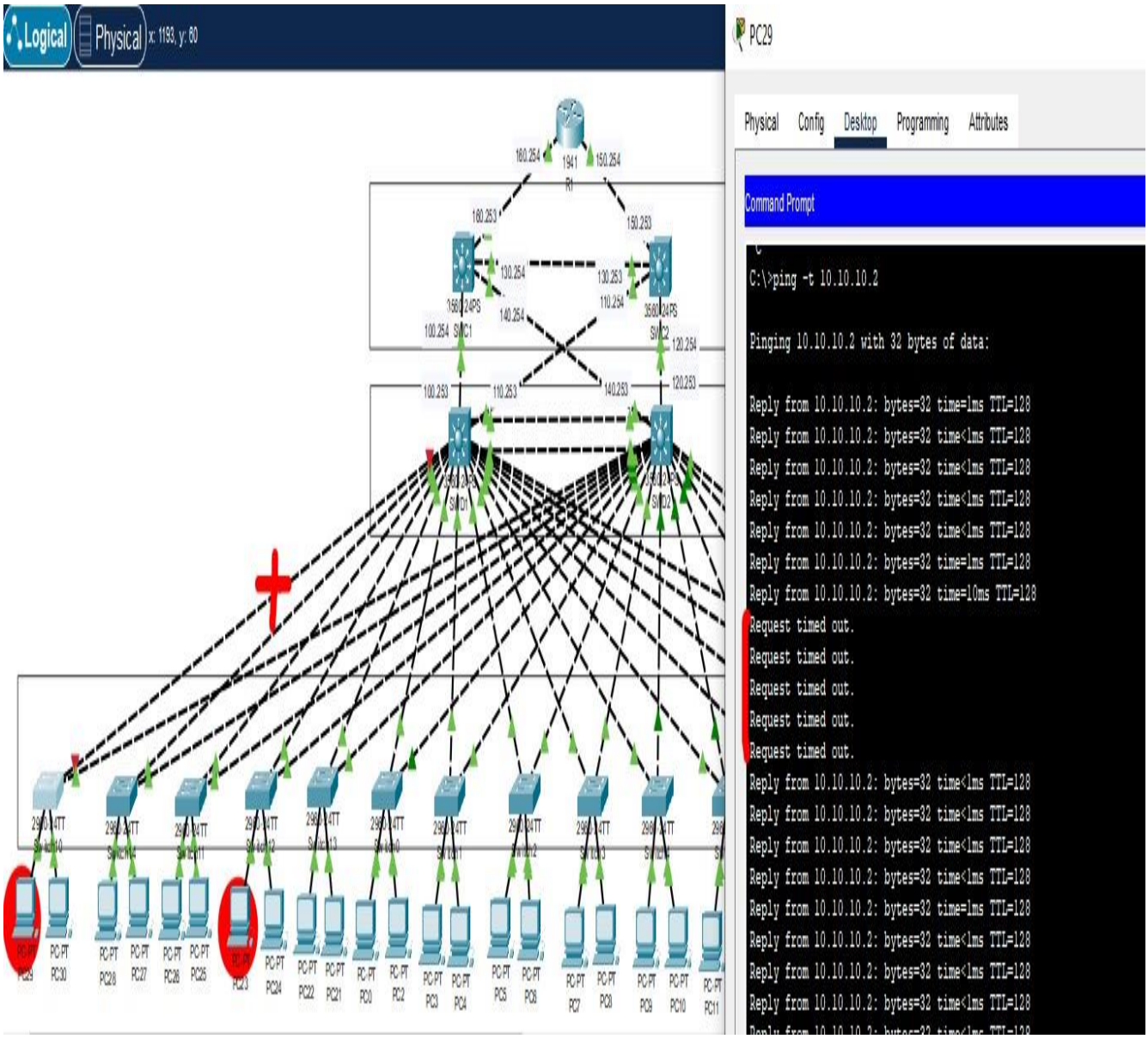


Figure 65: Capture explicative du Ping continu lors d'une panne.

Maintenant, nous allons réactiver l'interface principale sur le SDW1 afin de s'assurer qu'il va reprendre sa route principale et vérifier que le preempt du HSRP fonctionne parfaitement. Dès qu'on active l'interface, on constate qu'il y a encore un arrêt dans le Ping, le temps que les deux switches discutent les priorités puis il reprend facilement sa route et le Ping remarche.

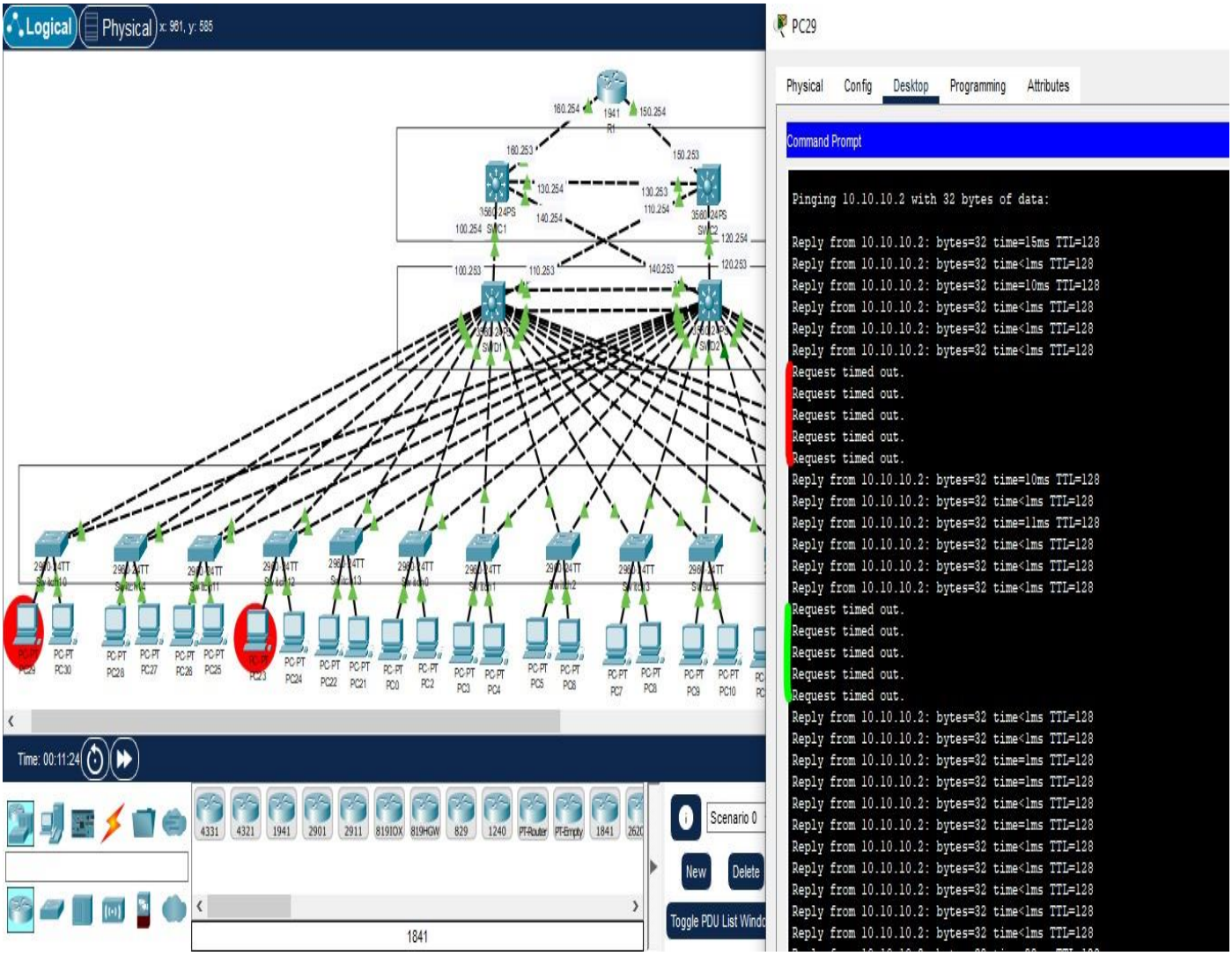


Figure 66: Capture explicative du ping continu lors de re-fonctionnement du SWD1.

- **Test de haute disponibilité du réseau LAN**

Suivant la même méthode nous allons tester la haute disponibilité de tout le réseau local de Cevital, en simulant une défaillance de l'un des switches de distribution (SWD2) et les interfaces amenant au routeur.

Sur un PC du Vlan 23 (10.10.23.129) nous allons réaliser un Ping continu vers l'adresse de l'interface du routeur (10.10.160.254). Puis on simule une panne au niveau du Switch de distribution SWD2 (Root Bridge du Vlan 23) et aussi au niveau l'un des liens de Switch SWD1 (interface Fa0/18) et SWC1 (interface Fa0/1) et au niveau du lien reliant SWC2 (interface Gig0/1) au routeur (interface Gig0/0/1), afin de vérifier non seulement le HSRP mais aussi l'OSPF illustré dans Figure 67 :

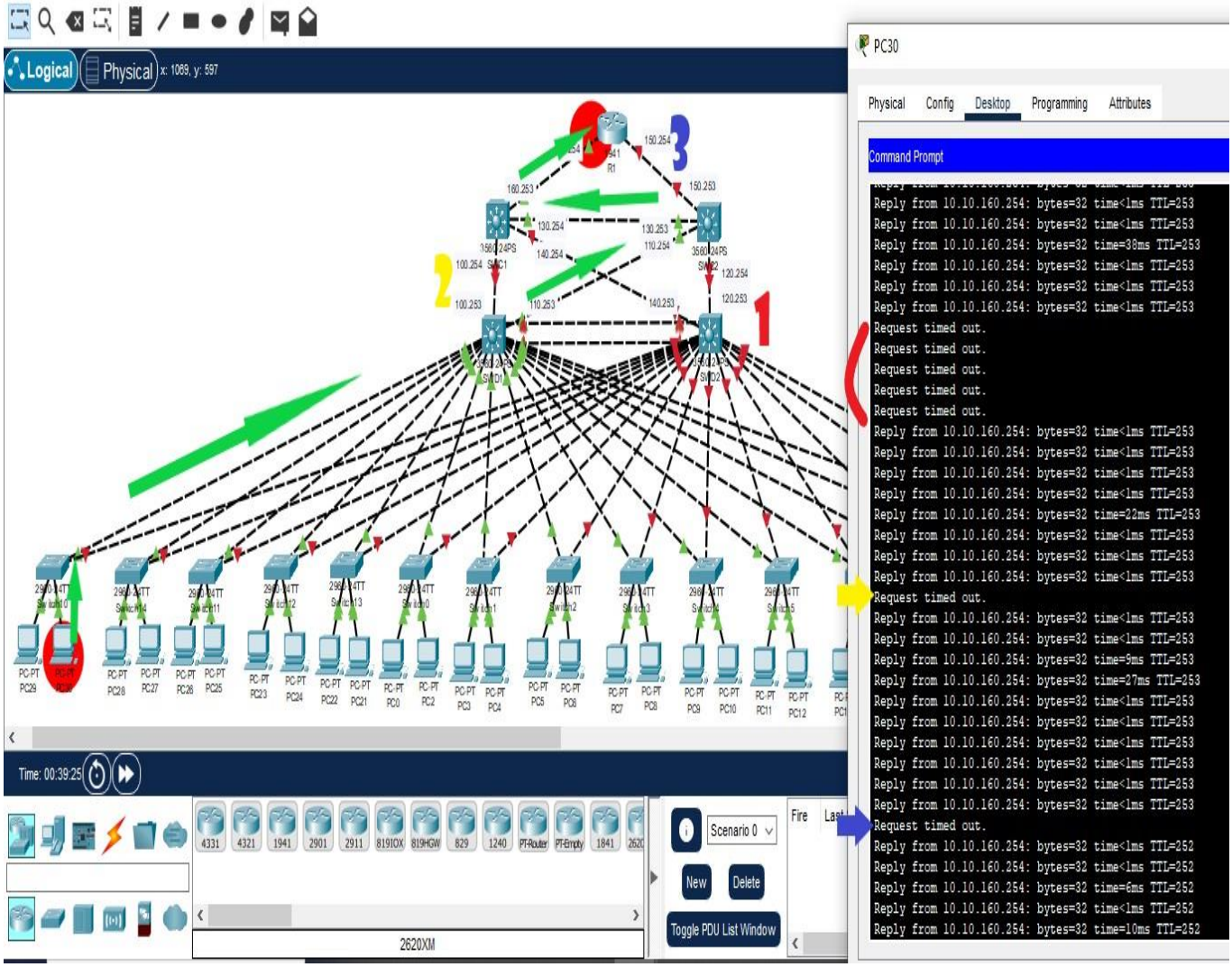


Figure 67: Capture d'un test explicatif de la haute disponibilité LAN.

Désormais nous avons réalisé un réseau LAN hautement disponible à l'aide du protocole HSRP et le routage OSPF. Pour propager cette disponibilité au niveau WAN nous allons suivre ensemble de configuration dans la partie suivante.

III.4 La mise en place d'un réseau WAN redondant

III.4.1 Architecture WAN

Nous avons configuré la nouvelle architecture proposée au réseau CEVITAL sur le simulateur CISCO Packet Tracer 8.2 La topologie est représentée ci-dessous.

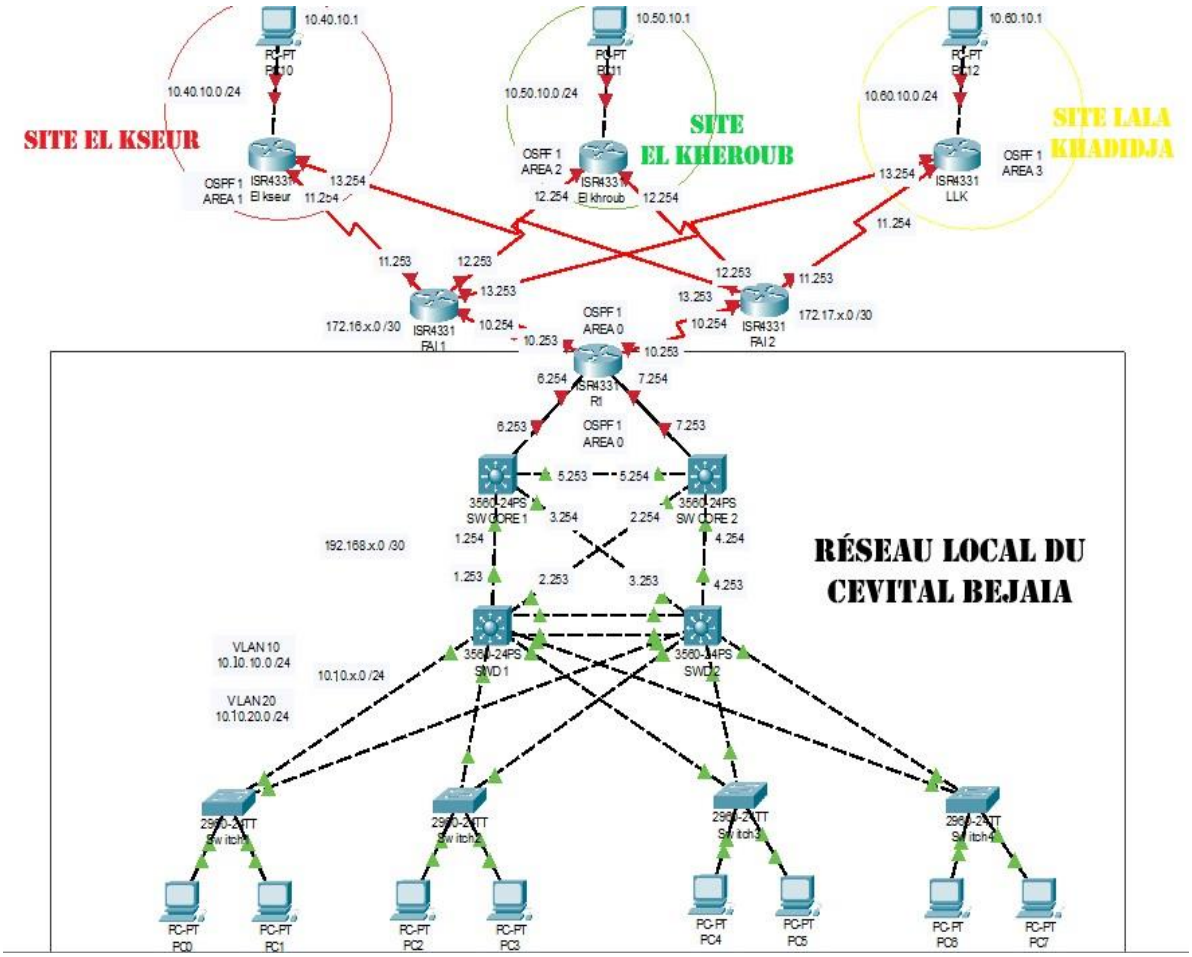


Figure 68: Architecture WAN de Cevital.

III.4.2 Configuration des équipements du réseau WAN

Dans cette partie, nous avons interconnecté le réseau local de la première partie aux autres sites distants (site Cojek d'EL Kseur, site Lala Khadija de Tizi-Ouzou, et site EL khroub) avec des liaisons spécialisées, où nous avons mis en place des connexions vers les routeurs d'Algerie Télécom, pour qu'ils puissent établir des liaisons de fibre optique point à point entre ces derniers. Afin d'assurer un équilibrage de charges et de permettre le partage de ressources et de la communication.

Pour simplifier l'architecture, nous avons diminué le nombre des switches d'accès du réseau LAN de BEJAIA (site central), comme nous avons représenté les autres sites distants par des routeurs connectés à des PCs configurés statiquement avec des adresses IP adaptées à chaque réseau.

- **Configuration LAN**

Nous avons gardé la même architecture LAN, par ailleurs les mêmes configurations de la première partie du chapitre. En ajoutant les interfaces montantes du R1 vers les routeurs d'Algérie télécoms (FAI1, FAI2).

- **Configuration WAN**

Pour garantir le routage du réseau, nous avons configuré le protocole OSPF au niveau des

routeurs qui relient les sites distants. Nous avons alloué un groupe 1 et des aires OSPF dans chaque configuration, et avons saisi les réseaux directement connectés dans chaque routeur.

III.4.3 Tableau des interfaces des routeurs

Routeur	Interfaces (IP adresse)
R1	S0/1/0 : 172.16.10.253/30
	S0/1/1 : 172.17.10.253/30
	Loopback: 1.1.1.1 /32
FAI1	S0/1/0 : 172.16.10.254/30
	S0/2/1 : 172.16.13.253/30
	S0/1/1 : 172.16.11.253/30
	S0/2/0 : 172.16.12.253/30
	Loopback: 2.2.2.2/32
FAI2	S0/1/0 : 172.17.10.254/30
	S0/1/1 : 172.17.13.253/30
	S0/2/0 : 172.17.12.253/30
	S0/2/1 : 172.17.11.253/30
	Loopback: 3.3.3.3/32
EL KSEUR	S0/1/0 : 172.16.11.254/30
	S0/1/1 : 172.17.13.254/30
	G0/0/0 : 10.40.10.254/24
	Loopback: 4.4.4.4/32
EL KHROUB	S0/1/0 : 172.16.12.254/30
	S0/1/1 : 172.17.12.254/30
	G0/0/0 : 10.50.10.254/24
	Loopback: 5.5.5.5/32
LLK	S0/1/0 : 172.16.13.254/30
	S0/1/1 : 172.17.11.254/30
	G0/0/0 : 10.60.10.254/24
	Loopback: 6.6.6.6/32

Tableau 9: Attribution des adresses IP pour les interfaces des routeurs.

III.4.4 Configuration des interfaces

Avant de configurer le routage OSPF, nous allons d'abord configurer les interfaces avec des adresses IP comme indiquées sur Tableau 10. Nous avons attribué des adresses de Loopback sur chaque routeur afin de les identifier et tester les ports de ces derniers.

- **Exemple sur FAI1**

```
FAI1 (config) #Interface s0/1/0
FAIl (config-if)#Ip address 172.16.10.254 255.255.255.252
FAIl (config-if)#No shutdown
FAI1 (config-if)#
FAI1 (config-if)#Interface s0/1/1
FAIl (config-if)#Ip address 172.16.11.253 255.255.255.252
FAIl (config-if)#No shutdown
ALINK-5-CHANGED: Interface Serial0/1/1, changed state to down
FAI1 (config-if)#
```

```
FAI1 (config-if)#Interface s0/2/0
FAIl (config-if)#Ip address 172.16.12.253 255.255.255.252
FAIl (config-if)#No shutdown
GLINK-5-CHANGED: Interface Serial0/2/0, changed state to down
FAI1 (config-if)#
FAIl (config-if)#Interface s0/2/1
FAI1 (config-if)#Ip address 172.16.13.253 255.255.255.252
FAIl (config-if)#No shutdown
FLINK-5-CHANGED: Interface Serial0/2/1, changed state to down
FAI1 (config-if)#Exit
FAI1 (config)#
FAIl (config)#Interface 10
FAIl (config-if)#Ip address 2.2.2.2 255.255.255.255
```

Listing 33:Configuration des interfaces du FAI1.

- **Vérification des interfaces**

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

```
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
!
interface GigabitEthernet0/0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/1/0
 ip address 172.16.10.254 255.255.255.252
!
interface Serial0/1/1
 ip address 172.16.11.253 255.255.255.252
 clock rate 2000000
!
interface Serial0/2/0
 ip address 172.16.12.253 255.255.255.252
 clock rate 2000000
!
```

Figure 69:Vérification des interfaces de FAI1.

La même configuration sera réalisée sur les différents routeurs en respectant le tableau des interfaces.

III.4.5 Configuration de l'OSPF

Nous avons alloué le même groupe OSPF1 sur tous les routeurs, et attribué des aires pour chacun afin de les différencier et réaliser un travail plus réel, (Bejaia : area 0, Elkseur : area 1, Elkhroub : area 2, LLK : area 3). Les étapes de configurations sont illustrées dans les listings 34-39 :

- **Sur R1**

```
R1 (config) #Ip routing
R1 (config)#Router ospf 1
R1 (config-router)#Network 192.168.6.252 0.0.0.3 area 0
Rl (config-router)#Network 192.168.7.252 0.0.0.3 area 0
RI (config-router)#Network 172.16.10.252 0.0.0.3 area 0
Rl (config-router)#Network 172.17.10.252 0.0.0.3 area 0
```

Listing 34: Configuration de l'OSPF sur R1.

- **Sur FAI1**

```
FAIl (config) #Ip routing
FAIl (config)#Router ospf 1
FAIl (config-router)#Network 172.16.10.252 0.0.0.3 area 0
FAIl (config-router)#Network 172.16.11.252 0.0.0.3 area 1
FAIl (config-router)#Network 172.16.12.252 0.0.0.3 area 2
FAIl (config-router)#Network 172.16.13.252 0.0.0.3 area 3
```

Listing 35: Configuration de l'OSPF sur FAI1.

- **Sur FAI2**

```
FAI2 (config)#Ip routing
FAI2 (config)#Router ospf 1
FAI2 (config-router)#Network 172.17.10.252 0.0.0.3 area 0
FAI2 (config-router)#Network 172.17.11.252 0.0.0.3 area 3
FAI2 (config-router)#Network 172.17.12.252 0.0.0.3 area 2
FAI2 (config-router)#Network 172.17.13.252 0.0.0.3 area 1
```

Listing 36: Configuration de l'OSPF sur FAI2.

- **Sur EL KSEUR.**

```
Elkseur (config)#Ip routing
Elkseur (config)#Router ospf 1
Elkseur (config-router)#Network 10.40.10.0 0.0.0.255 area 1
Elkseur (config-router)#Network 172.16.11.252 0.0.0.3 area 1
Elkseur (config-router)#Network 172.17.13.252 0.0.0.3 area 1
```

Listing 37: Configuration de l'OSPF sur EL KSEUR.

- **Sur ELKHROUB**

```
Elkhroub (config)#Ip routing
Elkhroub (config)#Router ospf 1
Elkhroub (config-router)#Network 10.50.10.0 0.0.0.255 area 2
Elkhroub (config-router)#Network 172.16.12.252 0.0.0.3 area 2
Elkhroub (config-router)#Network 172.17.12.252 0.0.0.3 area 2
```

Listing 38: Configuration de l'OSPF sur le site ELKHROUB.

- **Sur Lalla KHEDIDJA**

```
LLK (config) #Ip routing
LLK (config)#Router ospf 1
LLK(config-router)#Network 10.60.10.0 0.0.0.255 area 3
LLK(config-router)#Network 172.16.13.252 0.0.0.3 area 3
```

```
LLK(config-router)#Network 172.17.11.252 0.0.0.3 area 3
```

Listing 39: Configuration de l'OSPF sur le site LLK.

- **Vérification de l'OSPF**

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

```
router ospf 1
 log-adjacency-changes
 network 192.168.6.252 0.0.0.3 area 0
 network 192.168.7.252 0.0.0.3 area 0
 network 172.16.10.252 0.0.0.3 area 0
 network 172.17.10.252 0.0.0.3 area 0
```

```
router ospf 1
 log-adjacency-changes
 network 172.16.10.252 0.0.0.3 area 0
 network 172.16.11.252 0.0.0.3 area 1
 network 172.16.12.252 0.0.0.3 area 2
 network 172.16.13.252 0.0.0.3 area 3
```

Figure 70: Vérification de l'OSPF sur R1 et FAI1.

- **Vérification des configurations sur les sites distants**

LLK

Physical Config CLI Attributes

IOS Com

```
interface Loopback0
 ip address 6.6.6.6 255.255.255.255
!
interface GigabitEthernet0/0/0
 ip address 10.60.10.254 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/1/0
 ip address 172.16.13.254 255.255.255.252
!
interface Serial0/1/1
 ip address 172.17.11.254 255.255.255.252
 clock rate 2000000
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 10.60.10.0 0.0.0.255 area 3
 network 172.16.13.252 0.0.0.3 area 3
 network 172.17.11.252 0.0.0.3 area 3
```

El khroub

Physical Config CLI Attributes

IOS Com

```
interface Loopback0
 ip address 5.5.5.5 255.255.255.255
!
interface GigabitEthernet0/0/0
 ip address 10.50.10.254 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/1/0
 ip address 172.16.12.254 255.255.255.252
!
interface Serial0/1/1
 ip address 172.17.12.254 255.255.255.252
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 10.50.10.0 0.0.0.255 area 2
 network 172.16.12.252 0.0.0.3 area 2
 network 172.17.12.252 0.0.0.3 area 2
```

Figure 71: Vérification des configurations sur les sites distants.

III.4.6 Configuration des PCs des sites distants

Afin de tester la connectivité de notre architecture, nous allons attribuer des adresses IP statiques aux PCs connectés aux différents routeurs des sites distants.

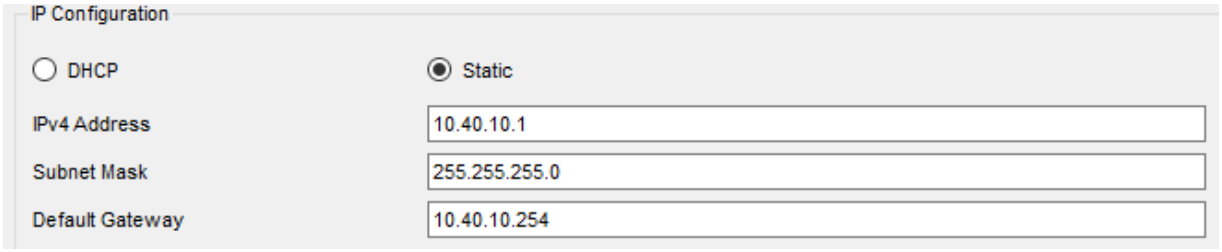


Figure 72: Configuration PC ELKSEUR.

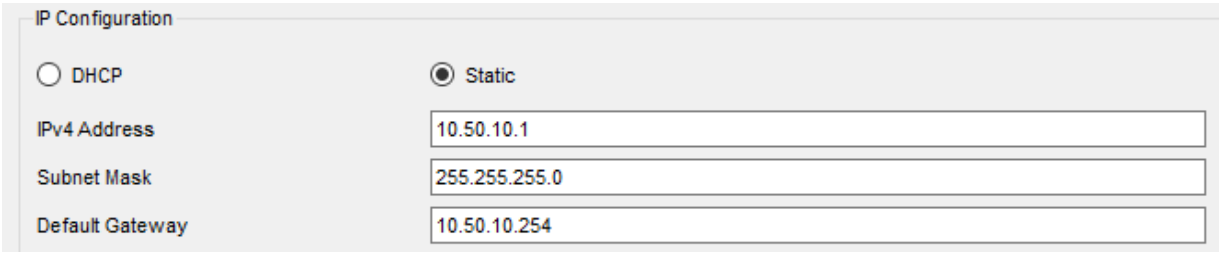


Figure 73: Configuration PC ELKHROUB.

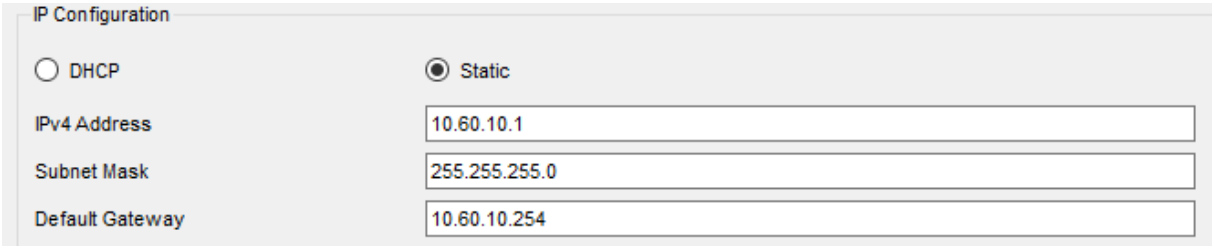


Figure 74: Configuration PC LLK.

III.4.7 Test de connectivité WAN

Nous allons d'abord vérifier que la connexion inter-sites est opérationnelle, pour ce faire nous allons simuler un Ping entre un PC du site local (Bejaia) vers un PC du site distant Lala Khadidja (LLK), puis entre le site Elkseur et les différents sites distants, afin de tester la connectivité de notre architecture WAN.

La commande **« Ping –t »** nous permet de simuler un Ping continu, et **« tracert »** permet de suivre le chemin des paquets qui transitent de la source vers la destination.

Sur la figure suivant, on remarque que les paquets transitent du PC1 (10.10.20.253) du site local vers le PC du site distant LLK (10.60.10.1) à partir du FAI 1, qui est le routeur principal qui s'occupe de la distribution des paquets.

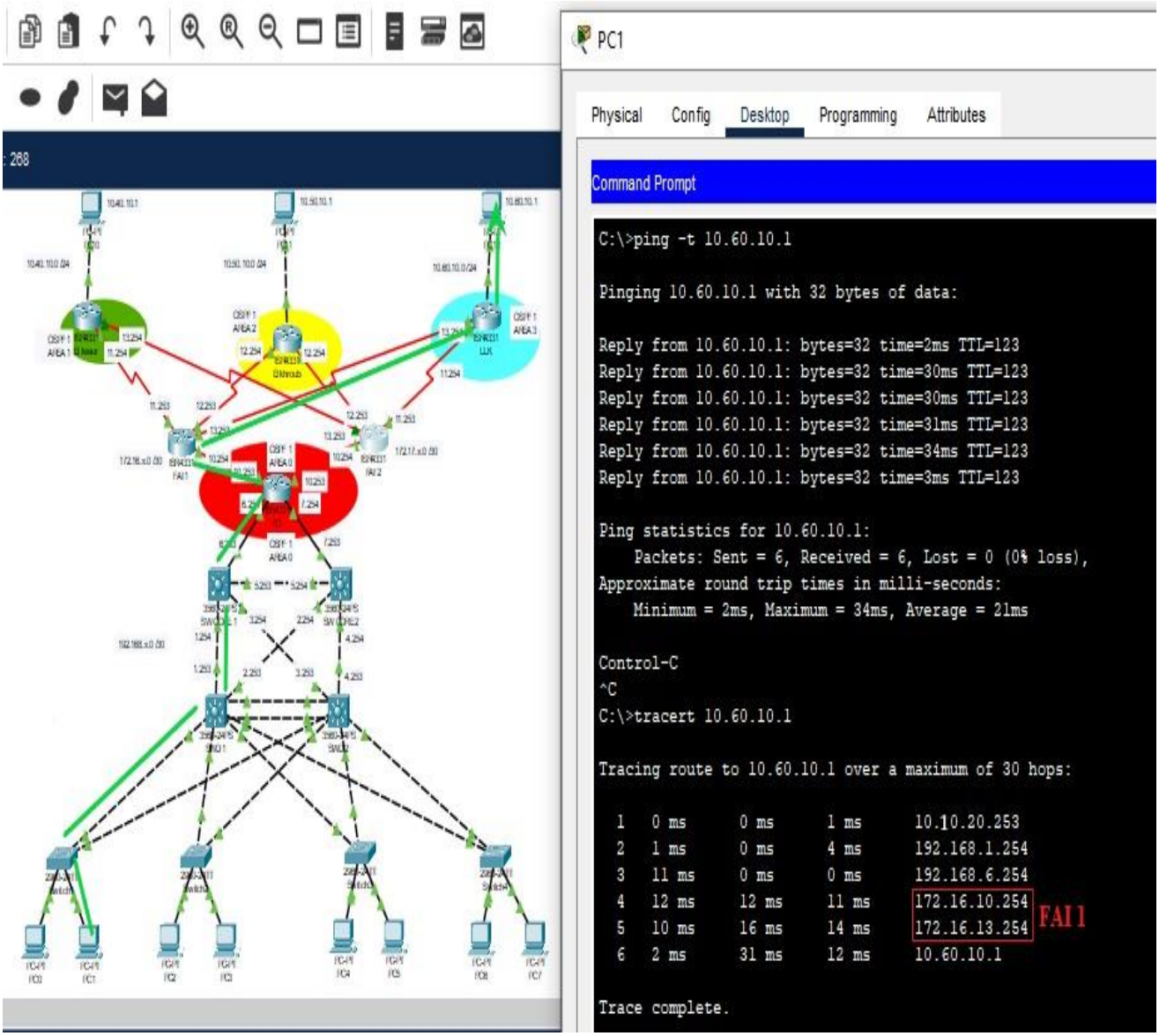


Figure 75: Ping du site local vers un PC du site LLK.

Puis nous avons simulé un Ping du site Elkseur vers les autres sites.

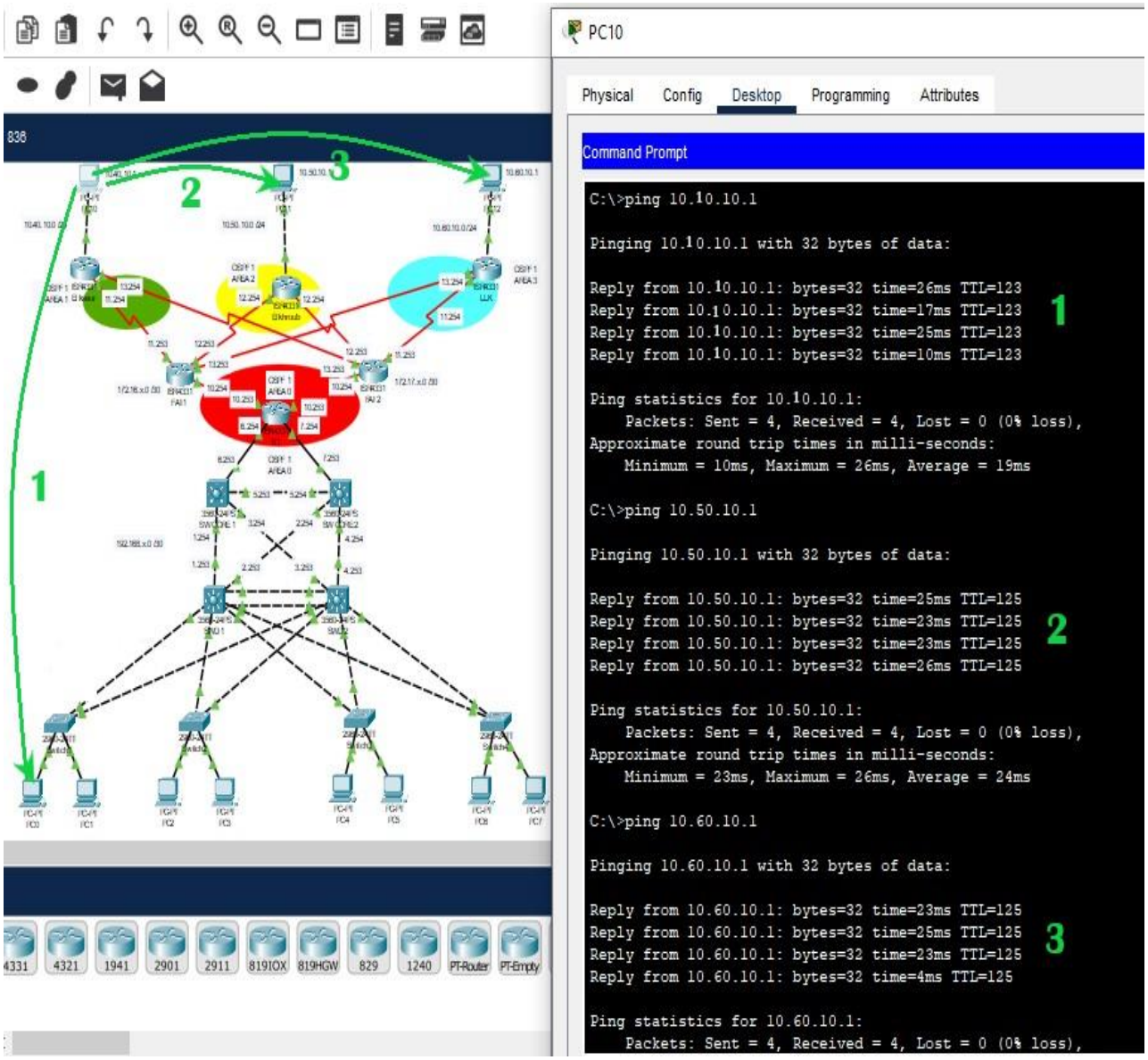


Figure 76: Ping du site ELKSEUR vers les autres sites

III.4.8 Test de la redondance WAN

En gardant le même Ping précédent, nous allons simuler une panne sur le FAI 01 en éteignant le routeur de ce dernier. Nous allons remarquer que les paquets transitent à travers le FAI 2,ce qui garantit la haute disponibilité de notre réseau.

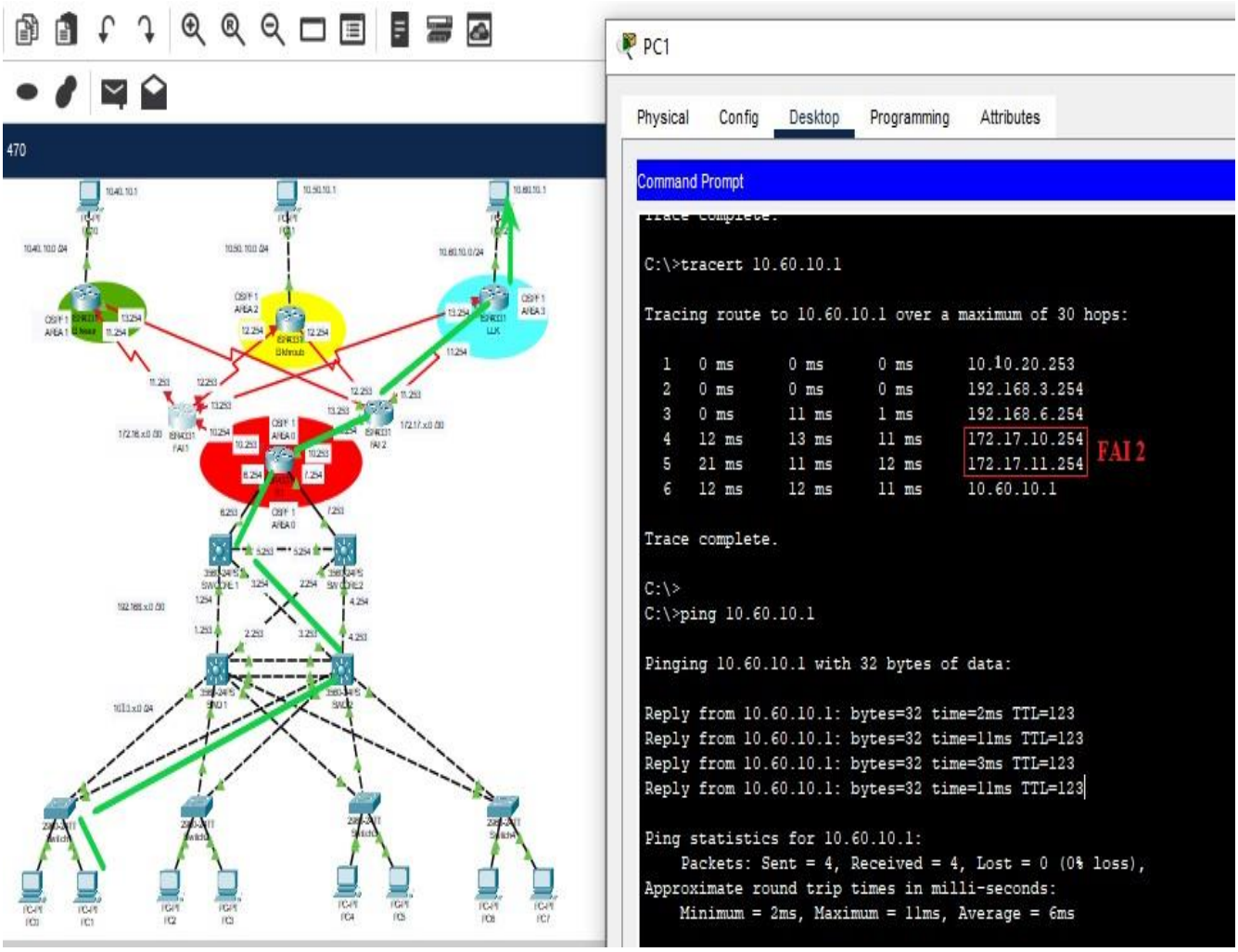


Figure 77: Ping du site local vers le site LLK avec une panne sur le FAI1.

III.5 Conclusion

Ce chapitre s'est scindé en deux parties. Dans la première nous avons configuré le réseau LAN proposé, où nous avons mis en avant les configurations et les protocoles de redondance, à savoir la configuration des VLANs, des liens Trunk, les protocoles VTP, HSRP, etc. Puis dans la deuxième nous avons mis en place des connexions redondantes vers les sites distants du Cevital, en utilisant le protocole de routage OSPF. Les résultats obtenus et détaillés dans ce chapitre démontrent que le réseau proposé est la solution adéquate à la problématique citée en chapitre 2.

Conclusion générale

Conclusion

En conclusion, ce mémoire a examiné l'importance de la redondance LAN et WAN dans les réseaux informatiques d'entreprises. Nous avons constaté que la redondance joue un rôle crucial dans la garantie de la disponibilité, de la fiabilité et des performances des réseaux. Comme il nous a permis d'acquérir beaucoup d'information sur la situation de réseau LAN du complexe Cevital ainsi de pratiquer nos nouvelles acquisitions théoriques et comprendre au mieux le fonctionnement de ce réseau durant notre période de stage, à cet effet nous avons proposé des solutions afin d'avoir une infrastructure réseau opérationnelle et idéale, en s'appuyant sur la redondance des matériels et des liaisons tout en assurant la continuité de service.

Afin d'atteindre le résultat escompté, nous avons choisi de simuler notre réseau physique virtuel en utilisant Cisco Packet Tracer 8.2, pour les divers avantages qu'il présente notamment la simplicité de la configuration des équipements et protocoles dont on a besoin.

En ce qui concerne la redondance LAN, nous avons exploré différentes techniques telles que la configuration des liens agrégés, la mise en place de boucles redondantes et l'utilisation de protocoles de spanning-tree. Ces approches permettent de fournir des chemins alternatifs aux données, évitant ainsi les points de défaillance uniques et minimisant les temps d'arrêt en cas de panne. Puis en redondance WAN, nous avons examiné les solutions telles que les connexions doubles ou multiples avec des fournisseurs de services Internet, les protocoles de routage dynamique avec la mise en place de liens de secours. Ces mesures de redondance WAN garantissent une connectivité continue et une disponibilité accrue des services, même en cas de défaillance d'un lien ou d'un fournisseur.

Nous avons également discuté des avantages et des considérations liées à la mise en œuvre de la redondance LAN et WAN. Parmi les avantages, citons la réduction des temps d'arrêt, l'amélioration des performances, la capacité de tolérance aux pannes, la gestion efficace du trafic et la meilleure satisfaction des utilisateurs finaux. Cependant, il est important de prendre en compte les coûts et la complexité associés à la mise en place de la redondance, ainsi que de maintenir une gestion efficace pour assurer son bon fonctionnement. Avec une planification et une mise en œuvre adéquates, la redondance LAN et WAN peut être un atout précieux pour les entreprises qui dépendent de leurs réseaux informatiques pour leurs opérations quotidiennes.

Bien que notre projet ait apporté des éclairages significatifs sur l'efficacité de la redondance sur les réseaux d'entreprise, il reste des questions en suspens concernant l'impact des différentes configurations de réseau sur les performances spécifiques à chaque industrie. Des études supplémentaires pourraient être entreprises pour mieux comprendre ces nuances. Et plusieurs perspectives méritent d'être explorées pour améliorer davantage la mise en place d'un réseau redondant, telles que l'automatisation des configurations, le passage vers des liaisons sans fils tout en prenant en considération le côté sécurité, et finalement l'utilisation de l'Ip_Map qui permet la représentation visuelle des adresses IP sur la carte géographique de l'entreprise ce qui facilite la gestion des réseaux et des ressources.

ANNEXE

1. Présentation et utilisation de Packet Tracer

Packet Tracer est un logiciel de CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc.

2. Description générale

La figure 1 montre un aperçu général de Packet Tracer. La zone (1) est la partie dans laquelle le réseau est construit. Les équipements sont regroupés en catégories accessibles dansla zone (2). Une fois la catégorie sélectionnée, le type d'équipement peut être sélectionné dans la zone (3).

La zone (6) contient un ensemble d'outils :

- Select : pour déplacer ou éditer des équipements.
- Move Layout : permet de déplacer le plan de travail.
- Place Note : place des notes sur le réseau.
- Delete : supprime un équipement ou une note.
- Inspect : permet d'ouvrir une fenêtre d'inspection sur un équipement (tableARP, routage).

La zone (5) permet d'ajouter des indications dans le réseau. Enfin, la zone (4) permet de passer du mode temps réel au mode simulation.

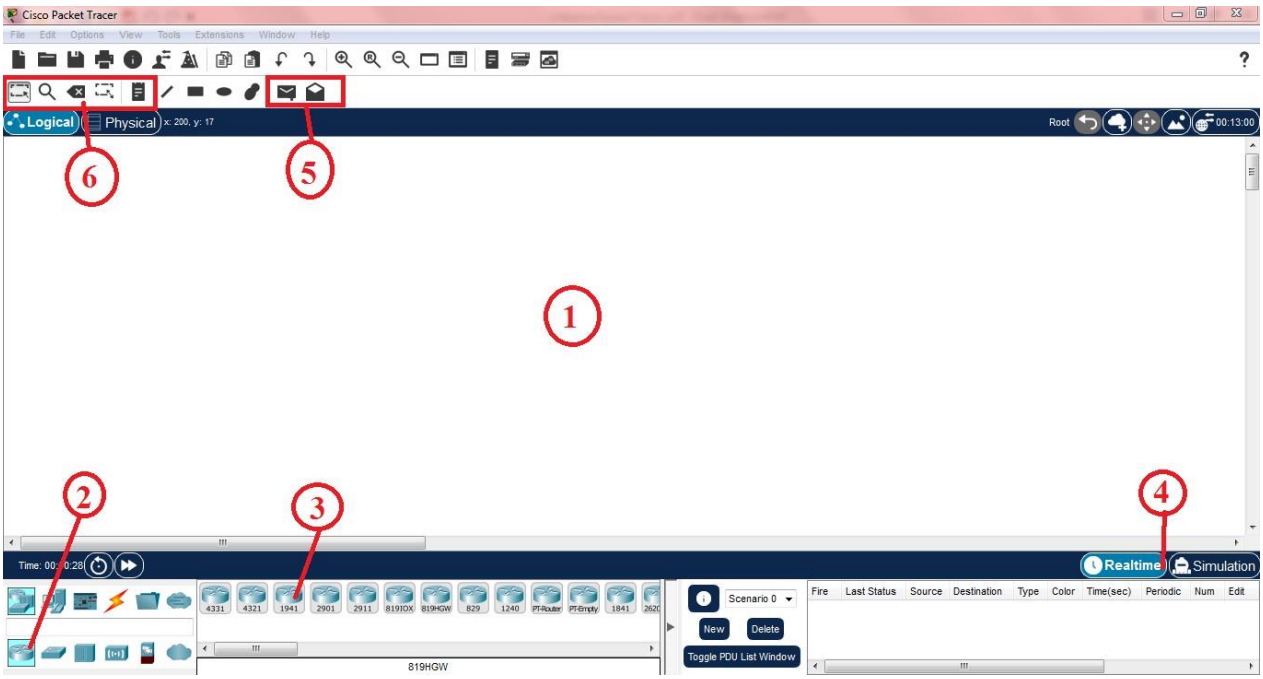
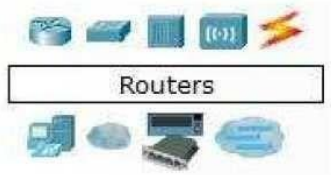


Figure 1 : environnement de Cisco Packet Tracer.

3. Construire un réseau

Pour construire un réseau, l'utilisateur doit choisir parmi les 8 catégories proposées par Packet Tracer : les routeurs, les switchs, les hubs, les équipements sans-fil, les connexions, les équipements dits terminaux (ordinateurs, serveurs), des équipements personnalisés et enfin, uneconnexion multi-utilisateurs. Lorsqu'une catégorie est sélectionnée, l'utilisateur a alors le choix entre plusieurs équipements différents. Pour ajouter un équipement, il suffit de cliquer dessus puis de cliquer à l'endroit choisi.

La figure 2 correspond à la zone décrite.



Types d'équipements

Les différentes connexions proposées

Figure 2 : outils de construction d'un réseau.

Pour relier deux équipements, il faut choisir la catégorie "Connections" puis cliquer sur la connexion désirée. Dans nos différents travaux pratiques, nous n'utilisons que 2 sortes de connexions : les câbles droits (Copper Straight- Through) et les câbles croisés (Copper Cross-Over). Ils sont en position 3 et 4 sur la partie droite de la figure 2.

4. Configuration d'un équipement

✓ Configuration d'un PC

Lorsqu'un ordinateur a été ajouté (appelé PC-PT dans Packet Tracer), il est possible de le configurer en cliquant dessus, une fois ajouté dans le réseau. Une nouvelle fenêtre s'ouvre comportant 5 onglets : Physical (aperçu réel de la machine et de ses modules), Config (configuration passerelle, DNS et adresse IP) et Desktop (ligne de commande ou navigateur Web).

Dans l'onglet Config, il est possible de configurer la passerelle par défaut, ainsi que l'adresse du serveur DNS (cliquez pour cela sur le bouton Settings en-dessous du bouton Global). Il est possible aussi de configurer l'adresse IP et le masque de sous-réseau (cliquez pour cela sur le bouton FastEthernet en- dessous du bouton INTERFACE), comme il est possible de le configurer sur l'onglet Desktop puis IP configuration comme sur la figure suivante :

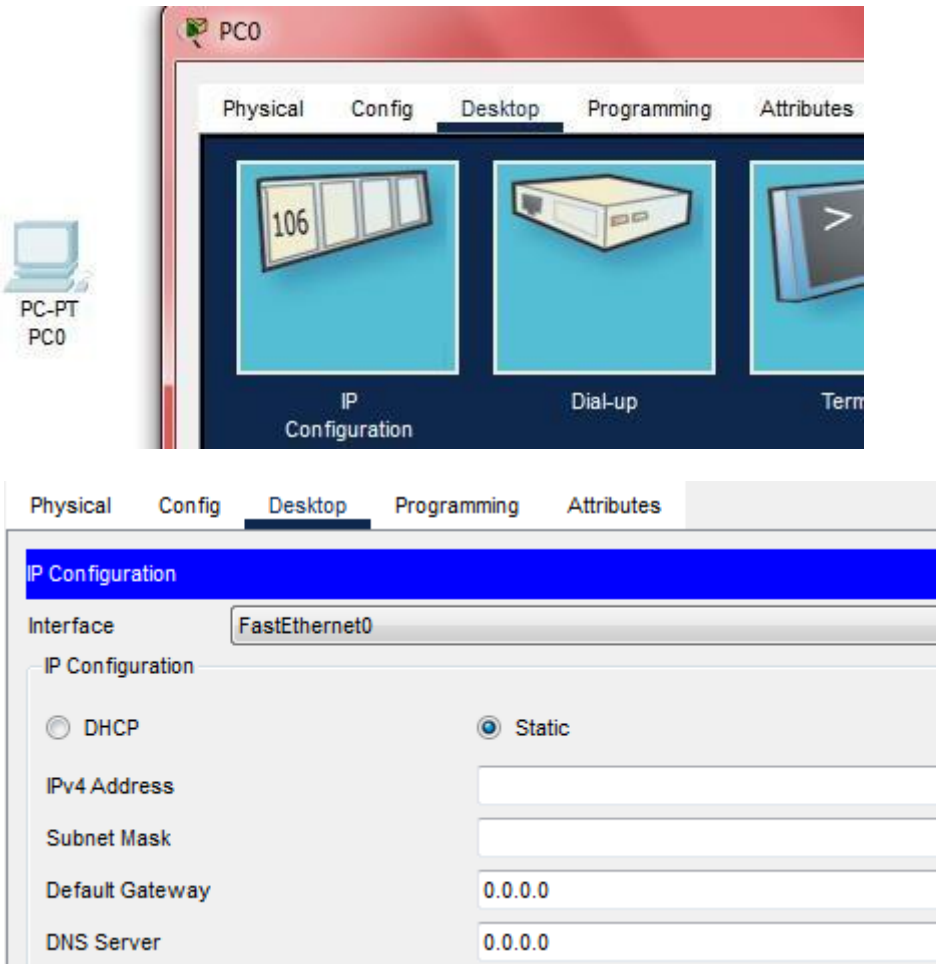


Figure 3 : configuration d'un PC sur Desktop.

- ✓ **Configuration d'un switch**

Une fois l'équipement est ajouté, pour le configurer on clique dessous et une fenêtre s'ouvre comportant onglets physical (aperçu réel de la machine et de ses modules), config (configuration globale, configurations des interfaces du switch), CLI (une interface virtuelle que les équipements utilisent comme système d'exploitation pour les configurations), attributes.

L'onglet CLI est généralement utilisé pour configurer l'équipement (que ce soitun switch ou routeur). Ça permet de configurer les interfaces (attribution des adresses IP, les activer, etc.).

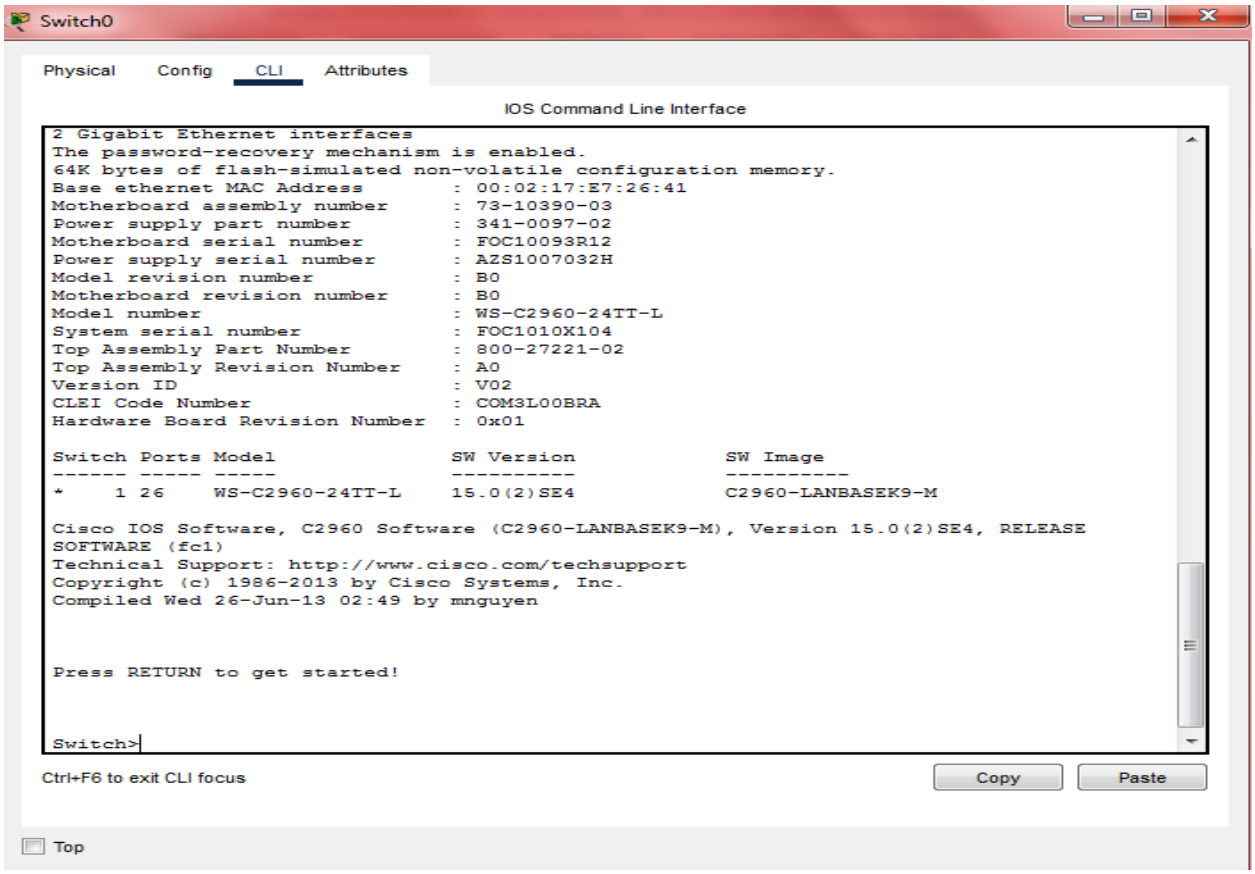
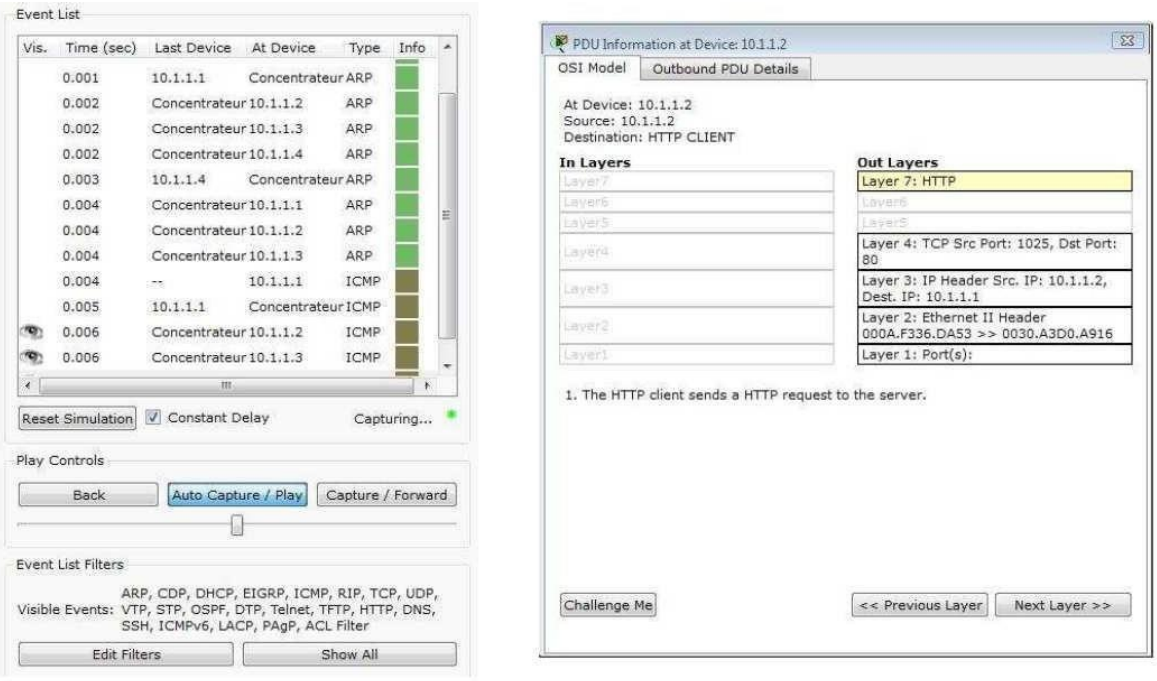


Figure 4 : onglet CLI.

5. Mode simulation

Une fois le réseau créé et prêt à fonctionner, il est possible de passer en mode simulation, ce qui permet de visualiser tous les messages échangés dans le réseau. En mode simulation, la fenêtre principale est scindée en deux, la partie de droite permettant de gérer le mode simulation:exécution pas-à-pas, vitesse de simulation, protocoles visibles. La partie gauche de la figure 4 montre la partie simulation et sa partie droite montre les détails obtenus en cliquant sur un message (ici HTTP).



Partie simulation *Détails sur un paquet*

Figure 5 : fenêtre de mode de simulation.

6. Invite de commandes

Il est possible d'ouvrir une invite de commandes sur chaque ordinateur du réseau. Elle est accessible depuis le troisième onglet, appelé Desktop, accessible lorsque l'on clique sur un ordinateur pour le configurer (mode sélection). Cet onglet contient un ensemble d'outils dont l'invite de commandes (Command prompt) et un navigateur Internet (Web Browser).

L'invite de commandes permet d'exécuter un ensemble de commandes relatives au réseau. La liste est accessible en tapant help. En particulier, les commandes ping, arp, tracert et ipconfig sont accessibles. Si Packet Tracer est en mode simulation, les messages échangés suite à un appel à la commande ping peuvent ainsi être visualisés.

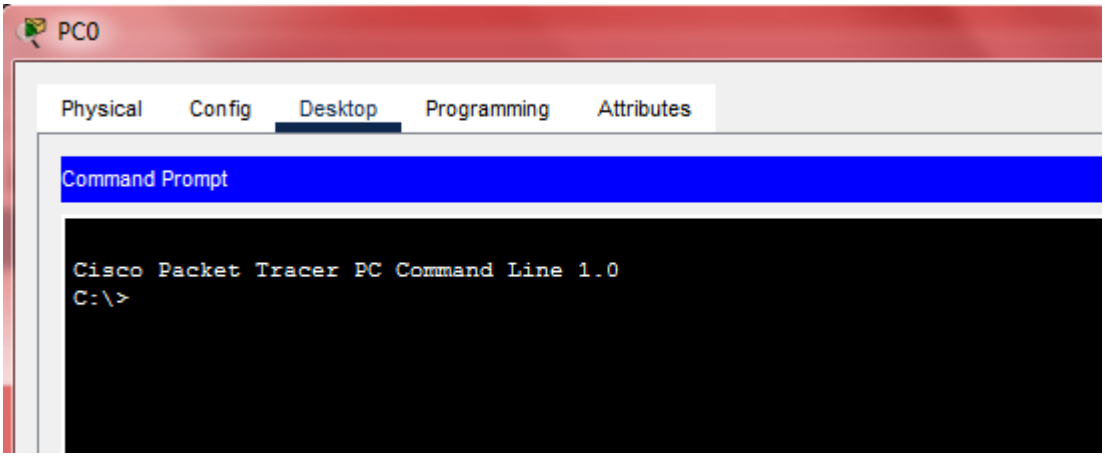


Figure 6 : command prompt

Bibliographie

[10]Waterman, R., Lahaye, B., Romascanu, D., & Waldbusser, S. (1999). RFC2613: Remote Network Monitoring MIB Extensions for Switched Networks Version 1.0.

[11]Freed, N. (2000). Behavior of and requirements for Internet firewalls (No. rfc2979).

[14]Pujolle, G. (2014). Les réseaux. Editions Eyrolles.

[18]Dromard, D., & Seret, D. (2013). Architecture des réseaux. Pearson Education France.

[19]Forouzan, B. A. (2007). Data communications and networking. Huga Media.

[20]Bradley, R. (2001). Understanding computer science for advanced level: the study guide (Cheltenham: Nelson Thornes) (p. 244). ISBN 978-0-7487-6147-0.

[23]Postel, J. (1980). RFC 760. Internet Protocol.

[25]Socolofsky, T., & Kale, C. (1991). A TCP/IP Tutorial. RFC 1180. United States.

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

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

[28]Atkinson, R. J., & Bhatti, S. N. (2012). Address resolution protocol (ARP) for the identifier-locator network protocol for IPv4 (ILNPv4) (No. rfc6747).

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

[31]Hoffman, P., Sullivan, A., & Fujiwara, K. (2019). RFC 8499: DNS Terminology.

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

[36]Reynolds, J. K., & Postel, J. (1983). RFC0870: Assigned numbers.

[39]Informations interne de l'entreprise Cevital

[43]Nadas, S. (Ed.). (2010). Rfc 5798: Virtual router redundancy protocol (vrrp) version 3 for ipv4 and ipv6.

[45]Li, T., Cole, B., Morton, P., & Li, D. (1998). Cisco hot standby router protocol (HSRP) (No. rfc2281).

[47]Zhang, M., Wen, H., & Hu, J. (2016). Spanning tree protocol (STP) application of the inter-chassis communication protocol (ICCP) (No. rfc7727).

[51]Savage, D., Ng, J., Moore, S., Slice, D., Paluch, P., & White, R. (2016). Cisco's enhanced interior gateway routing protocol (EIGRP) (No. rfc7868).

[52]Moy, J. (1998). Open Shortest Path Fast (OSPF) Version 2. *RFC2328*.

[53] Jesin, A. (2014). Packet Tracer Network Simulator. Packt Publishing Ltd.

Webographie

[1] https://www.techno-science.net/definition/3799.html (consulté le 11/02/2023)

[2] https://techno-skills.com/reseaux/les-fondamentaux/composants-reseau/ (consulté le25/02/2023)

[3] http://dlr13.free.fr/Reseaux/medias.htm (consulté le 25/02/2023)

[4]https://cableriedaumesnilblog.com/le-cable-de-cuivre-nu-proprietes-et-utilisations

[5]https://www.futura-sciences.com/tech/definitions/electronique-cable-coaxial-4388/ (consulté le 28/02/2023)

[6] https://fr.theastrologypage.com/twisted-pair-cable (consulté le 28/02/2023)

[7]https://www.futura-sciences.com/tech/definitions/informatique-fibre-optique-18133/ (consulté le 28/02/2023)

[8]https://www.techno-science.net/definition/7260.html (consulté le 02/03/2023)

[9]https://techno-skills.com/reseaux/les-fondamentaux/composants-reseau/ (consulté le 02/03/2023)

[10]https://fr.wikipedia.org/wiki/Hub_Ethernet (consulté le 02/03/2023).

[12]https://www.cisco.com/c/fr_ca/solutions/small-business/resource-center/networking/what-is-access-point.html (consulté le 05/03/2023)

[13]http://hautrive.free.fr/reseaux/architectures/protocoles-de-reseaux.html (consulté le05/03/2023)

[15]http://chloecabot.com/mmi/M1203/synthese_reseaux.html (consulté le 18/02/2023)

[16]https://waytolearnx.com/2019/06/topologie-reseau-en-bus.html (consulté le 18/02/2023)

[17]https://www.techtarget.com/searchnetworking/definition/star-network(consulté le 09/03/2023)

[21]http://eventus-networks.blogspot.com/2013/11/les-topologies-physiques-et-logiques.html (consulté le 20/04/2023)

[22]https://www.frameip.com/osi/ (consulté le 05/03/2023)

[24]https://cisco.goffinet.org/ccna/fondamentaux/protocoles-modeles-communication/#1-d%C3%A9finition-dun-protocole-de-communication (consulté le 16/04/2023)

[32]https://fr.wikipedia.org/wiki/R%C3%A9seau_local_virtuel (consulté le 14/03/2023)

[33]https://www.fingerinthenet.com/vlan/ (consulté le 14/03/2023)

[35]https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml/ (consulté le 09/06/2023)

[37]https://www.ionos.fr/digitalguide/serveur/know-how/adresse-de-broadcast/ (consulté le 15/03/2023)

[38]https://fr.ryte.com/wiki/Sous-r%C3%A9seau (consulté le 07/03/2023)

[40]https://www.algerietelecom.dz/fr/entreprises/rms-reseau-multiservices-prod24 (consultéle 13/05/2023)

[41]https://www.ionos.fr/digitalguide/serveur/securite/redondance/ (consulté le 22/03/2023)

[42]https://ccnareponses.com/notions-de-base-sur-la-commutation-le-routage-et-sans-fil-modules-9-concepts-du-fhrp-protocoles-de-redondance-au-premier-saut/ (consulté le 22/03/2023)

[46]https://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glbp.html (consulté le 23/03/2023)

[48]https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html (consulté le13/04/2023)

[49]https://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/12023-4.html (consulté le 09/06/2023)

[50]https://www.cloudflare.com/fr-fr/learning/network-layer/what-is-routing/ (consulté le17/04/2023)

Références des figures

[F1] https://formip.com/reseau-kesako/
[F2] https://www.researchgate.net/figure/Examples-of-transmission-media_fig3_328006364
[F3] https://formip.com/composants-routeur/
[F4] https://techno-skills.com/reseaux/les-fondamentaux/composants-reseau/
[F5] https://www.techno-science.net/definition/3746.html
[F6] https://waytolearnx.com/2019/06/qu-est-ce-qu-un-pare-feu.html
[F7] https://www.youtechinfo.com/produit/d-link-point-dacces-wifi-dap-1360-300mbps/
[F8] https://moncoursenligne.fr/reseaux/
[F9] https://www.geonov.fr/architecture-client-serveur/
[F10] http://papynet.eklablog.com/reseaux-poste-a-poste-et-blockchains-a127867464
[F11] https://waytolearnx.com/2019/06/topologie-reseau-en-bus.html
[F12] https://www.researchgate.net/figure/Topologie-en-etoile_fig7_350340759
[F13] http://www.materiel-informatique.be/anneau.php
[F14] https://www.researchgate.net/figure/Topologie-maillee-Topologie-arborescente-offre-des-liens-dedies-qui-permettent-de_fig6_350340759
[F15] https://sti2d.ecolelamache.org/ii_rseaux_informatiques___7_topologie_des_rseaux.html
[F16] https://waytolearnx.com/2018/07/difference-entre-le-modele-tcp-ip-et-le-modele-osi.html
[F17] https://www.ionos.fr/digitalguide/serveur/know-how/presentation-de-tcp/
[F18] http://ccna4ever.22web.org/ccna3_final/v2/ccna3%20v2.htm?i=1
[F19] https://math.univ-lyon1.fr/irem/Formation_ISN/formation_reseau/couche_reseau/masque.html
[F20] https://www.fingerinthenet.com/wildcard/
[F21] https://waytolearnx.com/2019/06/adresse-de-diffusion.html
[F22] https://www.cisco.com/c/en/us/support/switches/catalyst-4500-series-switches/series.html
[F23] https://www.cisco.com/c/en/us/support/switches/catalyst-2960-series-switches/series.html
[F24] https://www.cisco.com/c/fr_ca/support/routers/2900-series-integrated-services-routers-isr/series.html
[F25] https://www.logiscenter.fr/mod-ruckus-r500-zoneflex-series
[F26] https://www.ldlc.pro/fiche/PB00405079.html
[F27] https://www.legrand.dz/fr/espaces/data-center-pme
[F28] Https://www.it-connect.fr/mise-en-place-du-protocole-hsrp
[F29] https://formip.com/portfast-bpdu-guard/
[F30] https://formip.com/dtp/
[F31] Https://mondiluca.files.wordpress.com/2018/03/ppe4.pdf
[F32] https://www.it-connect.fr/chapitres/les-zones-ospf/
[F33] https://packet-tracer.fr.softonic.com/

Résumé

En résumé, la haute disponibilité est un aspect essentiel de la conception et de la gestion des systèmes informatiques et des services. Elle permet d'assurer la continuité des opérations, de réduire les interruptions coûteuses et d'offrir une expérience utilisateur fiable et sans failles. Pour cela, la présente étude consiste à désigner une solution de haute disponibilité et d'équilibre des charges au niveau du réseau local et étendu de Cevital-Béjaïa en utilisant le protocole HSRP, cette solution consiste à mettre en place une redondance (liens et équipements) dans le réseau.

A l'aide du simulateur Packet Tracer, une architecture hiérarchique interconnectant différents VLANs est proposée assurant ainsi la haute disponibilité afin de faciliter la communication entre les stations.

Mots clés : réseau local, haute disponibilité, Cevital, VLAN's, HSRP.

Abstract

In summary, high availability is an essential aspect of designing and managing IT systems and services. It helps to ensure business continuity, reduce costly downtime, and deliver a reliable, seamless user experience. For this, the present study consists in designating a solution of extended high availability and load balancing at the level of the local network and wide area network of Cevital-Béjaïa using the HSRP protocol, this solution consists in setting up a redundancy (links and equipments) in the network.

Using the Packet Tracer simulator, a hierarchical architecture interconnecting different VLANs is proposed, thus ensuring high availability in order to facilitate communication between stations**.**

Keywords: local network, high availability, Cevital, VLANs, HSRP.