République Algérienne Démocratique et Populaire
الجمهورية الجزائرية الديمقراطية الشعبية
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
وزارة التعليم العالي والبحث العلمي

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Université A/Mira de Bejaia
Faculté des sciences exactes
Département Informatique

Mémoire de projet de fin de cycle
Pour l'obtention du diplôme de Master en informatique
Spécialité : Administration et Sécurité des Réseaux Informatiques

Thème

Proposition d'une configuration sécurisée d'un réseau local - cas d'étude : CEVITAL, Béjaia.

Réalisé par :
- BEDHOUCHE Salma
- YOUSFI Abdenour

Encadré par :
- Dr. BOUDRIES Abdelmalek

Jury composé de :

Président	Dr. SADI Mustapha	U. A/Mira Bejaia
Examinateur	Dr. BOUZIDI Zair	U. A/Mira Bejaia

Promotion : 2021 / 2022

Dédicaces

Nous dédions ce travail,

***À** nos familles, pour leur soutien et leurs sacrifices durant toutes ces années d'étude. Ils nous ont doté d'une éducation digne, leur dévouement leur amour et parfois leur rigueur, ont fait de nous ce que nous sommes aujourd'hui.*

***À** nos pères et mères particulièrement, en guise de gratitude et de reconnaissance, que ce travail soit le meilleur cadeau que nous puissions leur offrir.*

***À** tous nos frères et sœurs, proches et amis qui nous ont encouragé et aidé de près ou de loin.*

Remerciements

Nous nous devons de remercier ALLAH le tout puissant pour toute la volonté et le courage qu'il nous a donné pour l'achèvement de ce travail.

Nous tenons à remercier en premier lieu notre encadreur, Monsieur le **BOUDRIES Abdelmalek** qui a bien voulu accepter de diriger et d'encadrer notre PFE, pour sa patience, ses sacrifices, ses conseils et l'aide qu'il nous a fourni tout au long de l'année, pour ses qualités humaines et scientifiques qui nous ont toujours motivé à faire plus.

Nous remercions également les membres de jury pour l'intérêt qu'ils ont porté à notre modeste travail en acceptant de l'examiner et de l'enrichir par leurs précieuses propositions.

Nous tenons aussi à remercier chaleureusement Monsieur **ARAB Younes**, notre encadreur de stage, qui a été à notre coté et qui nous a aidé par ses conseils et ses présences auprès de nous, nous lui souhaitons le bon courage pour la continuation dans ses projets.

Nous aimerions adresser un remerciement particulier à tout le personnel et à tous les travailleurs de l'entreprise **Cevital**, qui ont été toujours à notre service.

Enfin, nous remercions l'ensemble du personnel du département d'informatique et tout le corps professoral de l'Université Abderrahmane Mira de Bejaia pour la qualité de leur enseignement et pour les valeurs qu'ils nous ont inculquées et tous ceux qui ont contribué de près ou de loin à la concrétisation de ce travail.

Sommaire

Sommaire …… i

Liste des figures …….. iii

Liste des tableaux …… .viii

Liste des abréviations …… ix

Introduction Générale……..... 1

Chapitre I : Généralité Sur Les Réseaux Informatique

Introduction ……..... 2

I.1.Définiton d'un réseau ……... 2

I.2.Classifcation des réseaux informatique ……... 2

I.2.1. Classification selon leur taille …….. 2

I.2.2. Classification selon l'architecture des réseaux ……... 3

I.2.3. Classification selon leur topologie ……... 4

I.3. Les équipements d'interconnexion ……..... 7

I.4. Les équipements terminaux …..... 10

I.5. Les supports de transmission …..... 10

I.5.1. Câbles réseaux …..... 10

I.5.2. Transmission sans fil …..... 13

I.6. Modèle général de communication …..... 13

I.6.1. Le modèle OSI (Open System Interconnected) …… 13

I.6.2. le modèle TCP/IP …..... 15

I.7. Les protocoles réseaux …..... 16

I.8. L'adressage IPv4 (Internet Protocol version 4) ……... 17

Conclusion …..... 20

Chapitre II : La Sécurité d'un Réseau Local

Introduction …..... 21

II.1. Définition de la sécurité des réseaux …..... 21

II.2. Objectifs de la sécurité …..... 21

II.3. Domaines d'application de la sécurité informatique …..... 21

II.4. Les attaques …..... 23

II.4.1. Outils et types d'attaques …..... 23

II.5. Principes de sécurité sur un réseau local …..... 24

II.5.1. Sécurité des communications …..... 25

II.5.1.1. VLAN (Virtual Local Area Network) …..... 25

II.5.1.2. Pare-feu (firewalls) ……... 27

II.5.1.3. IDS & IPS ……... 28

II.5.1.4. DMZ (demilitarized zone) …..... 29

II.5.1.5. VPN (Virtuel Privat Network) …..... 29

II.5.1.6. IPSec (Internet Protocol Security) …..... 30

Sommaire

II.5.2. Sécurité au niveau des commutateurs …. 30
II.5.2.1. mécanisme de sécurité de port (port-Security) …. 30
II.5.3. DHCP Snooping …. 30
II.5.4. STP (Protocole Spanning Tree) …. 31
II.6. Sécurité des accès à l'administration du commutateur …… 31
II.6.1. Telnet …. 31
II.6.2. SSH ……..……..... 31
Conclusion …. 32

Chapitre III : Réalisation des solutions proposées
Introduction …. 33
III.1. Presentation de l'organisme d'accueil …. 33
III.1.1. Présentation de l'entreprise et de son historique …. 33
III.1.2. Vision, Mission du Groupe Cevital …. 35
III.1.3. Valeurs du Groupe Cevital …. 35
III.1.4. Codification des équipements de Cevital …. 35
III.1.5. Utilisation du réseau informatique …. 35
III.1.6. Situation géographique …. 35
III.1.7. Infrastructure matériel …. 36
III.1.8. La sécurité au niveau de Cevital …. 37
III.1.9. Les Vlans par direction …. 37
III.2.Présentation de simulateur « Cisco Packet Tracer » …. 37
III.3. La réalisation …. 39
III.3.1. Le matériel utilisé …. 39
III.3.2. Les étapes de simulation …. 40
III.3.2.1. configuration entière du réseau ……..…..……..40
III.3.2.2. Sécuriser le réseau …. 56
Conclusion …. 64

Conclusion générale …. 65
Références bibliographiques …. 66
Résumé

Liste des figures

Figure I.1 : Types de réseaux …… 3

Figure I.2 : Architecture poste à poste …… 4

Figure I.3 : Architecture client/serveur …… 4

Figure I.4 : Topologie en bus …… 5

Figure I.5 : Topologie en étoile …… 5

Figure I.6 : Topologie en anneau …… 6

Figure I.7 : Topologie en arbre …… 6

Figure I.8 : Topologie maillée …… 6

Figure I.9 : Le répéteur …… 7

Figure I.10 : Le pont …… 8

Figure I.11 : Le routeur …… 8

Figure I.12 : La carte réseau …… 8

Figure I.13 : Le Hub …… 9

Figure I.14 : Le commutateur (Switch) …… 9

Figure I.15 : Le modem (Modulateur-Démodulateur) …… 9

Figure I.16 : Câble paire torsade non blindée (UTP) …… 10

Figure I.17 : Câble paire torsadée blindée (STP) …… 11

Figure I.18 : Câble coaxial …… 11

Figure I.19 : Câble fibre optique …… 11

Figure I.20 : Fibre optique multimode …… 12

Figure I.21 : Fibre optique monomode …… 12

Figure I.22 : Représentation de modèle OSI…… 14

Figure I.23 : L'architecture en couche de modèle TCP/IP …… 15

Figure I.24 : Structure de l'adresse IPv4 …… 17

Figure I.25 : Constitution d'une adresse IPv4 …… 17

Figure I.26 : La classe d'adresse A …… 19

Figure I.27 : La classe d'adresse B …… 19

Figure I.28 : La classe d'adresse C …… 19

Liste des figures

Figure I.29 : La classe d'adresse D …….. 19

Figure I.30 : La classe d'adresse E……... 20

Figure II.1 : Domaines d'application de la sécurité ……... 22

Figure II.2 : Exemple de VLANs …… 25

Figure II.3 : VLANs en mode Trunk …….. 26

Figure II.4 : Le VTP Client et VTP Serveur …….. 27

Figure II.5 : Un pare-feu (Firewall) …… 27

Figure II.6 : IDS & IPS ……. 28

Figure II.7 : DMZ …….. 29

Figure II.8 : VPN ……... 29

Figure III.1 : Logo de Cevital …….. 33

Figure III.2 : Organigramme général du Groupe Cevital……. 34

Figure III.3 : Direction du système d'information …… 34

Figure III.4 : Carte géographique de Cevital Bejaia ……. 36

Figure III.5 : Interface Cisco Packet Tracer …….. 38

Figure III.6 : Interface CLI …….. 38

Figure III.7 : L'architecture proposée de Cevital sous Packet Tracer …..…….. 39

Figure III.8 : Représentation des couches de réseau proposé ……... 40

Figure III.9 : Configuration du nom ……... 40

Figure III.10 : Création des VLANs …… 41

Figure III.11 : Vérification de la création des VLANS …….. 41

Figure III.12 : La mise des interfaces en mode Trunk …….. 41

Figure III.13 : Les interfaces en mode Trunk …… 42

FigureIII.14 : Configuration de VTP serveur …… 42

Figure III.15 : Configuration de VTP clients ……. 42

Figure III.16 : Les clients VTP (Switch2-Distribution) ……. 43

Figure III.17 : Les clients VTP (Switch1-Accés) …… 43

Figure III.18 : Les clients VTP (Switch2-Accés) …… 43

Figure III.19 : Représentation des VTPs sur L'architecture réseau …… 44

Liste des figures

Figure III.20 : Configuration de l'Etherchannel …… 44

Figure III.21 : Vérification de la configuration d'Etherchannel ……. 45

Figure III.22 : Les boucles bloquées par le STP ……. 45

Figure III.23 : Configuration de STP au niveau de switch1-Distribution ……... 45

Figure III.24 : Configuration de STP au niveau de switch2-Distribution ……... 46

Figure III.25 : Résultat de la configuration de STP ……... 46

Figure III.26 : Exclusion des adresses au niveau de Switch1-Distribution …….. 46

Figure III.27 : Vérification des adresses exclure sur le Switch1-Distribution …… 47

Figure III.28 : Exclusion des adresses au niveau de Switch2-Distribution …….. 47

Figure III.29 : Vérification des adresses exclure sur le Switch2-Distribution …… 47

Figure III.30 : Les pools d'adresse pour les VLANs …….. 48

Figure III.31 : Attribution des adresses IP aux interfaces des VLANs …… 48

Figure III.32 : Vérifications de l'arrivée des adresses ……... 48

Figure III.33 : L'ajout des passerelles par défauts …… 48

Figure III.34 : Attribution des ports au VLANS …… 49

Figure III.35 : Vérification de l'attribution des ports aux VLANs …….. 49

Figure III.36 : Le mode trunk et allocation des VLANs …… 49

Figure III.37 : Vérification de l'activation du mode trunk ……... 50

Figure III.38 : Interfaces de configuration du pc ……... 50

Figure III.39 : Activation de DHCP …… 50

Figure III.40 : Configuration de HSRP au niveau du Switch1-Distribution ……... 51

Figure III.41 : Configuration de HSRP au niveau du Switch2-Distribution ……... 51

Figure III.42 : Ping continue …… 52

Figure III.43 : Représentation de passage de VLANs sur son root-bridge ……. 52

Figure III.44 : Fonctionnement de HSRP après avoir désactivé les ports …..……. 53

Figure III.45 : Le Ping après avoir désactivé les ports …..…… 53

Figure III.46 : Ping après la reprise de Switch1-Destribution …….. 54

Figure III.47 : Les ports de niveau 2 qu'on doit passer au niveau 3 …… 54

Figure III.48 : Configuration des ports de niveau 2 …….. 55

Liste des figures

Figure III.49 : Montrer la configuration des ports …… 55

Figure III.50 : Configuration de l'OSPF dans la couche Cœur …… 55

Figure III.51 : Vérifié la configuration de l'OSPF …… 55

Figure III.52 : Configuration de l'OSPF dans la couche Distribution …… 56

Figure III.53 : Vérifié la configuration de l'OSPF …… 56

Figure III.54 : Testé la connectivité des deux réseaux avec le Ping …….. 56

Figure III.55 : Configuration de la sécurité d'exécution privilégiée …… 57

Figure III.56 : Vérification de la configuration …….. 57

Figure III.57 : Configuration chiffrée …… 57

Figure III.58 : Vérification de la configuration …….. 57

Figure III.59 : Configuration des lignes consoles ……... 57

Figure III.60 : Vérifie la configuration des lignes consoles ……... 57

Figure III.61 : Configuration des lignes virtuelles …… 58

Figure III.62 : Vérifie la configuration des lignes virtuelles …… 58

Figure III.63 : Accéder à distance via le PC5 avec Telnet …… 58

Figure III.64 : Chiffrés les mots de passes …….. 58

Figure III.65 : Les mots de passe cryptés …… 59

Figure III.66 : Configuration de l'SSH ……... 59

Figure III.67 : Vérification de la configuration de l'SSH …….. 59

Figure III.68 : Accéder à distance via le PC7 avec SSH …… 60

Figure III.69 : L'architecture réseau avant la configuration de STP GUARD ……... 60

Figure III.70 : Configuration du STP BPDUGUARD ……... 61

Figure III.71 : L'architecture réseau avant la configuration de STP GUARD ……... 61

Figure III.72 : Désactivation des ports …… 62

Figure III.73 : Placement des interfaces désactivés dans un VLAN non utilisé …….. 62

Figure III.74 : Montrer les interfaces désactivées …….. 62

Figure III.75 : La configuration de port-Security …….. 62

Figure III.76 : Vérification le fonctionnement de la configuration …….. 63

Figure III.77 : Configuration de DHCP Snooping ……..……... 63

Liste des figures

Figure III.78 : Vérification de la configuration de DHCP Snooping …….……. 64

Figure III.79 : Afficher les clients DHCP avec leurs adresses ……...….. 64

Liste des tableaux

Liste des tableaux

Tableau I .1 : Valeur des débits suivant la nature des informations …… 13
Tableau I.2 : Caractéristiques des déférents supports …….. 13
Tableau I.3 : Tableau représentatif de services et protocoles des couches du modèle OSI……... 15
Tableau I.4 : Tableau représentatif de modèle TCP/IP..…….…….. 16
Tableau I.5 : Représentation de valeurs des bits du masque en valeurs numériques … 18
Tableau I.6 : Exemple de la division d'une adresse IPv4 …….. 18
Tableau I.7 : Réseau privé …… 20

Tableau III.1 : Les modèles de switches constituée l'entreprise ……... 36
Tableau III.2 : Classification des Vlans de l'entreprise Cevital ……... 37

Liste des abréviations

PAN	Personnel Area Network
LAN	Local Area Network
MAN	Metropolitan Area Network
RAN	Regional Area Network
WAN	Wide Area Network
FDDI	Fiber Distributed Data Interface
UTP	Unshielded Twisted Pair
STP	Shielded Twisted Pair
OSI	Open System Iterconnected
ISO	International Organisation for Standardization
ARP	Address Resolution Protocol
RARP	Reverse Address Resolution Protocol
ICMP	Internet Control Message Protocol
DHCP	Dynamic Host Configuration Protocol
IP	Internet Protocol
IGMP	Internet Group Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
HSRP	Hot Standby Routing Protocol
OSPF	Open Shortest Path First
IPv4	Internet Protocol version 4
VLAN	Virtual Local Area Network
DTP	Dynamic Trunking Protocol

Liste des abréviations

VTP	Vlan Trunking Protocol
NVRAM	Non –Volatile Random-Access Memory
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
DMZ	Demilitarized Zone
VPN	Virtuel Privat Network
IPsec	Internet Protocol Security
STP	Protocol Spanning Tree
BPDU	Bridge Protocol Data Unit
SSH	Secure SHell

Introduction Générale

Aujourd'hui, les réseaux informatiques sont indispensables dans tous les domaines de la vie, y compris la banque, l'assurance, la sécurité, Internet, la santé, l'administration, transports...etc. Il est essentiel pour toute organisation de faciliter la transmission, la duplication et le partage des fichiers et des périphériques. Cela permet le traitement et la consultation des bases de données et une transmission rapide et fiable.

Dans un environnement hautement concurrentiel, les entreprises doivent développer de nouvelles technologies de survie pour s'adapter. Ainsi, les entreprises construisent non seulement leurs propres réseaux locaux, mais surtout, profitent de nouveaux services qui facilitent la communication et l'accès des employés depuis les stations du réseau local ou un ensemble de réseaux bien définis et invisibles de l'extérieur pour réduire les coûts, les distances et gagner du temps dans le partage de données.

L'évolution rapide de l'interconnexion des réseaux d'entreprises, la croissance phénoménale du nombre d'entreprises connectées à Internet et l'utilisation des outils informatiques pour effectuer des tâches importantes liées à la mission des entreprises placent les gestionnaires des technologies de l'information et, en particulier, les gestionnaires de réseaux informatiques devant l'obligation de se former en matière de sécurité des réseaux.

La sécurité ne consiste pas seulement à protéger des équipements, mais également à protéger les informations. Puisque les données (informations) de l'entreprise représentent plus grande richesse. Celles-ci sont de plus en plus volumineuses et sont entreposées dans des réseaux de stockage de données. Donc elles doivent être protégées efficacement contre le vol, la perte ou l'altération.

Il est important de respecter les normes, les règles et les politiques de sécurité. Cela assure la protection des données et des informations personnelles des individus, de même que celles des systèmes d'information des organisations contre la fraude et la cybercriminalité.

Les administrateurs de réseaux informatiques analysent et mettent en œuvre les risques de manière exhaustive et cohérente pour leur permettre de gérer les risques liés à la sécurité des systèmes d'information et de gestion aussi efficacement et au coût le plus élevé possible. Et à cet effet, notre principal objectif visé dans notre travail de mémoire est : « proposition d'une configuration sécurisé d'un réseau local » Au sein de l'entreprise Cevital de Bejaia.

Notre mémoire est structuré en trois chapitres :

Le premier chapitre s'intitule « Généralité Sur Les Réseaux Informatiques », nous présentons d'une manière générale des informations sur les réseaux et quelques principes de base. Le deuxième chapitre titré « La Sécurité d'un Réseau Local » sera basé sur les techniques de sécurisation du réseau contre les attaques. Le dernier chapitre nommé « Réalisation des Solutions Proposées » qui est décomposé en deux parties qui sont : la première qui se repose sur la presentation de l'organisme où nous avons effectué notre stage et la deuxième qui sera consacrée à l'implémentation des solutions présentées.

Nous allons terminer notre mémoire par une conclusion générale tirée à travers notre travail.

Chapitre I

Généralité Sur Les Réseaux Informatiques

Introduction

Un réseau informatique permet à plusieurs machines (Ordinateurs, Impriment, ...) de communiquer entre elles afin d'assurer des échanges d'informations: du transfert de fichiers, du partage de ressources (imprimantes et données), de la messagerie ou de l'exécution de programmes à distance. L'objectif de ce chapitre est de présenter les concepts de bases lies aux réseaux informatiques.

I.1.Définiton d'un réseau

Un réseau est un ensemble fédérateur constitué d'éléments interconnectés, qui permet à des machines d'échanger des informations.

Les éléments raccordées sont des machines délivrant des informations (serveurs) ou bien des machines qui reçoivent ou émettent des informations (terminaux), telles qu'ordinateurs et des périphériques, par exemple des terminaux bureautiques (imprimantes, scanners…), des terminaux industriels (lecteurs de codes-barres, capteurs, contacts télécommandés…), des terminaux téléphoniques, etc.

Un réseau peut également être constitué d'un ensemble de réseaux interconnecté, comme c'est le cas d'Internet.

Le réseau est organisé sur une infrastructure de communication filaire ou radio sur laquelle vont circuler divers flux d'information : données informatiques, phonie, vidéo, commandes à distance, acquisition de données par capteurs, etc.

Un réseau est public ou privé, mais appartient à une entité [1].

I.2.Classifcation des réseaux informatiques

La classification se fait par rapport à un critère donné, ainsi nous pouvions classifier les réseaux informatiques de la manière suivante :

- Classification selon leur taille ;
- Classification selon l'architecture des réseaux;
- Classification selon leur topologie.

I.2.1. Classification selon leur taille

Nous distinguons généralement cinq catégories de réseaux informatiques, (Figure I.1) dont les limites ne sont pas fixées de manière absolue et qui peuvent former, ensemble, un réseau d'entreprise [2].

- **Les réseaux personnels (PAN: personnel Area Network) :** qui interconnectent sur quelques mètres des équipements personnels tels que téléphone mobile, portables, etc.., d'un même utilisateur [3].
- **Les réseaux locaux (LAN: Local Area Network) :** ces réseaux sont en général circonscrits à un bâtiment ou à un groupe de bâtiment pas trop éloignés les uns des

autres (site universitaire, usine ou 'campus'). L'infrastructure est privée et est gérée localement par les personnels informatiques.

- **Les réseaux métropolitains (MAN: Metropolitan Area Network) :** ce type de réseau est apparu relativement récemment et peut regrouper un petit nombre de réseau locaux au niveau d'une ville ou d'une région. L'infrastructure peut être privée ou publique.
- **Les réseaux régionaux (RAN : Régional Area Network) :** ont pour objectif de couvrir une large surface géographique. Dans le cas des réseaux sans fil, les RAN peuvent avoir une cinquantaine de Kilomètres de rayon, ce qui permet, à partir d'une seule antenne, de connecter un très grand nombre d'utilisateurs [3].
- **Les réseaux distants (WAN: Wide Area Network) :** l'infrastructure est en général publique (PTT, Télécom etc.) et l'utilisation est facturée en fonction du trafic et/ou en fonction de la bande-passante réservée, pour les lignes louées (une ligne louée est réservée exclusivement au locataire, 24h sur 24, pour la durée du contrat).

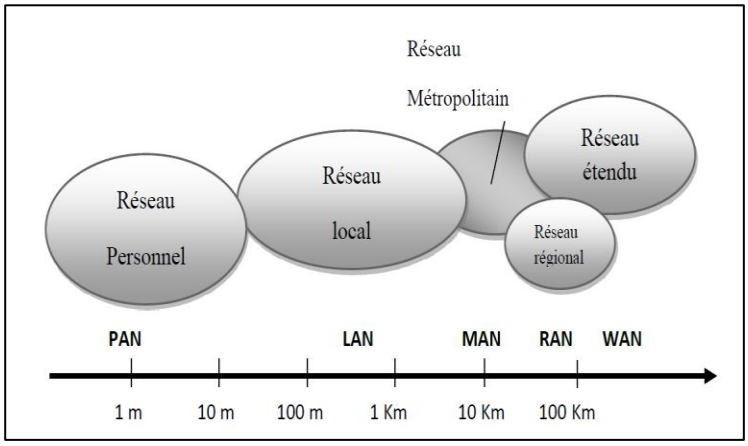


Figure I.1 : Types de réseaux.

I.2.2. Classification selon l'architecture des réseaux

Les réseaux sont dits soit « de postes à postes », soit de type « client/serveur ». En fait, dans la majorité des cas, un réseau est de type « mixte », c'est-à-dire que coexistent les deux types [4].

- **Le réseau poste à poste (peer to peer) :** les réseaux postes à postes ne comportent en général que peu de postes, moins d'une dizaine de postes, parce que chaque utilisateur fait office d'administrateur de sa propre machine, il n'y a pas d'administrateur central, ni de super utilisateur ni de hiérarchie entre les postes ni entre les utilisateurs (Figure I.2). Dans un réseau peer to peer, chaque poste est à la fois client et serveur. Toutes les stations ont le même rôle, et il n'y a pas de statut privilégié pour l'une des stations.

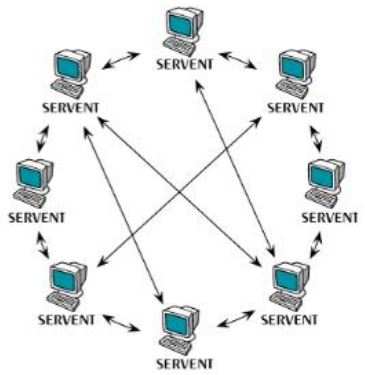


Figure I.2 : Architecture poste à poste.

- **Le réseau client/serveur :** les réseaux Client/serveur comportent en général plus de dix postes. La plupart des stations sont des « postes clients », c'est-à-dire des ordinateurs dont se servent les utilisateurs, les autres stations sont dédiées à une ou plusieurs tâches spécialisées, on dit alors qu'ils sont des serveurs (Figure I.3). Les « postes serveurs » sont en général de puissantes machines, elles fonctionnent à plein régime et sans discontinuité.

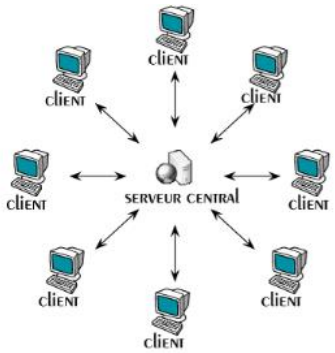


Figure I.3 : Architecture client/serveur.

I.2.3. Classification selon leur topologie

a) La topologie physique

L'arrangement physique, c'est-à-dire la configuration spatiale du réseau est appelé topologie physique. On distingue généralement les topologies suivantes [1]:

- **Topologie en bus :** ce modèle est basé sur le protocole Ethernet, normalisé par l'IEEE sous la référence 802.3. La première structure de réseau Ethernet est celle sous forme de bus (Figure I.4). Le bus, en l'occurrence, est un câble coaxial Ethernet sur lequel viennent se greffer les composants du réseau. Le raccordement utilise des prises vampire qui percent le blindage du câble coaxial pour venir écouter et émettre dans le bus. Les collisions sont gérées par les machines du réseau elles-mêmes, chacune devant s'assurer avant d'émettre que le bus est libre… comme le piéton regarde à gauche et à droite avant de traverser la rue. Comme pour l'anneau, l'information est émise sur le bus avec une identification de destinataire et seules les machines concernées l'acceptent.

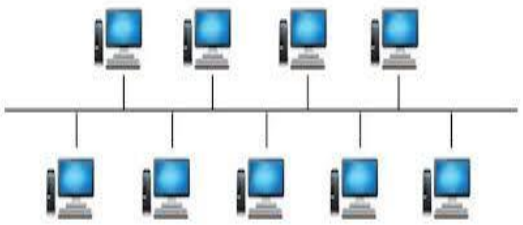


Figure I.4 : Topologie en bus.

- **Topologie en étoile :** la transmission Ethernet est limitée par la longueur du câble et l'architecture en bus trouve vite ses limites. Pour palier ceci, l'architecture Ethernet est également présentée en étoile (Figure I.5). Toutes les machines sont raccordées à un point central du réseau, que l'on nomme un concentrateur.

  Le mécanisme de transmission est le même que pour le bus, avec test anticollision et diffusion sur toutes les branches de l'étoile.

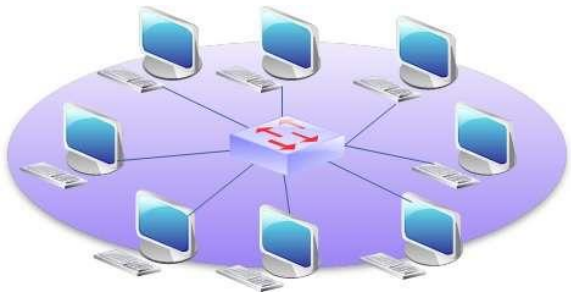


Figure I.5 : Topologie en étoile.

- **Topologie en anneau :** c'est la forme la plus ancienne de réseau sur support unique, le Token Ring d'IBM, normalisé par l'IEEE sous la référence 802.5.

  Toutes les machines sont placées sur une boucle fermée, l'anneau (Figure I.6). Les liaisons se font toutes dans le même sens, par exemple celui inverse des aiguilles d'une montre. Pour éviter les collisions, un mécanisme de jeton gère les droits d'émission. Par exemple une machine A est possesseur du jeton et émet. Quand il a terminé, il passe le jeton à la machine suivante B qui émet puis repasse le jeton à la suivante C, etc.

  L'information est émise sur l'anneau avec l'identification de son destinataire. Chaque machine examine cette information pour savoir si elle est en est destinataire. Seuls le ou les destinataires acceptent l'information.

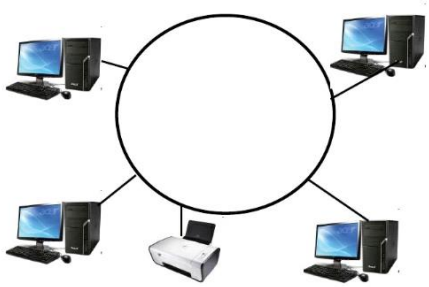


Figure I.6 : Topologie en anneau.

- **Topologie en arbre (topologie hiérarchique) :** dans cette topologie un réseau est divisé en niveaux. Le sommet, le haut niveau, est connectée à plusieurs nœuds de niveau inférieur, dans la hiérarchie (Figure I.7). Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le tout dessine alors un arbre, ou une arborescence [5].

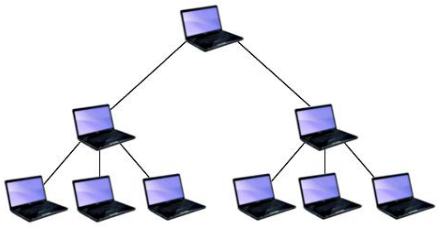


Figure I.7 : Topologie en arbre.

- **Topologie maillée :** une topologie maillée, est une évolution de la topologie en étoile, elle correspond à plusieurs liaisons point à point. Une unité réseau peut avoir (1,N) connexions point à point vers plusieurs autres unités. Chaque terminal est relié à tous les autres (Figure I.8). L'inconvénient est le nombre de liaisons nécessaires qui devient très élevé.

  Cette topologie se rencontre dans les grands réseaux de distribution (Exemple : Internet) [5]. L'avantage de cette configuration est sa fiabilité. Si par malchance un lien est rompu, il existe toujours un chemin alternatif en transitant par un nœud tiers.

  Elle a aussi l'avantage d'être optimisée en termes de temps de transfert. Comme il existe un chemin direct entre deux nœuds, la transmission utilise toujours le plus court chemin entre deux, sans transit, et la fonction de routage est réduite à sa plus simple expression [1].

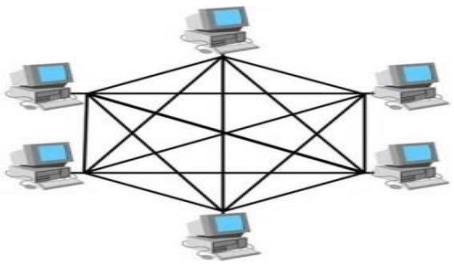


Figure I.8 : topologie maillée.

b) La topologie logique

Représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont [6]:

- **Token Ring :** Token Ring repose sur une topologie en anneau (ring). Il utilise la méthode d'accès par jeton (token). Dans cette technologie, seul le poste ayant le jeton a le droit de transmettre. Si un poste veut émettre, il doit attendre jusqu'à ce qu'il ait le jeton. Dans un réseau Token ring, chaque nœud du réseau comprend un MAU (Multi station Access Unit) qui peut recevoir les connexions des postes. Le signal qui circule est régénéré par chaque MAU.
- **Ethernet :** Ethernet est aujourd'hui l'un des réseaux les plus utilisés en local. Il repose sur une topologie physique de type bus linéaire, c'est-à-dire tous les ordinateurs sont reliés à un seul support de transmission. Dans un réseau Ethernet, la communication se fait à l'aide d'un protocole appelé CSMA/CD (Carrier Sense Multiple Access with Collision Detect), ce qui fait qu'il aura une très grande surveillance des données à transmettre pour éviter toute sorte de collision. Par un conséquent un poste qui veut émettre doit vérifier si le canal est libre avant d'y émettre.
- **FDDI :** la technologie LAN FDDI (Fiber Distributed Data Interface) est une technologie d'accès réseau utilisant des câbles fibres optiques. Le FDDI est constitué de deux anneaux : un anneau primaire et anneau secondaire. L'anneau secondaire sert à rattraper les erreurs de l'anneau primaire. Le FDDI utilise un anneau à jeton qui sert à détecter et à corriger les erreurs. Ce qui fait que si une station MAU tombe en panne, le réseau continuera de fonctionner.

I.3. Les équipements d'interconnexion

L'interconnexion des réseaux consiste à mettre en relation des machines appartenant à des réseaux physiquement distincts. Les éléments d'interconnexion, ou relais dans la terminologie OSI peuvent n'être que de simples éléments matériels (pont, routeur, ...etc.) mais aussi des réseaux. Ces principaux matériels sont [7]:

- **Le répéteur :** c'est un équipement qui réalise une connexion physique entre deux segments d'un même réseau logique. Agissant au niveau physique, les réseaux interconnectés doivent être homogènes. Le répéteur (Figure I.9) est utilisé pour réaliser l'adaptation des supports (passage du coaxial à la fibre optique, par exemple), ou pour régénérer les signaux reçus sur son interface d'entrée et les transfère sur son interface de sortie au format de celle-ci.

Figure I.9 : Le répéteur.

- **Un pont (Bridge) :** est un élément d'interconnexion de niveau 2. Il permette d'interconnecter deux ou plusieurs réseaux (ponts multiports) dont les couches physiques sont dissemblables. Les ponts (Figure I.10) sont transparents aux protocoles de niveau supérieur.

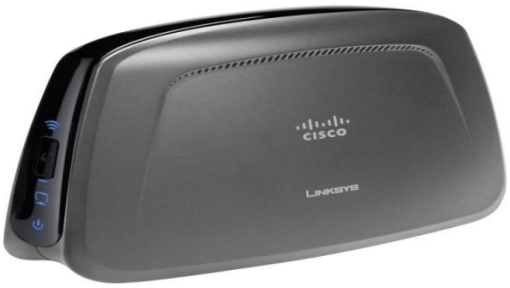


Figure I.10 : Le pont.

- **Le routeur :** est un élément d'interconnexion de niveau 3 qui achemine (route) les données vers un destinataire identifié par son adresse de niveau 3. Agissant au niveau 3, les routeurs (Figure I.11) offrent plus de possibilités que les ponts, ils peuvent mettre en œuvre les mécanismes du niveau 3 (segmentation, réassemblage, contrôle de congestion ...etc.).

Figure I.11 : Le routeur.

D'autres équipements que nous pouvons les distinguer [8]:

- **La carte réseau:** la carte réseau (NIC, Network Interface Card) (Figure I.12) est le composant le plus important, elle est indispensable. C'est par elle que transitent toutes les données à envoyer et à recevoir du réseau par un ordinateur. La notion d'adresse MAC (l'adresse physique de la carte) permet d'identifier la machine dans un réseau, un peu comme l'adresse IP. L'adresse physique est relative à la carte réseau, elle lui est attribuée à sa fabrication et ne peut pas changer (unique au monde).

Figure I.12 : La carte réseau.

- **Le concentrateur (Hub) :** un hub (Figure I.13) est un dispositif en réseau qui permet de mettre plusieurs ordinateurs en contact. Il est moins intelligent que les autres, ce que signifie qu'il reçoit des données par un port, et envoie ce qu'il reçoit aux autres. Il a une interface de réception (un port) et une interface de diffusion (plusieurs autres ports par où les autres ordinateurs sont connectés).

Figure I.13 : Le Hub.

- **Le commutateur (Switch) :** un commutateur (Figure I.14) fonctionne à peu près comme un hub, sauf qu'il est plus discret et intelligent. Il n'envoie pas tout ce qu'il reçoit à tout le monde, mais il l'envoie uniquement au destinataire. Par exemple si l'ordinateur A envoie des données à l'ordinateur B, seul ce dernier les recevra et pas les autres connectés. Afin de déterminer l'ordinateur à qui il faut renvoyer les données, le switch se base sur les adresses physiques (adresses MAC) des cartes réseau. Les transmissions sont plus confidentielles, les autres ne savent rien des données ne leur étant pas destinées. Son utilisation reste limitée aux réseaux locaux.

Figure I.14 : Le commutateur (Switch).

- **Un modem (Modulateur-Démodulateur) :** c'est un périphérique utilisé pour transférer des informations entre plusieurs ordinateurs via les lignes téléphoniques. Le modem (Figure I.15) module les informations numériques en ondes analogiques, en sens inverse il retranscrit les données sous forme analogique en données numériques.

Figure I.15 : Le modem (Modulateur-Démodulateur).

I.4. Les équipements terminaux

La fonction principale d'un équipement terminal est de permettre à l'utilisateur d'accéder aux ressources du réseau par l'intermédiaire d'une interface, qui est généralement multipoint soit, filaire ou sans fil. C'est l'équipement à l'extrémité de la liaison de données auquel l'utilisateur a directement accès. La famille des terminaux comprend les terminaux spécifiques (smartphone, terminal bancaire, terminal de paiement …etc.), les ordinateurs de type pc (Personnal Computer), qui peuvent être des clients dans une organisation client-serveur, et les serveurs.

Dans les premiers réseaux informatiques l'organisation suivez était celle de client-serveur avec des terminaux (des stations) très limites, de type écran-clavier, et des serveurs concentraient toutes les ressources en termes de calcul et de stockage. De nos jours, les pc sont suffisamment puissants pour être autonomes et les serveurs sont utilisés pour l'authentification sur le réseau, le stockage sécurisé, ou la gestion de services (mal, web fichier, bases de données, …etc.) [9].

I.5. Les supports de transmission

Ils sont nombreux, parmi-ci nous distinguons trois type de support, y'a ceux qui sont en cuivre, en fibre optique et immatériels. Les supports en cuivre comme les paires torsadés et les câbles coaxiaux, sont les plus anciens et les plus largement utilisés ; ils transportent des courants électriques. Les supports de verre ou de plastique (fibre optique) transportent la lumière, tandis que les supports immatériels des communications sans fil, propagent des ondes électromagnétiques [10].

I.5.1. Câbles réseaux

a) Câbles en cuivre

- **Câble paire torsadée :** l'utilisation courante de la paire torsadée est le raccordement de l'usager central téléphonique (la boucle locale) ou la desserte de l'usager des réseaux privés. La paire torsadée suffit pour les réseaux locaux d'entreprise où les distances se limitent à quelques kilomètres.

On définit deux types de la paire torsadée :

- **Paire torsadé non blindée (UTP, Unshielded Twisted Pair) :** se compose de deux conducteurs en cuivre, isolés l'un de l'autre et enroulés de façon hélicoïdales autour de l'axe de symétrie longitudinal (Figure I.16).

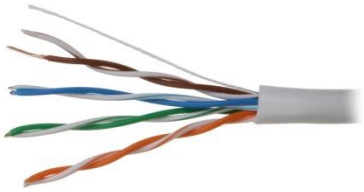


Figure I.16 : Câble paire torsade non blindée (UTP).

- **Paire torsadé blindée (STP, Shielded Twisted Pair) :** enrobées d'un conducteur cylindrique, elle est mieux protégée des rayonnements électromagnétiques parasites. Une meilleure protection prévoit un blindage par paire (Figure I.17).

Figure I.17 : Câble paire torsadée blindée (STP).

- **Câble coaxial :** pour éviter les perturbations dues aux bruit externes, on utilise deux conducteurs métalliques cylindriques de même axe séparer par un isolant le tout formes un câble coaxial (Figure I.18). Ce câble présente des meilleures performances que la paire torsade.

Figure I.18 : Câble coaxial.

b) Câble en fibre optique

Ce câble est constitué d'un fil de verre très fin (Figure I.19). Il comprend un cœur, dans lequel se propage la lumière émise par une diode électroluminescente ou une source laser et une gaine optique dont l'indice de réfraction garantit que le signal lumineux reste dans la fibre.

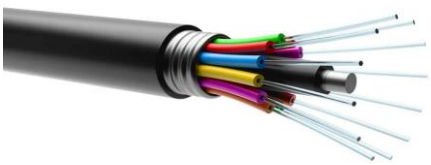


Figure I.19 : Câble fibre optique.

Les premières fibres optiques employées dans les télécommunications étaient multimode et monomode.

- **Multimode :** ce type de fibre est réservée aux débits inférieurs au gigabit par seconde, sur des distances de l'ordre du kilomètre .plusieurs longueurs d'onde bien choisies se propagent simultanément en de multiples de trajets dans le cœur de la fibre.

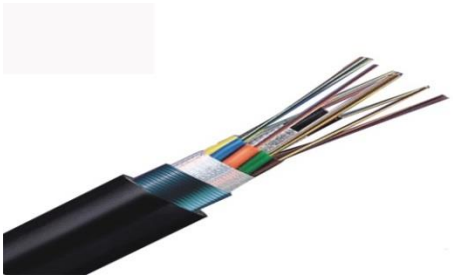


Figure I.20 : Fibre optique multimode.

- **Monomode :** ce type est réservé aux débits plus élevés et des distances plus longues. La fibre monomode, de fabrication récente, plus fine, assure la propagation d'une seule longueur d'onde dans son cœur et offre donc de meilleures performances.

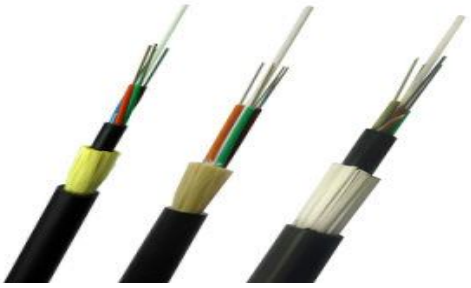


Figure I.21 : Fibre optique monomode.

Le choix du support est fonction de critère indépendant parmi lesquelles [11] :

- La distance maximum entre stations ;
- Le débit minimum et maximum ;
- Le type de transmission (numérique ou analogique) ;
- La nature des informations échangées (données, voix, vidéo, …) ;
- La connectique ;
- La fiabilité, le cout …etc.
- Le tableau I.1 donne l'ordre de grandeur des débits nécessaires en fonction de la nature des informations à transmettre.

Natures des informations	**Débits**
Page A4 de texte transmise en 1 s	10 Kb/ s
Fichiers de 10 Mo transmise en 1 s	80 Mbit/ s
Voix échantillonnée sur 8 bits à 8 kHz	64 Kbits/s
Son stéréo échantillonnée sur 16 bits à 44,1 kHz	1,4 Mbit/s
Image N&B non compressée (50 image/s)	12,5 Mbit/s
Image N&B compressée	500 Kbit/s
Image couleur non compressée (50 image/s)	200 Mbit/s

Image couleur compressée	2 Mbit/s

Tableau I .1 : valeur des débits suivant la nature des informations.

Le tableau I.2 résume les caractéristiques principales des supports usuels pour des transmissions en bande de bas.

Type de support	Débit max	Distance max (sans répéteurs)	Temps de propagation	Immunité au bruit	remarques
Paire torsadée non blindée (0,2 mm)	1 Gbit/s	1 km	≈ 5,3 µs/km	Faible	Affaiblissements important
Paire torsadée blindée (0,2 à 1 mm)	10Gbit/s	1 km(56m à 10 Gbit/s)	≈ 5,3 µs/km	Bonne	Liaisons multifils
Câble coaxial (2,6/9,5 mm ou 1,2/4,4 mm)	100 Mbit/s	1 km	≈ 4,1 µs/km	Très bonne	Impédance caractéristique de 50 Ω ou 75 Ω B ≈ 500 MHz
Fibre optique	10 Gbit/s	10 km	≈ 5 µs/km	Excellente	Débit en progression B= 10GHz pour 1 km

Tableau I.2 : caractéristiques des déférents supports.

I.5.2. Transmission sans fil

Elle se repose sur la propagation des ondes électromagnétiques dans l'atmosphère ou dans le vide .l'absence de support matériel apporte une certaine souplesse et convient aux applications comme la téléphonie ou la télécommunication mobile, sans nécessiter la pose couteuse de câbles [10].

I.6. Modèle général de communication

I.6.1. Le modèle OSI (Open System Interconnected)

Le modèle OSI (Open Systems Interconnection) a été créé par l'ISO (International Organization for Standardization) il y a une trentaine d'années. Il fait l'objet d'une norme qui s'appelle 7498-1 :1994 à l'ISO et X.200 à l'ITU (International Télécommunication Union).

C'est uniquement une référence, un texte abstrait destiné à fournir un cadre conceptuel pour les ingénieurs en télécoms et les informaticiens qui travaillent dans les réseaux.

Autrement dit, ce n'est pas un standard de communications, c'est seulement un moyen de mieux se comprendre [12].

- **Rôle des différentes couches du modèle OSI :** Il définit sept couches (Figure I.22). Chacune correspond à une famille de fonctions de communication:

- 7.Application (application layer) interface avec les programmes locaux (système d'exploitation, Utilitaires et applications).
- 6. Présentation (presentation) transformations des données.
- 5.Session (session) gestion du dialogue dans le temps (ouverture du dialogue, déroulement, fin).
- 4.Transport (transport) gestion du dialogue dans l'espace, vérification que le programme destinataire reçoit bien les données envoyées par le programme expéditeur.
- 3.Réseau (network) gestion de l'adressage et du choix du chemin (routing).
- 2.Liaison (data link) type de réseau.
- 1.Physique (physical) définition des caractéristiques réelles de la transmission (type de prise, type de câble, voltage, etc.).

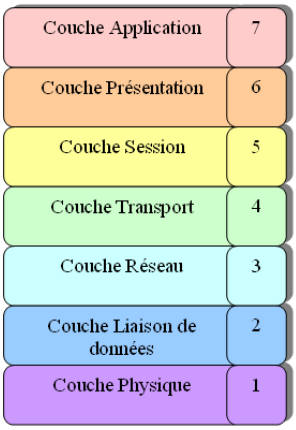


Figure I.22 : Représentation de modèle OSI.

- **Les services de chaque couche :** le tableau I.3 représente les principaux services et protocoles de chaque couche du modèle OSI :

Couche	Principaux services	Protocoles
7. Application	Messagerie électronique, web, transfert de fichiers, accès à distance, systèmes de fichiers distribués, téléphonie sur IP, émulation de terminal, etc.	HTTP, SMTP, POP3, FTP, telnet, NFS, VoIP, BitTorrent, DNS, DHCP
6. Présentation	Format des données, chiffrement.	MIME
5. Session	Gestion du dialogue entre les applications.	
4. Transport	Contrôle que les données parviennent bien à leur destinataire.	TCP, UDP
3. Réseau	Adressage et gestion de l'itinéraire suivi par les données.	IP, IPsec, ICMP, BGP
2. Liaison	Sous-couche LLC : gestion du déplacement des données (LLC signifie *Logical Link Control*) Sous-couche MAC : gestion de l'accès des données au réseau physique (MAC signifie *Media Access*	802.3 (Ethernet), 802.11 (Wi-Fi)

	Control).	
1. Physique	Définition du matériel : cuivre, fibre ou sans-fil, débit, nombre de fils, fonction de chaque fil, forme des prises, etc.	1000Base-T et autres normes Ethernet physiques, liaison sérielle, etc.

Tableau I.3 : Tableau représentatif de services et protocoles des couches du modèle OSI.

I.6.2. le modèle TCP/IP

Le modèle TCP / IP reprend l'approche modulaire du modèle OSI (utilisation de modules ou de couches) mais ne contient, lui que quatre couches (Figure I.23). Ces couches ont des taches beaucoup plus diverses étant donné qu'elles correspondent a plusieurs couches du modèle OSI [13].

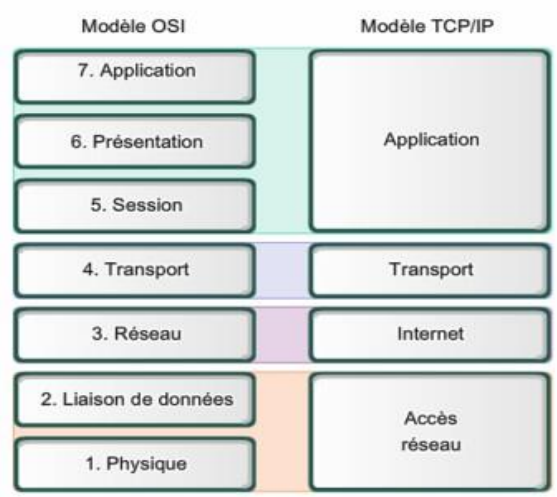


Figure I.23 : L'architecture en couche de modèle TCP/IP.

- **Rôle des différentes couches du modèle TCP/IP :** Les rôles des différentes couches sont les suivants :

- **La couche Accès réseau :** Spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé.
- **La couche Internet :** Cette couche est chargée de fournir le paquet de données (Datagramme).
- **La couche Transport :** Elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaitre l'état de la transmission.
- **La couche Application :** Cette couche englobe les applications standards du réseau.

Le tableau I.4 représente les protocoles de chaque couche du modèle TCP/IP :

Niveau	Modèle TCP/IP	Modèle OSI	Protocole TCP/IP
Niveau 4	Couche Application	Couche Application	Application réseau (Telnet, SMTP, FTP …).
		Couche Presentation	

		Couche Session	
Niveau 3	Couche Transport (TCP)	Couche Transport	TCP ou UDP.
Niveau 2	Couche Internet (IP)	Couche réseau	IP, ARP, RARP.
Niveau 1	Couche Accès réseau	Couche liaison données	FTS, FDDI, PPP, Ethernet, Anneau à jeton (Token Ring).
		Couche physique	

Tableau I.4 : Tableau représentatif de modèle TCP/IP.

I.7. Les protocoles réseaux

Nous définissons un protocole réseaux qu'un ensemble des règles de communication, il existe de nombreux protocoles, nous citons [14] :

- **ARP (Address Resolution Protocol) :** permet de faire la correspondance entre les adresses logiques (Internet) et les adresses physiques (MAC). Ce protocole permet de masquer les adresses nécessaires a l'acheminement des trames de niveau MAC.
- **RARP (Reverse Address Resolution Protocol) :** permet d'établir la correspondance entre les adresses physique (MAC) et le adresses logiques (Internet).
- **ICMP (Internet Control Message Protocol) :** sert à la gestion du protocole IP, il permet de collecter les erreurs qui surviennent lors de l'émission de message.
- **DHCP (Dynamic Host Configuration Protocol) :** utilise les encapsulations IP et UDP mais n'est pas exactement un protocole applicatif. Son rôle, très frètement lié à IP, est de permettre la location dynamique par un serveur des adresses IP aux clients demandeurs dans le but de fédérer et de simplifier la gestion de ces adresses.

D'autres protocoles a cité [15]:

- **IP (Internet Protocol) :** assure une livraison des paquets sans connexion et sans garantie. Son inconvénients majeur est qu'il la mise en place d'un plan d'adressage explicite. Ça signifié que chaque nœud du réseau doit avoir une adresse IP.
- **IGMP (Internet Group Management Protocol) :** ce protocole de la couche réseau permet à une station de joindre ou de quitter un groupe de multidiffusion (multicast).
- **TCP (Transmission Control Protocol) :** ce protocole est oriente connexion. Permet de s'assurer de la bonne arrivée de toutes les informations. En contrepartie, cette fonction peut ralentir la communication.
- **UDP (User Datagram Protocol) :** contrairement à TCP, UDP n'assure pas de connexion et reporte le processus de fiabilisation a la couche supérieure (applicatif). Il fonctionne en mode non connecté, ce qui permet de gagner en débit pour la transmission gourmande, telles que vidéos et sons.

Deux autres protocoles que nous pourrons les rajouter [16] :

- **HSRP (Hot Standby Routing Protocol) :** permet une redondance de routeurs Cisco, il autorise un routeur de secours à remplacer le routeur principal, au cas où ce dernier n'est plus présent sur le réseau (redémarrage, panne …).

- **OSPF (Open Shortest Path First) :** est un protocole de routage à état de liens, son développement est public, ce qui permet de le trouver sur de nombreux systèmes. Ce protocole présente les avantages de converger rapidement et d'être très adaptable. Cependant il est assez complexe à mettre en œuvre. Il est utilisé dans les réseaux de taille moyenne.

I.8. L'adressage IPv4 (Internet Protocol version 4)

- **Définition :** une adresse IPv4 se compose de 32 bits organisés en quartes séquences de 8 bits représentées numériquement et séparer par des points (Figure I.25).

Une adresse ipv4 est composée de deux parties (Figure I.24) :

- L'adresse du réseau (préfixe réseau) (NetID) ;
- L'adresse de l'hôte (HostID) [17].

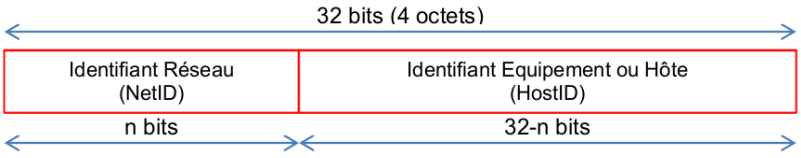


Figure I.24 : Structure de l'adresse IPv4.

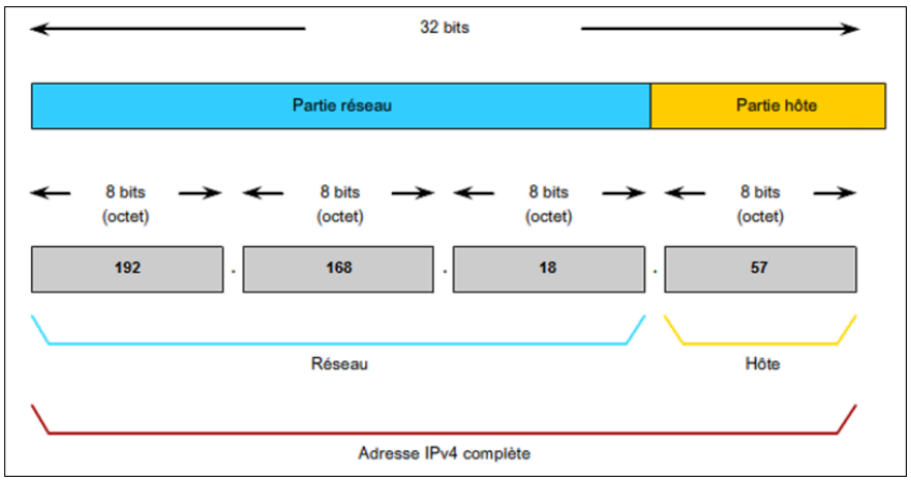


Figure I.25 : Constitution d'une adresse IPv4 (exemple d'une adresse privée de classe B).

- **Masque réseau :** un masque réseau se compose de 32 bits, similaire à une adresse IPv4. L'opération AND entre l'adresse IPv4 et le masque détermine où s'arrête la partie réseau de l'adresse. (C'est un séparateur entre la partie réseau et la partie machine d'une adresse IP).
  Le masque est donc une suite plus ou moins longue de bits consécutifs valant 1. Cette propriété signifie qu'une séquence de 8 bits ne peut avoir qu'une série de valeurs numériques bien définies, comme suit :

Valeurs des bits du masque	Valeurs numériques
0000 0000	0
1000 0000	128
1100 0000	192
1110 0000	224
1111 0000	240
1111 1000	248
1111 1100	252
1111 1110	254
1111 1111	255

Tableau I.5 Représentation de valeurs des bits du masque en valeurs numériques.

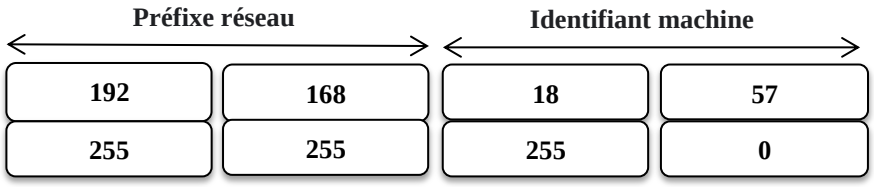
Ces valeurs numériques sont codées sur 8 bits, la longueur totale du masque est donc 32 bits.

Voici un exemple qui montre une utilisation de la division d'une adresse IPv4 :

Adresse IP	192	168	18	57
	1100 0000	1010 1000	00010010	00111001
Masque	255	255	255	0
	1111 1111	1111 1111	1111 1111	0000 0000
Résultat XOR	1100 0000	1010 1000	00010010	0000 0000
Adresse réseau	192	168	18	0

Tableau I.6 : Exemple de la division d'une adresse IPv4.

Dans cet exemple on a converti l'adresse IPv4 et le masque réseau en binaire puis on a effectué l'opération AND entre les deux, pour obtenir un résultat qui correspond à une adresse réseau. Le masque signifie ici que les 24 premiers bits de l'adresse font partie de l'adresse réseau et les 8 derniers bits font partie de l'identification de l'hôte.



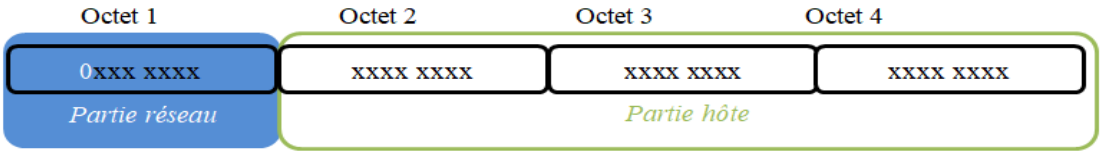
Masque de 24 bits

En plus de la représentation numérique et binaire du masque réseau, il existe une autre façon de représenter le masque à côté d'une adresse réseau, et cette notation est appelée CIDR (Classless Inter Domain Routing). Par exemple 192.168.18.0 /24 signifie que la masque contient 24 bits et que l'adresse réseau est 192.168.18.x.

- **Les classes d'adresse** : lorsqu'IP est utilisé pour la première fois sur un réseau, seul le premier octet de l'adresse est utilisé comme préfixe de réseau. Cette façon d'attribuer des adresses permettait d'avoir 256 réseaux de 16 millions d'hôtes. Pour lever cette limitation, RFC 790 spécifie qu'une adresse IP doit être divisée en deux parties, NetID et HostID.

Puis cinq classes sont créées, identifiées de A à E, qui correspondent au nombre de bits utilisés pour définir les parties du réseau.

- **La classe A :** la classe A définit une longueur de préfixe de 8 bits. Le premier bit d'une adresse de classe A commence toujours par 0 ce que signifie que la valeur du premier octet est comprise entre 0 et 127. Une classe A dispose de 24 bits pour l'adressage des machines, elle peut donc contenir jusqu'à $\mathbf{2^{24}}$ -2 (16 777 214) hôtes.

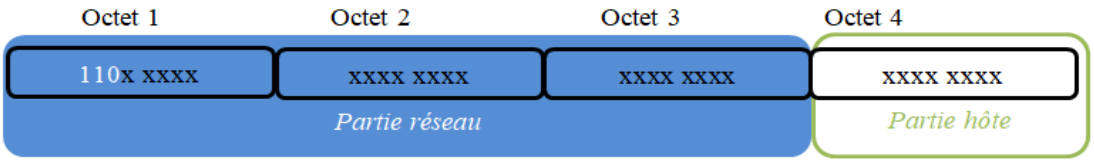


FigureI.26 : La classe d'adresse A.

- **La classe B :** la classe B définit une longueur de préfixe de 16 bits, ce qui laisse 16 bits pour l'identification des hôtes soit $\mathbf{2^{16}}$ -2 (65 534). Le premier bit du premier octet d'une adresse de classe B a toujours la valeur 1 ce qui implique que les adresses de classe B se situent entre 128.0.0.0 et 191.255.255.255.

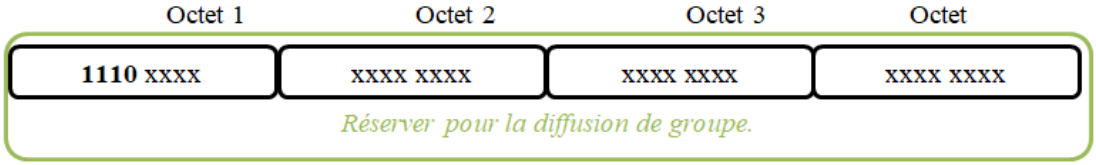
FigureI.27 : La classe d'adresse B.

- **La classe C :** la classe C est probablement la plus connue et la plus utilisée dans les reseaux domestiques. Elle utilise les 24 premiers bits pour définir le prefixe reseau (partie reseau) et laisse 8 bits pour l'adressage des hotes soit $\mathbf{2^{8}}$ -2 (254) hôtes possible. La plage de la classe C va de 192.0.0.0 à 223.255.255.255.



FigureI.28 : La classe d'adresse C.

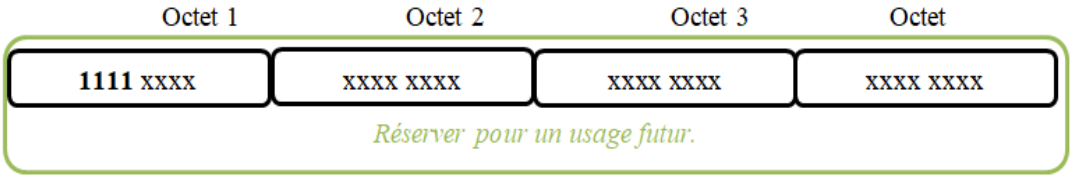
- **La classe D :** c'est la classe Multicast. Les trois premiers ont la valeur 1 ce qui signifie que la plage de la classe D va de 224.0.0.0 à 239.255.255.255. La classe D n'utilise



FigureI.29 : La classe d'adresse D.

que le premier octet pour définir le préfixe. Son utilisation est réservée pour l'adressage de groupes ou des équipements (finaux ou intermédiaires) qui viendront s'enregistrer pour recevoir les données dont l'adresse de destination correspond au groupe.

- **La classe E :** c'est une classe réservées à un usage non déterminé. Les 4 premiers bits du premier octet doivent être a 1 ce qui donne une plage qui va de 240.0.0.0 à 255.255.255.255.



FigureI.30 : La classe d'adresse E.

➢ **Types d'adresses IPv4s :** il existe deux type d'adresses :

- **Les adresses IP privées :** c'est une adresse qui est attribuée à un hôte et qui n'est pas diffuser sur Internet. Elle ne sont pas routable sur Internet ce que veut dire que les fournisseurs d'accès Internet n'échangent pas ces plages.

Une plage par classe d'adresses a été choisie pour devenir une plage privée :

Classe	Plage privée	Masque réseau	Etendue
A	10.0.0.0 /8	255.0.0.0	10.0.0.0 -10.255.255.255
B	172.16.0.0/12	255.240.0.0	172.16.0.0 - 172.31.255.255
C	192.168.0.0/16	255.255.0.0	192.168.0.0 - 192.168.255.255

Tableau I.7 : Réseau privé .

- **Les adresses IP publiques :** les adresses qui ne font pas partie de la plage définie comme privée sont considérées comme publique . Ces plage d'adresses sont routables sur Internet et peuvent donc être joignables directement ce qui implique qu'elles doivent être unique.

Conclusion

Ce chapitre nous a permis de découvrir et de mieux comprendre les notions et les aspects élémentaires des réseaux informatiques à savoir leurs classifications, les topologies, les équipements de transmission, leurs outils d'interconnexion, leurs adressages et les protocoles réseaux, ainsi il nous a permis de différencier entre le modèle OSI qui présente un standard de communications (modèle de référence) entre les équipements terminaux tel que les ordinateurs et le modèle TCP/IP qui est un ensemble de communication sur Internet.

Dans ce chapitre, nous avons traités des connaissances générales sur les réseaux qui faut acquérir, afin de pouvoir installer une sécurité, que nous allons développer dans le chapitre suivant.

Chapitre II

La Sécurité d’un Réseau Local

Introduction

La sécurité informatique est de nos jours devenue un problème majeur dans la gestion des réseaux d'entreprise ainsi que pour les particuliers toujours plus nombreux à se connecter à Internet. La transmission d'informations sensibles et le désir d'assurer la confidentialité de celles-ci est devenue un point primordial dans la mise en place de réseaux informatiques.

II.1. Définition de la sécurité des réseaux

La sécurité d'un réseau est un ensemble de moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir sa sécurité. En général, la sécurité d'un réseau englobe celle du système informatique sur lequel il s'appuie [18].

II.2. Objectifs de la sécurité

La sécurité des données informatique couvre des objectif que nous allons les citer ci-dessous [19] :

- **La confidentialité :** seule les personnes habilitées doivent avoir accès aux données. Toute interception ne doit pas être en mesure d'aboutir, les données doivent être cryptées, seuls les acteurs de la transaction possèdent la clé de compréhension.
- **L'intégrité :** il faut garantir à chaque instant que les données qui circulent sont bien celles que l'on croit, qu'il n'y a pas eu d'altération (volontaire ou non) au cours de la communication. l'intégrité des données doit valider l'intégralité des données, leur précision, l'authenticité et la validité.
- **La disponibilité :** il faut s'assurer du bon fonctionnement du système, de l'accès à un service et aux ressources à n'importe quel moment. La disponibilité d'un équipement se mesure en divisant la durée durant laquelle cet équipement est opérationnel par la durée durant laquelle il aurait dû être opérationnel.
- **La non-répudiation :** une transaction ne peut être niée par aucun des correspondants. La non-répudiation de l'origine et de la réception des données prouve que les données ont bien été reçues. Cela se fait par le biais de certificats numériques grâce à une clé privée.
- **L'authentification :** elle limite l'accès aux personnes autorisées. Il faut s'assurer de l'identité d'un utilisateur avant l'échange de données.

II.3. Domaines d'application de la sécurité informatique

Pour une organisation, toutes les sphères d'activité de l'informatique et des réseaux de télécommunication sont concernées par la sécurité d'un système d'information [20]. En fonction de son domaine d'application la sécurité informatique se décline en (Figure II.1) :

- Sécurité physique et environnementale ;
- Sécurité de l'exploitation ;
- sécurité logique, sécurité applicative et sécurité de l'information ;
- sécurité de l'infrastructure informatique et de la télécommunication (sécurités des réseaux, sécurité Internet et cybersécurité).

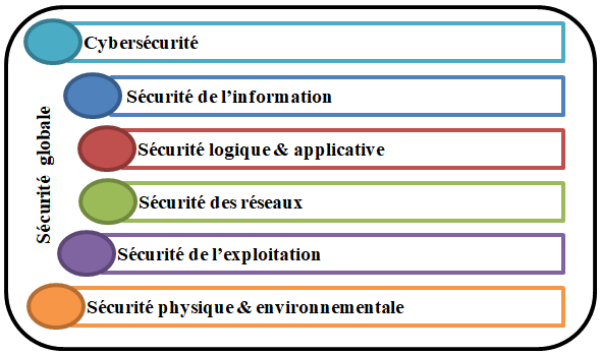


Figure II.1 : Domaines d'application de la sécurité.

- **Sécurité physique et environnementale :** la sécurité physique et environnementale concerne tous les aspects liés à la maitrise des systèmes et de l'environnement dans lesquels ils se situent. Elle se repose essentiellement sur :
  - la protection des sources énergétiques et de la climatisation (alimentation électrique, refroidissement, etc.) ;
  - la protection de l'environnement (mesures ad hoc notamment pour faire face aux risques d'incendie, d'inondation ou encore de terriblement de terre … pour respecter les contraintes liées à la température, a l'humidité, etc.) ;
  - l'usage d'équipements qui possèdent un bon degré de sureté de fonctionnement et de fiabilité ;
  - la redondance physique des infrastructures et sources énergétiques ;
  - le marquage des matérielles pour notamment contribuer à dissuader le vol de matériel et éventuellement le retrouver ;
- **Sécurité de l'exploitation :** la sécurité de l'exploitation doit permettre au système informatique de fonctionner correctement. Cela comprend l'établissement d'outils et de procédures liés aux médiologies d'exploitation, la maintenance, les tests, les diagnostics, la gestion des performances et la mise à jour.
  La sécurité de l'exploitation est largement déterminée par son degré d'industrialisation, qui dépend du niveau de maîtrise de l'application et du degré d'automatisation de la tâche. Bien que les opérations soient responsables, ces conditions sont directement liées à la conception et à la mise en œuvre des applications elles-mêmes et à leur intégration avec les systèmes d'information.
- **Sécurité logique, applicative et sécurité de l'information :** la sécurité logique fait référence aux mécanismes de sécurité mis en œuvre par les logiciels qui contribuent au bon fonctionnement des programmes, des services fournis et à la protection des données. La sécurité applicative comprend le développement associé de solutions logicielles (ingénierie logicielle, qualité logicielle) ainsi que leur intégration et leur exécution fluides dans l'environnement opérationnel. Bien protéger l'information, c'est également assurer son exactitude et sa pérennité pour le temps nécessaire à son exploitation et à son archivage. Cela nécessite de déterminer le niveau de protection nécessaire aux informations manipules, par une classification des données qui permet de qualifier leur degré de sensibilité (normale, confidentielle, etc.) et de les protéger en fonction de ce dernier.

- **Sécurité des infrastructures de télécommunication :**la sécurité des télécommunication consiste à offrir à l'utilisateur final et aux applications communicantes, une connectivité fiable de « bout en bout ».Cela passe par la réalisation d'une infrastructure réseau sécurisée au niveau des accès au réseau et du transport de l'information (sécurité de la gestion des noms et des adresses, sécurité du routage, sécurité des transmissions à proprement parler) et cela s'appuie sur des mesures architecturales adaptées, l'usage de plates-formes matérielles et logicielles sécurisées et une gestion de réseau de qualité.
- **Cybersécurité :** la cybersécurité est un sous-ensemble de la sécurité informatique et des réseaux appliques aux cyberespaces et a tout environnement informatique connecté à l'Internet. Elle peut être mise en défaut par des cyberattaques informatiques. Du fait de l'usage extensif de l'Internet, de nouvelles menaces sont apparues générant des risques additionnels dont les impacts, de niveaux d'importance variables, peuvent affecter les individus, les organisations ou les Etats.

II.4. Les attaque

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque, qui est une exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables [21].

Sur Internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir des machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques. Ces attaques peuvent être classées en deux grandes catégories : attaques passive et attaques actives [22].

Attaques passives : consiste à écouter indiscrètement ou surveillance de transmissions. Le but de l'adversaire est d'obtenir une information qui a été transmise. Ces attaques passives sont la capture du contenu d'un message et l'analyse de trafic sans modifier les données ou le fonctionnement du réseau.

Attaques actives : ces attaques impliquent certaines modifications du flot de données ou la création d'un flot frauduleux.

II.4.1. Outils et types d'attaques

Hormis la pénétration d'un système, les attaques par déni de service sont très prisées. Elles visent à solliciter un service réseau qu'il ne répond plus aux demandes légitimes, voire s'arrêter. Les types d'attaques sont nombreux qu'il serait imaginaire de prétendre les décrire toutes, voici les attaques les plus utilisées [23] :

- **Ingénierie sociale :** cette technique consiste à manipuler des personnes pour contourner les dispositifs de sécurité. L'escroquerie par 'phishing' (pêche), en est une variante très efficace. Cette arnaque complète l'envoi de mail par une usurpation de charte graphique de site web. Elle incite un individu à transmettre des données

confidentielles, bancaires par exemple. Un message électronique est d'abord envoyé. Il contient un lien redirigeant vers un faux site aux couleurs de l'entité usurpée. Très souvent, l'objectif poursuivi est l'obtention d'un numéro de carte bleue.

- **Ecoute réseau :** dans le monde des logiciels libres, de nombreuses applications existent. Parmi celles-ci, WireShark qui est capable de reconstituer une session TCP, il est gratuit et sous licence GPL. L'écoute réseau, ou est avant tout une affaire de connaisseurs, car les outils ne remplacent pas des capacités d'interprétation.
- **Analyse des ports :** dans un réseau de type TCP/IP, un service serveur écoute sur un port, TCP ou UDP, qui lui est propre. À chacun correspond un numéro, entre 0 et 65 535. La première série, jusqu'à 1024, comprend les ports bien connus des applicatifs standard comme (80 pour HTTP, 25 pour SNMP, 53 pour DNS et 21pour FTP …etc.).L'analyse de ports consiste à les balayer successivement. On parle de 'scan'. Lorsqu'un port en écoute est sollicité, il répond. Parfois, il renvoie beaucoup d'informations.

  De nombreux logiciels non payants sont disponibles sur internet, tels que NMap (Network Mapper) ou SuperScan. Ils proposent différents techniques de balayage, plus ou moins discrètes, qui permettent de rendre l'écoute moins active.
- **Code malveillants :** de tels logiciels peuvent être composés de deux fonctions distinctes :

- Une possibilité de reproduction;
- Une capacité d'attaque, avec une charge nocive.

Un virus est un bloc de code qui est introduit dans un hôte pour d'y propager, mais nécessite l'exécution de celui-ci pour s'activer. Par contre un ver se propage par la messagerie ou les failles réseaux. Il ne contient pas obligatoirement de charge nocive.

- **Programmes furtifs :** de nombreux programmes furtifs existés, on cetera certains :

- **Le cheval de trois (Trojan horse)** : pourrait entrer dans la catégorie des codes malveillants. Mais il n'en contient pas les deux fonctions. Une fois installé, ce programme reste dissimulé. Il peut simplement ouvrir un port réseau pour être utilise comme serveur. Le pirate a ainsi pris la possession de la machine.
- **Les logiciels espions** : sont une sous-catégorie du cheval de trois. Des logiciels espions, les programmes comme 'Keyloggers' sont chargées de renvoyer les informations saisies au clavier (mot de passe, numéro confidentiels,..).
- **Les bots, diminutif de robot** : sont des logiciels qui permettent de contrôler une machine à distance. Elles deviennent ainsi des 'Zombies' et peuvent être utilisées pour lancer une attaque programmée, ou servir de relais pour les attaques par spam.

II.5. Principes de sécurité sur un réseau local

À cause des menaces provenant des logiciels malveillants Il existe plusieurs dispositifs

Pour mettre en place une politique de sécurité, nous allons citer quelques-uns :

II.5.1. Sécurité des communications

II.5.1.1. VLAN (Virtual Local Area Network)

La virtualisation d'un LAN consiste à séparer l'infrastructure physique des services de transfert rapide fournis par les commutateurs (Figure II.2). Un VLAN est donc un LAN logique fonctionnant sur une infrastructure LAN physique commutée. Une infrastructure physique commune peut supporter plusieurs VLANs. Chaque LAN virtuel fonctionnera comme n'importe quel LAN distinct.

L'objectif fondamental d'un VLAN est de rendre la fonction d'un LAN indépendante de l'infrastructure physique. Cette technologie s'intègre pleinement dans les marchés des environnements virtualisés, des déploiements de réseaux sans fil, de la VoIP, des passerelles Internet d'entreprise et familiales.

De plus, cette fonctionnalité peut être étendue sur des ports de commutateurs distants à travers toute l'infrastructure. Dans ce cas, les commutateurs devront transporter entre eux du trafic appartenant à plusieurs VLANs sur une ou plusieurs liaisons spécifiques.

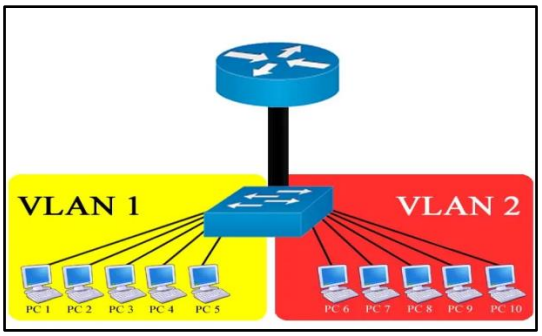


Figure II.2 : Exemple de VLANs.

- **Avantages et inconvénients de la technologie VLAN :** nous citerons quelques avantages acquis de la technologie VLAN :

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

A titre d'inconvénients, nous pouvons citer :

- Architecture adaptées ;
- Investissements dans l'infrastructure ;
- Montées en compétences du personnel [24].

- **Configuration des VLANs :** un commutateur gère l'attribution des VLAN par port ; ces ports peuvent être configurés dans l'un des deux modes suivants [25]:

- **Mode Access :** le port est directement connecté à un terminal (poste bureautique, imprimante, téléphone IP, **etc**.). Les trames Ethernet en provenance ou à destination de ces équipements ne sont pas marquées sur ce type de port.
- **mode Trunk :** le port est utilisé pour interconnecter le commutateur à tout autre équipement (Figure II.3). **Les** trames Ethernet en provenance ou à destination de ces équipements sont marquées sur ce type de port.

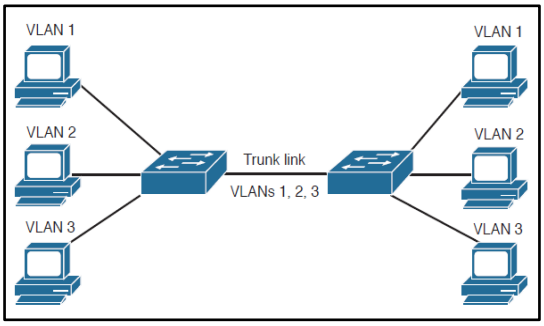


Figure II.3 : VLANs en mode Trunk.

- **DTP (Dynamic Trunking Protocol) :** est un protocole propriétaire Cisco permettant de négocier dynamiquement le mode (trunk ou access) d'un lien reliant un port du commutateur à l'équipement situé à l'autre bout du câble. Cette fonctionnalité est activée par défaut, le commutateur émet donc régulièrement des trames DTP sur toutes ses interfaces [25].
- **VTP (Vlan Trunking Protocol) :** le protocole VTP est un protocole de couche 2 propriétaires de la compagnie CISCO. Son avantage principal c'est sa capacité de propager automatiquement des VLAN configurés sur un commutateur en mode serveur vers les autres commutateurs configurés en mode client (Figure II.4).

Il existe 3 modes de configurations possibles d'un commutateur CISCO :

a) **Mode serveur :** c'est le mode par défaut de tous les commutateurs niveau 2 de CISCO. Le commutateur-serveur propage les VLANs et leurs paramètres aux autres commutateurs « client » du même domaine VTP. Le serveur-commutateur enregistre les informations des VLANs dans sa NVRAM. On peut créer, supprimer et renommer les VLANs tout en propageant ces changements aux autres commutateurs du réseau via des paquets « vtp advertisement ».

b) **Mode client :** on ne peut pas créer, supprimer ni renommer les VLANs au niveau du commutateur-client. Les informations des VLANs qui lui sont propagées ne sont pas enregistrées dans sa NVRAM.

c) **Mode transparent :** le commutateur en mode « transparent » ne participe pas au protocole VTP. Il transmet les « vtp advertisement » aux autres clients VTP. On peut créer, renommer ou supprimer des VLANs mais ils seront uniquement associés à ce commutateur [26].

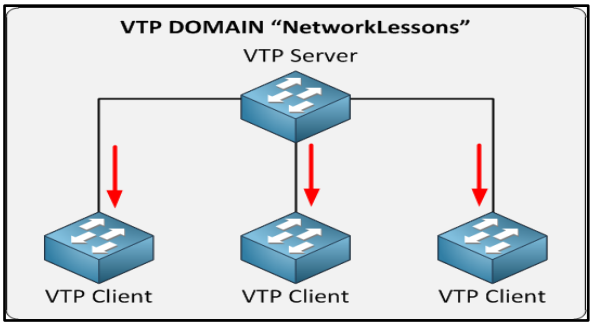


Figure II.4 : Le VTP Client et VTP Serveur.

II.5.1.2. Pare-feu (firewalls)

Un pare-feu est une appareille de protection du réseau qui surveille le trafic entrant et sortant et décide d'autoriser ou de bloquer une partie de ce trafic en fonction d'un ensemble de règles de sécurité prédéfinies (Figure II.5). Il peut être un équipement physique, un logiciel ou une combinaison des deux. Leur utilisation permet l'établissement d'une barrière entre les réseaux internes sécurisés et contrôlés qui sont dignes de confiance et les réseaux externes non fiables tels qu'Internet.

Afin qu'un firewall soit effectif, tout le trafic de et vers Internet doit passer par le firewall [27].

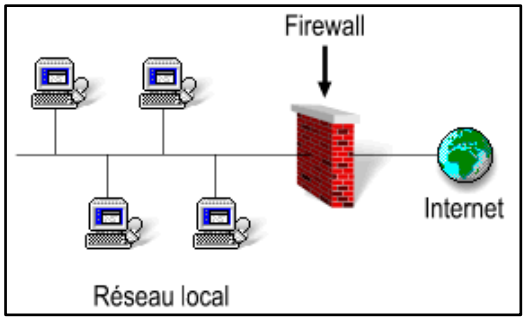


Figure II.5 : Un pare-feu (Firewall).

- **Les avantages du firewall :** les avantages du firewall sont nombreux. Nous citerons quelques-uns [28] :

- Il concentre la sécurité réseau en un seul point (chocke point) : l'administrateur peut définir un point de centralisation (chocke point) à partir duquel il pourra protéger le réseau privé dans son entier.
- Il permet la génération d'alarmes et le monitoring : le firewall est un système efficace de gestion des accès et de monitoring du réseau. Il est impératif que le responsable réseau évalue régulièrement le trafic qui transite par celui-ci. afin de s'assurer que le pare-feu n'a pas été contourné ou cracké.
- Il est un point unique de panne : en cas de panne, le réseau interne privé continuera cependant de fonctionner, seul l'accès inter-réseaux est perdu.

- **Les limitations du firewall :** voici les trois 3 principales limitations du firewall :

- Il ne protège pas contre les attaques qui ne passent pas par lui: les utilisateurs du réseau privé peuvent être tentés d'obtenir une connexion directe avec un provider Internet. Ce type de connexion ouvre un chemin d'accès potentiel à l'extérieur ;
- Il ne prévient pas contre le transfert de fichiers infectés par un virus : parce qu'il y a une multitude de virus différents, de systèmes d'exploitation et de manières d'encoder et de compresser les fichiers, un pare-feu peut difficilement analyser chaque fichier dans l'espoir incertain d'en déceler un. Il faut donc installer des antivirus sur chaque station ;
- Il ne prévient pas contre les applications du type Cheval de Troie : le Cheval de Troie est un programme à l'apparence sans dangers, mais qui se révèle, une fois exécuté, une véritable menace pour l'organisation. Par exemple, un Cheval de Troie exécuté sur une station hôte peut modifier les fichiers relatifs à la sécurité, rendant l'accès plus aisé pour un intrus désirant s'introduire dans le système.

II.5.1.3. IDS & IPS

Sont des objets lies au pare-feu qui fonctionne comme un filtrage de sécurité réseau (Figure II.6), Ils sont le résultat de l'évolution technologique. Un « IDS » détecte les intrusions, et lorsqu'il peut y réagir automatiquement, il devient un « IPS » [29].

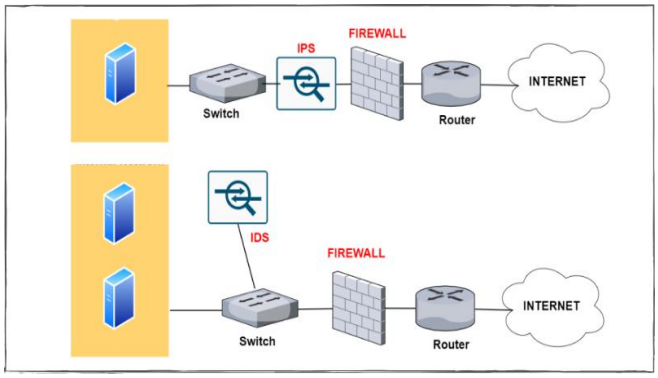


Figure II.6 : IDS & IPS.

- **IDS (Intrusion Detection System) :** un système de détection d'intrusion est un appareil qui surveille un réseau ou un système à la recherche d'activités malveillantes ou de violations des politiques de sécurité. Toute activité malveillante ou violation est généralement signalée aux administrateurs ou collectée de manière centralisée via des systèmes de gestion des informations et des événements de sécurité.
- **IPS (Intrusion Prevention Systems) :** systèmes de prévention des intrusions ou également connu sous le nom de système de détection et de prévention des intrusions (IDPS), sont des dispositifs de sécurité réseau qui surveillent les activités du réseau ou du système pour détecter toute activité malveillante. Les principales fonctions des IPS sont d'identifier les activités malveillantes, d'enregistrer des informations sur ces activités, de les signaler et de tenter de les bloquer ou de les arrêter**.**

II.5.1.4. DMZ (demilitarized zone)

La DMZ (zone démilitarisée) est un sous-réseau isolé à la fois du réseau local et de l'internet**,** c'est en quelque sorte une zone tampon, entre un réseau sécurisé et un réseau non sécurisé (Internet) (Figure II.7).

Les serveurs installés dans la partie externe de la DMZ permettent de fournir des services aux réseaux externes, tout en protégeant le réseau interne contres des intrusions possibles [30].

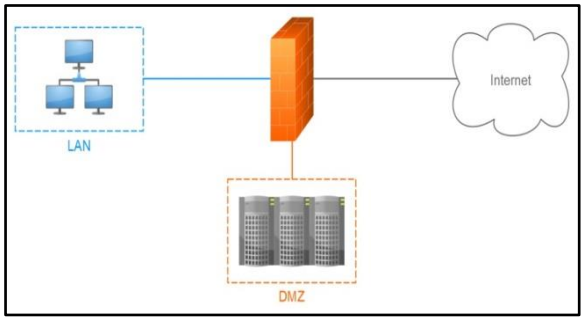


Figure II.7 : DMZ.

II.5.1.5. VPN (Virtuel Privat Network)

- **Définition** : un VPN est un tunnel sécurisé **permettant** la communication entre deux entités y compris au travers de réseau peu sûrs comme peut l'être le réseau Internet [31].
- **Principe d'un VPN :** un VPN (réseau privé virtuel) s'agira d'établir un canal chiffré entré deux nœuds quelconque de l'internet, ces nœuds pouvant eux-mêmes être des routeurs d'entrée de réseau (Figure II.8). On aura ainsi établé une sorte de tunnel qui, a travers l'internet, reliera deux parties éloignées l'une de l'autre du réseau d'une même entreprise. Avec le chiffrement un VPN personnel pourra établir pour un utilisateur (entre son ordinateur et un réseau local de l'entreprise) [32].

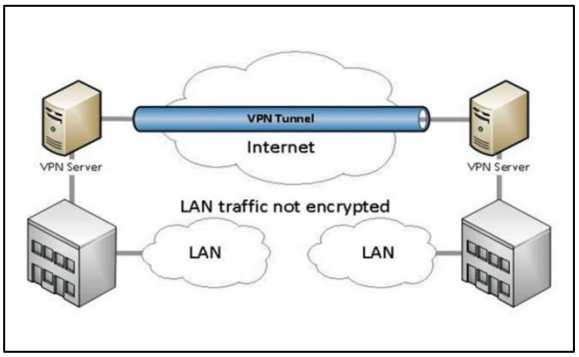


Figure II.8 : VPN.

II.5.1.6. IPSec (Internet Protocol Security)

Introduit des mécanismes de sécurité au niveau du Protocole IP, de telle sorte qu'il y ait indépendance vis-à-vis du protocole de transport. Le rôle de se protocole de sécurité est de garantir l'intégrité, l'authentification, la confidentialité et la protection contre les techniques rejouant des séquences précédentes [33].

II.5.2. Sécurité au niveau des commutateurs

II.5.2.1. mécanisme de sécurité de port (port-Security)

C'est un mécanisme qui permet de contrôler les adresses MAC source des en-têtes Ethernet des trames émises, d'une machine étant identifiée d'un commutateur. La configuration du port-Security nécessite que le commutateur de rattachement propose la fonctionnalité.

La fonction port-Security est capable d'analyser les adresses MAC des machines connectée sur un port spécifique, d'autoriser une machine sur un port si l'adresse MAC de cette dernière est préalablement déclarer, d'interdire des communications si certain adresses MAC ne sont pas déclarer sur un port donné. Il peut lutter contre l'usurpation d'adresse MAC en interdisant la présence d'une même adresse sur des ports déférents.

Il existe deux déférents types de configuration du port-Security :

a) **La configuration statique :** c'est à l'administrateur réseau de configurer manuellement l'ensemble des adresses MAC des machines du réseau.
b) **La configuration dynamique :** c'est le placement du switch dans un mode d'apprentissage dynamique où il va recenser l'ensemble des adresses MAC observées sur chaque port. La fonction « sticky mode » autorise en dur dans la configuration courante uniquement la première adresse connectée au port [34].

- **Mode de violation :** une Violation est une action prise en cas de non-respect d'une règle port-Security. Trois mode pour qu'un commutateur se réagira a une violation [35]:

a) **Mode protect :** dès que la violation est constatée, le port arrête de transférer le trafic des adresses non autorisées sans envoyer de message de log.
b) **Mode restrict :** dès que la violation est constatée, le port arrête de transférer le trafic des adresses non autorisées et transmet un message de log.
c) **Mode shutdown :** dès que la violation est constatée, le port passe en état err-disabled (shutdown) et un message de log est envoyé.

II.5.3. DHCP Snooping

Le DHCP Snooping est disponible directement sur les commutateurs. Il permet de détecter les serveurs pirates et de prémunir le réseau des paquets DHCP malicieux ou malformés.

- **Son fonctionnement :** sa mise en place consiste à déclarer explicitement les serveurs DHCP dits de confiance en indiquant les ports du commutateur sur lesquels ils sont rattachés. Le commutateur construit alors une base de données sous la forme d'un fichier brut contenant les correspondances entre adresse IP assignée par le serveur DHCP circulant sur le réseau. Au besoin, il bloque certaines requêtes et désactive les ports sur lequel il a détecté un serveur pirate, ou en tout cas, une machine émettant des requêtes qui ne correspondent pas à la logique du protocole par rapport aux entrées enregistrer dans la base [34].

II.5.4. STP (Protocole Spanning Tree)

Le protocole Spanning-Tree (STP) empêche la formation de boucles lorsque des commutateurs ou des ponts sont interconnectés via plusieurs chemins. Le protocole Spanning-Tree implémente l'algorithme IEEE 802.1D en échangeant des messages BPDU avec d'autres commutateurs pour détecter les boucles, puis supprime la boucle [36].

- **Garde BPDU ou BPDU Guard :** la protection BPDU est une amélioration de STP qui supprime les nœuds du réseau qui renvoient des BPDU. Il applique les limites de domaine STP et maintient les topologies actives prévisibles en n'autorisant aucun périphérique réseau derrière un port avec la protection BPDU activée à participer à STP.

  Dans certains cas, les appareils connectés (tels que les stations terminales) n'ont pas à initier ou participer aux changements de topologie STP. Dans ce cas, le port auquel la station terminale est connectée à la protection STP BPDU activée. La protection STP BPDU arrête le port et le met dans l'état errdisable. Cela désactive la capacité des appareils connectés à initier ou à participer à des topologies STP. Un message de journal est ensuite généré pour les violations de protection BPDU et un message CLI s'affiche pour informer l'administrateur réseau de la configuration gravement invalide. La fonction de protection BPDU fournit une réponse sécurisée aux configurations non valides, car si la récupération errdisable n'est pas activée, les administrateurs doivent remettre l'interface en service manuellement [37].

II.6. Sécurité des accès à l'administration du commutateur

II.6.1. Telnet

Est un protocole non sécurisé permettant l'accès à distance à des équipements. Étant donné que toutes les informations sont envoyées en clair sur le réseau, notamment le mot de passe de l'administrateur (sauf si Telnet est couplé à d'autres mécanismes de sécurité), ce protocole est à proscrire sur les matériels supportant des protocoles d'administration sécurisés comme SSH [25].

II.6.2. SSH

Est un protocole sécurisé d'accès à distance à l'interface en ligne de commande d'équipements. Le protocole SSH crypte les échanges ce qui rend son utilisation plus sécurisée [38].

Il existe deux versions de protocole SSH que nous devons les citer :

a) **SSHv1 :** est un protocole qui va permettre une connexion sécurisée (chiffrée) qui, dans un réseau moderne doit remplacer les anciennes connexions Telnet. Il couvre l'authentification, la confidentialité et l'intégrité des données.
b) **SSHv2 :** ce protocole est incompatible avec la version 1, il a été introduit avec de nombreuses amélioration par rapport SSH1 ce qui le rend plus sécurisé**.**

Conclusion

A travers ce chapitre, nous avons vu l'impact de la sécurité informatique sur le réseau, pour lequel nous avons décrit plus en détail les attaques provenant des logiciels malveillants et présenté des stratégies de sécurité. Ainsi, différents procédés et mécanismes connus comme (SHH, Port-Security, Le STP BPDU Guard,…etc.) pour sécuriser les réseaux. Le chapitre suivant portera sur le contexte des travaux et la sécurisation d'un réseau local.

Chapitre III

Réalisation des Solutions Proposées

Introduction

Dans ce chapitre, nous passerons à la dernière étape qui est la réalisation. Nous intéressons à la sécurité d'un réseau d'entreprise, Pour commencer nous présentons l'organisme d'accueil, par la suite le simulateur « PACKET TRACERT » qui est utilisé pour la configuration des éléments que contient le réseau et enfin nous configurons entièrement le réseau et nous appliquons les solutions proposées pour le sécuriser.

III.1. Presentation de l'organisme d'accueil

III.1.1. Présentation de l'entreprise et de son historique

Cevital agro-industrie est une des filiales du groupe Cevital, elle fait partie des entreprises algériennes qui ont vu le jour dès l'entrée de notre pays en économie de marché. Elle a été créée par des fonds privés en 1998, elle a pour actionnaires principaux, Mr ISSAD REBRAB et ses enfants. Le siège social de CEVITAL est sis à Garidi Kouba (Alger), le complexe qui a fait l'objet de notre cas d'étude est situé au nouveau quai de l'arrière port de Bejaïa.

Cevital 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. Elle couvre les besoins nationaux et a permis de faire passer l'Algérie du stade d'importateur à celui d'exportateur pour les huiles, les margarines et le sucre. Leader en Afrique et dans le Bassin Méditerranéen dans l'industrie du sucre et de l'huile végétale ; Ses produits se vendent dans plusieurs pays, notamment en Europe, au Maghreb, au Moyen Orient et en Afrique de l'Ouest.

Figure III.1 : Logo de Cevital.

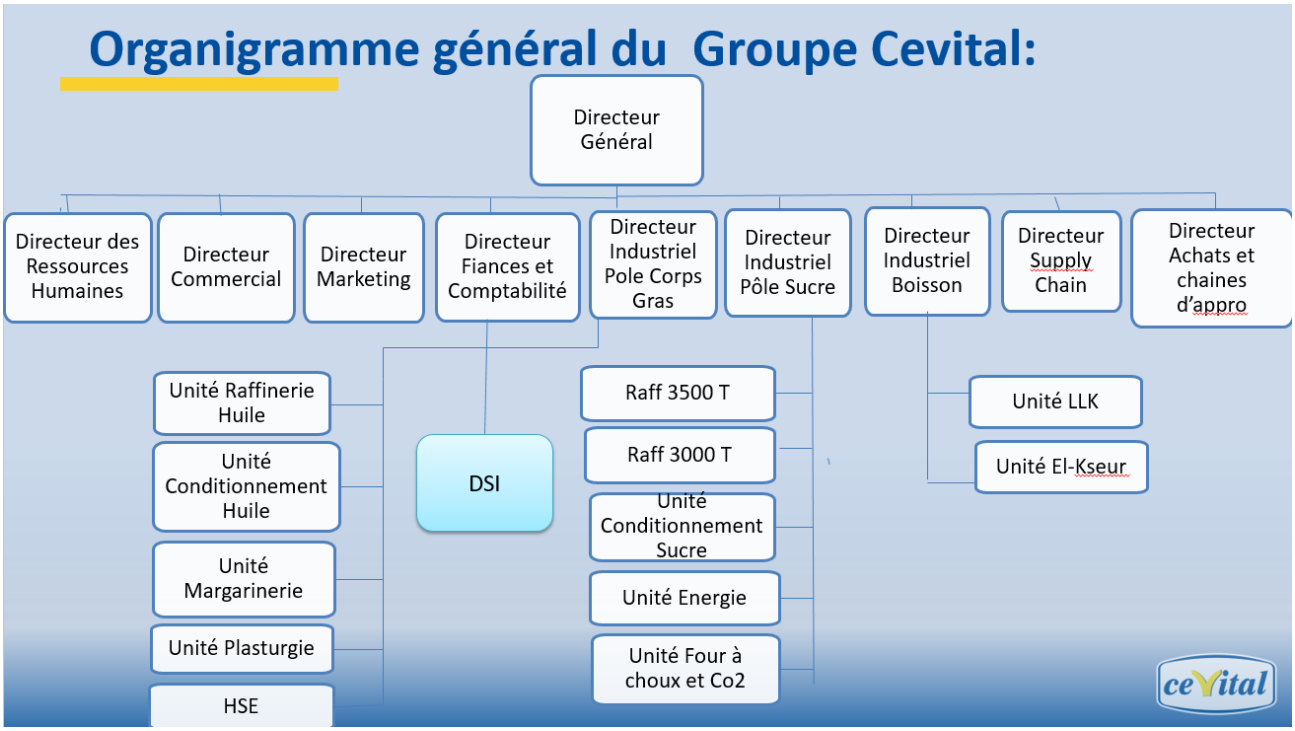


Figure III.2 : Organigramme général du Groupe Cevital.

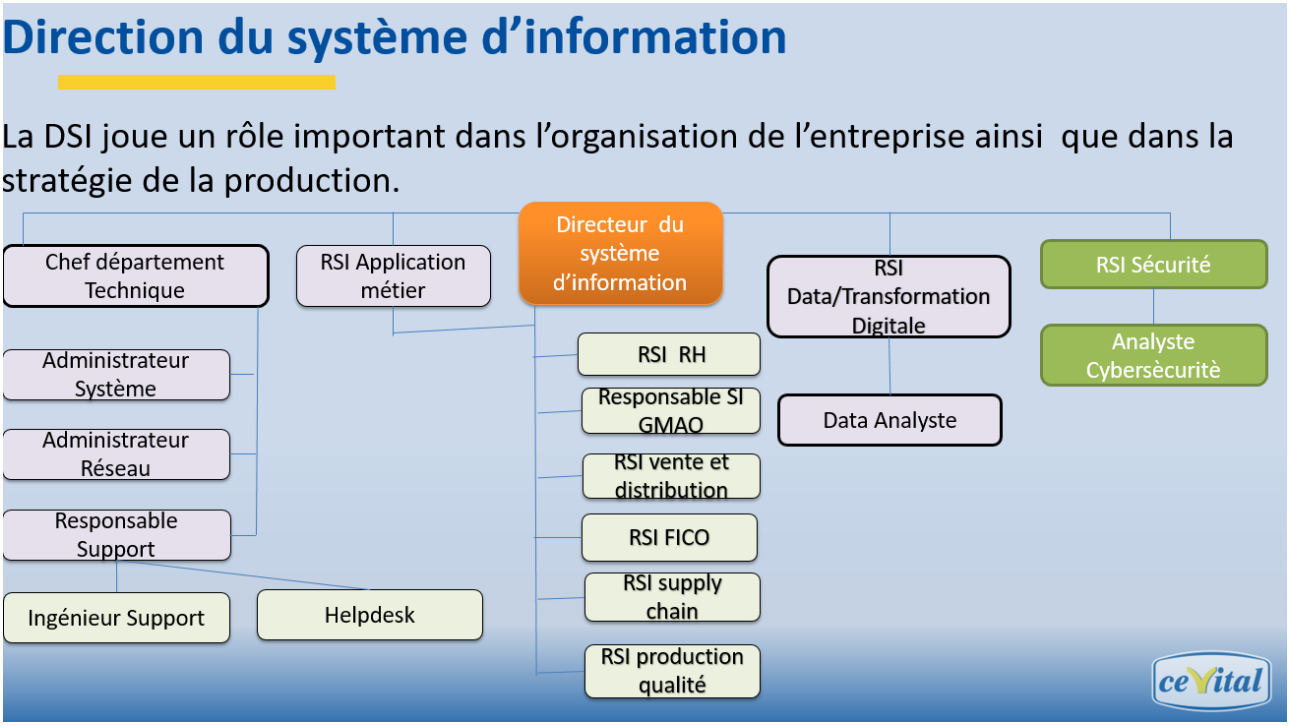


Figure III.3 : Direction du système d'information.

III.1.2. Vision, Mission du Groupe Cevital

Vision : Assurer la croissance et la diversification rentables pour devenir un acteur majeur en Afrique, en Europe et dans le bassin Méditerranéen.
Mission : Contribuer au développement économique de l'Algérie et couvrir la demande des citoyens national et même à l'international.

III.1.3. 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.

III.1.4. Codification des équipements de Cevital

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

III.1.5. Utilisation du réseau informatique

Cevital compte environ mille utilisateurs du réseau informatique ; ses différents collaborateurs utilisent chaque jour les différentes applications et service offerts par le réseau pour mener à bien leur travail. Nous pouvons citer les applications et services suivants :

- Applications de GPAO (Gestion de la production assistée par ordinateur).
- Le partage de document via un serveur dédié (cloud privé).
- Microsoft Exchange et Azure.
- Service Mail.
- Application comptabilité et gestion des stocks.
- Fournie un accès internet au collaborateur.

III.1.6. Situation géographique

Le complexe Cevital agro-industrie s'étends sur une superficie de 45 000 M2 (c'est le plus grand complexe privé en Algérie), il se situe au niveau du nouveau quai du port de Bejaia, à proximité de la route nationale N° 09 et N°26 ; Sur un terrain à l'origine inconstructible qui a été récupéré et viabilisé avec la dernière technologie de consolidation des

sols par le système de colonnes ballastées (337 km de colonnes ballastées de 18M chacune ont été réalisées) ainsi qu'une partie à gagner sur la mer. L'entreprise a beaucoup profité de cette situation qui lui donne un avantage de proximité économique car se trouve proche du port et de l'aéroport.

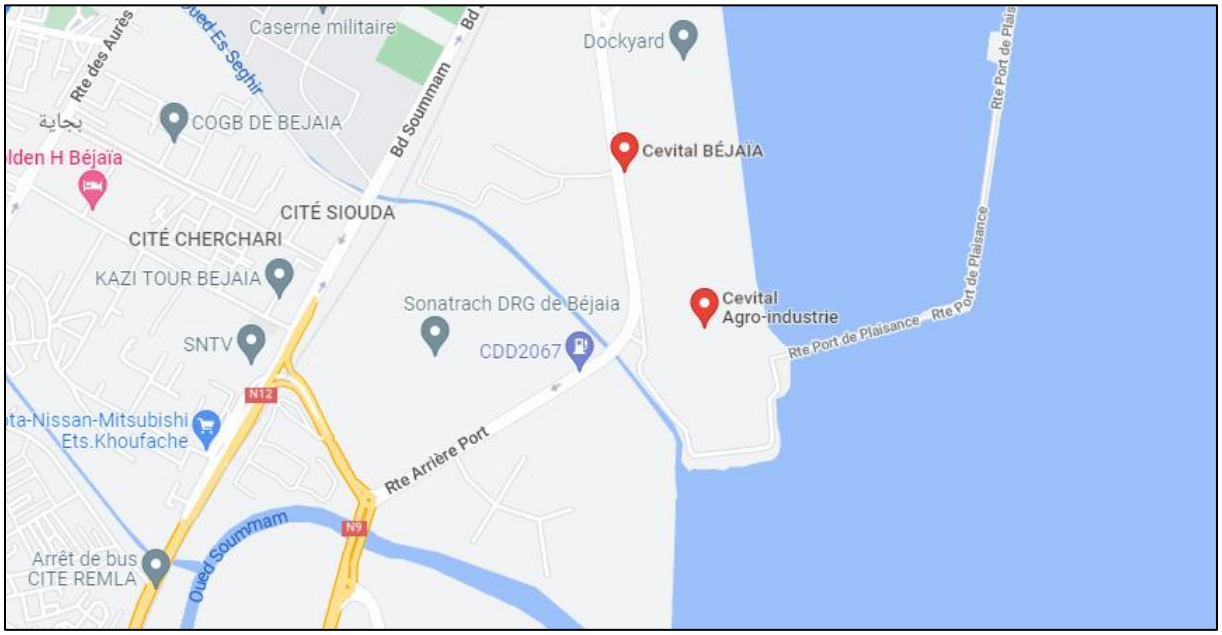


Figure III.4 : Carte géographique de Cevital Bejaia.

III.1.7. Infrastructure matériel

Le réseau actuel de Cevital est constitué de nombreux modèles de Switches :

Le model de Switch	Nombre de Switch
WS-C2960X-48FPS-L	9 Switches
WS-C2960X-24PS-L	16 Switches
C6807-XL	2 Switches
WS-C3850-24S	2 Switches
Nexus 3048	3 Switches
Cisco 2911/K9	1 Switches
Cisco 2921/K9	1 Switches
WS-C2960-48PST-L	2 Switches
WS-C2960-24TC-L	3 Switches
WS-C2960-8TC-L	1 Switches
WS-C2960C-12PC-L V05	5 Switches
WS-C2960-24TC-L	7 Switches
WS-C2960-48TC-L	9 Switches
WS-C2960G-24TC-L	2 Switches
WS-C2950G-12-EI	2 Switches
C2950-I6K2L2Q4-M	1 Switches

Tableau III.1 : Les modèles des Switches de l'entreprise

III.1.8. La sécurité au niveau de Cevital

L'entreprise Cevital utilise deux type de Firewall comme mécanisme de barrière, interdisant l'entrée a certain types de trafic et en autorisant à d'autres trafic suivant une politique de sécurité pour sécuriser son réseaux .

Firewalls :

- Data-Center : Palo Alto (Quantité 02)
- Internet: Palo alto (Quantité 02)
- Sites distants : Fortigate

Point d'accès WIFI : Marque Ruckus

III.1.9. Les Vlans par direction

Ce tableau présente la classification des Vlans de l'entreprise Cevital par leur direction :

Direction	**VLAN**
DRH	VLAN10
Direction des Appro	VLAN11
DSI	VLAN12
Raff Huile	VLAN13
Raff sucre 3000T	VLAN14
Division utilités	VLAN15
Supply-chain	VLAN16
Unité margarinerie	VLAN17
Printer	VLAN18
Téléphone	VLAN20
Voice	VLAN21
Direction R&D	VLAN22
Performance industriel	VLAN23
Unité Cdt Huile	VLAN24
Management switch	VLAN25
DFC	VLAN26
Commercial	VLAN27
Direction générale	VLAN28
Direction qualité et management système	VLAN 29
Raff sucre 3500T	VLAN30
Cdt sucre	VLAN31
Caméra	VLAN32
Projets	VLAN33
Trituration	VLAN36

Tableau III.2 : Classification des VLANs de l'entreprise Cevital.

III.2.Présentation de simulateur « Cisco Packet Tracer »

- **Définition :** C'est un outil pédagogique et simulateur de réseau, développé par CISCO System pour concevoir configurer, dépanner et visualiser le trafic réseau dans un environnement de programmes simulé et contrôle. Packet Tracer permet d'élaborer des représentations virtuelles de réseaux et d'émuler un grand nombre des fonctions

offertes par les périphériques réseau. La (figure III.5) illustre l'interface principale de logiciel Cisco Packet Tracer.

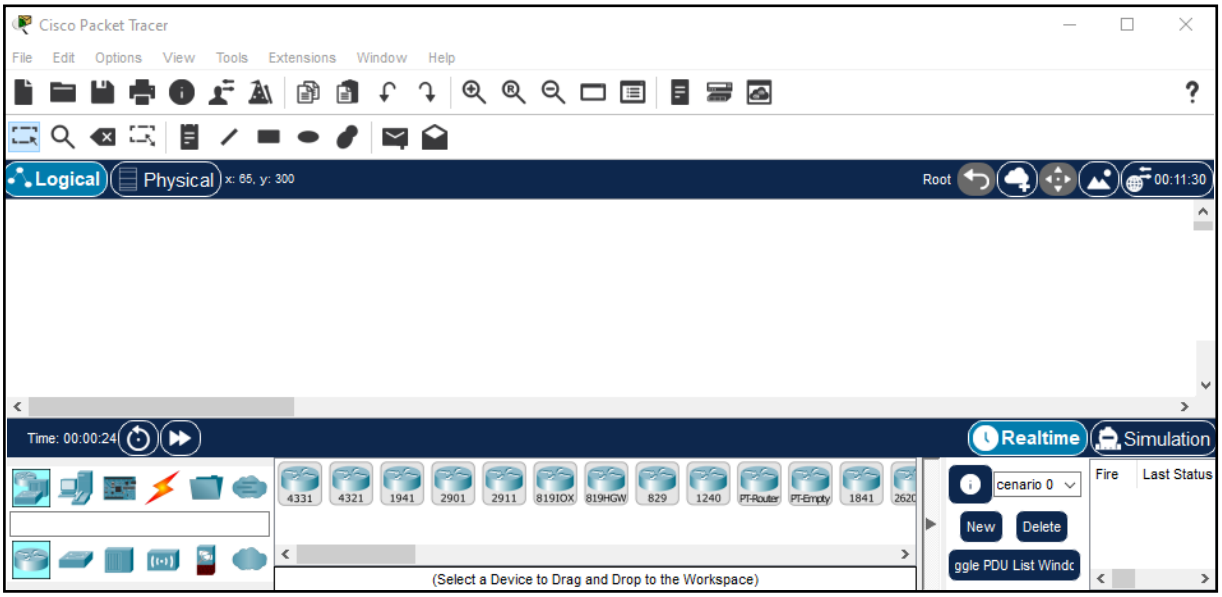


Figure III.5 : Interface Cisco Packet Tracer.

- **Méthode de configuration des équipements**

Toutes les configurations des équipements du réseau seront réalisées au niveau de CLI (Commande Langage Interface). CLI est une interface de simulateur Cisco Packet Tracer qui permet la configuration des équipements du réseau à l'aide d'un langage de commandes, c'est-à-dire que c'est à partir des commandes introduites par l'utilisateur du logiciel que la configuration est réalisée. La figure ci-dessous nous montre l'interface de CLI :

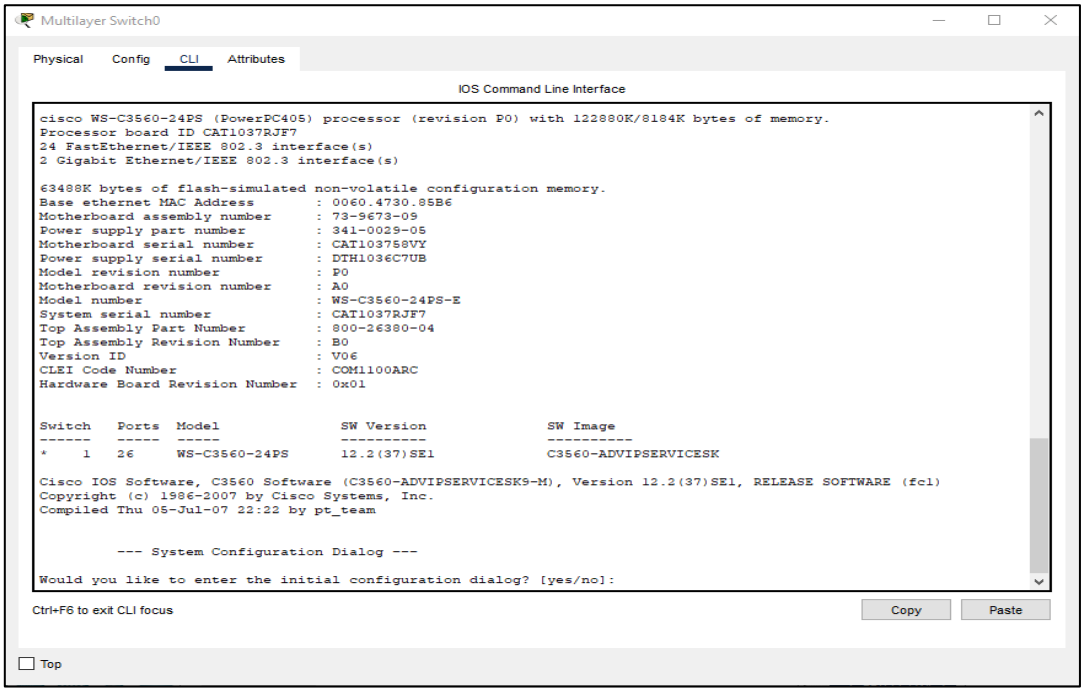


Figure III.6 : Interface CLI.

III.3. La réalisation

III.3.1. Le matériel utilisé

Avant d'entamer la configuration nous devons installer le réseau sur Packet Tracer. Pour ce faire, nous aurons besoins du matériel suivant :

- 04 Multilayer Switch de model 3560-24PS ;
- 02 commutateurs Cisco de model 2960 IOS15 ;
- 04 PC pour le test ;
- Des câbles droits pour connecter les ordinateurs ou commutateurs aux commutateurs ou Multilayer switch.

Le réseau de Cevital sera comme suit sous Packet Tracer :

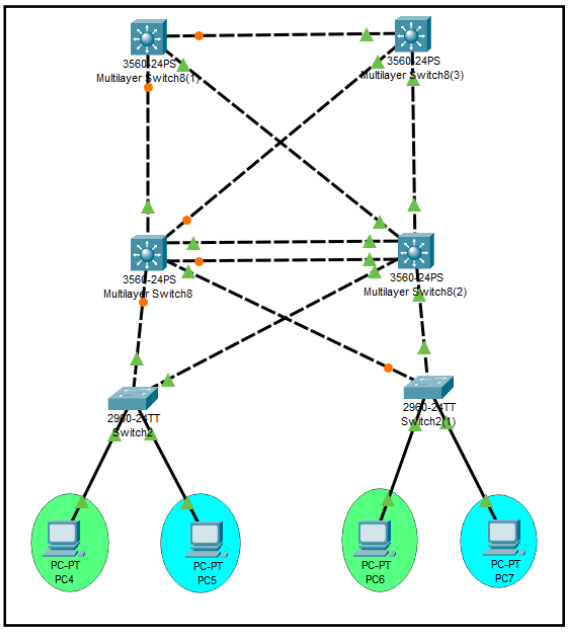


Figure III.7 : L'architecture proposée de Cevital sous Packet Tracer.

Réellement le réseau de l'entreprise Cevital est décomposé en trois parties « couches » :

- La partie 1 « couche Cœur » qui travaille sur un niveau de couche 3 ;
- La partie 2 « couche Distribution » qui travaille sur un niveau de couches 2 et 3 ;
- La partie 3 « couche Accès » qui travaille sur un niveau de couche 2.

Nous montrons ça sur l'architecteur proposée par cette dernière :

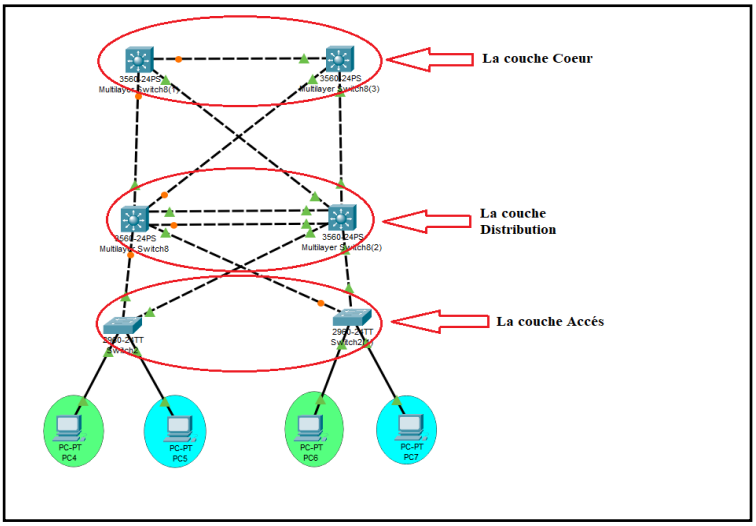


Figure III.8 : Représentation des couches de réseau proposé.

III.3.2. Les étapes de simulation

Nous avons deux étapes de configuration, la première qui est une configuration entière pour faire fonctionner le réseau, la deuxième est sécurisé le réseau.

III.3.2.1. configuration entière du réseau

Pour configurer entièrement le réseau nous devons passer par plusieurs étapes de configuration, une pour les commutateurs de niveau 3 « couche cœur », une autre pour les commutateurs de niveau 2&3 « couche Distribution » et une configuration pour les commutateurs de niveau 2 « couche Accès ».

- **Configuration du nom :** dans cette configuration, chaque commutateur se voit attribuer un nom, nous accédons d'abord au switch et activons le mode d'exécution privilégié avec la commande « enable », puis passons en mode configuration avec la commande « configure terminal », et enfin attribuons un nom au commutateur en utilisant la commande " hostname <nom de commutateur>".

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Switch1-Distribution
Switch1-Distribution(config)#
```

Figure III.9 : Configuration du nom.

Pour les autres Switches restants, nous attribuons un nom pour chaque ‘un avec la même configuration.

- **configuration de VTP :**

Sur les commutateurs de la couche Distribution :

- **Etape 1 :** d’abord nous commençons par la création des VLANs, le VLANs 10 sous le nom « DRH » et le VLANs 11 sous le nom « Direction des Appro ».

```
Switch1-Distribution(config)#vlan 10
Switch1-Distribution(config-vlan)#name DRH
Switch1-Distribution(config-vlan)#vlan 11
Switch1-Distribution(config-vlan)#name Direction-des-Appro
Switch1-Distribution(config-vlan)#
```

Figure III.10 : Création des VLANs.

Puis nous vérifions cette configuration à l'aide de la commande « show vlan brief »

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, 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-des-Appro               active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Figure III.11 : Vérification de la création des VLANS.

Ici nous voyons que les VLAN 10 et 11 sont bien crées.

- **Etape 2 :** ensuite nous mettons les interfaces agrégées dans les Switches (Switch1-Distribution et Switch2-Distribution) en mode trunk.

```
Switch1-Distribution(config)#int range Fa0/1-4
Switch1-Distribution(config-if-range)# switchport trunk encapsulation DOt1q
Switch1-Distribution(config-if-range)# switchport mode trunk



Switch1-Distribution(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up
```

Figure III.12 : La mise des interfaces en mode Trunk.

Nous tapons la commande « show running config », le résultat de cette commande montre les interfaces qui sont en mode trunk.

```
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
```

Figure III.13 : Les interfces en mode trunk.

- **Etape 03 :** dans cette étape, nous configurons le switch1-Distribution en mode serveur VTP avec un nom de domaine et nous donnons à lui un mot de passe.

```
Switch1-Distribution(config)#vtp mode server
Device mode already VTP SERVER.
Switch1-Distribution(config)#vtp domain Cevital.com
Changing VTP domain name from NULL to Cevital.com
Switch1-Distribution(config)#vtp password cisco
Setting device VLAN database password to cisco
Switch1-Distribution(config)#
```

FigureIII.14 : Configuration de VTP serveur.

- **Etape 04 :** maintenant nous créons trois clients VTP, le Switch « Switch2-Distribution » et les deux autres de la couche Accès qui sont « Switch1-Accès et Switch2-Accès » seront met en mode client.

```
Switch2-Distribution(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch2-Distribution(config)#vtp domain Cevital.com
Domain name already set to Cevital.com.
Switch2-Distribution(config)#vtp password cisco
Setting device VLAN database password to cisco
Switch2-Distribution(config)#
```

Figure III.15 : configuration de VTP clients.

Et même configuration pour les deux autres switches de la couche Accès.

Les switches mets en mode client reçoivent automatiquement les VLANs créés dans le switch serveur.

La commande « show vlan brief » montre que les VLANs sont bien diffuser par le serveur VTP, aux clients VTP.

```
Switch2-Distribution#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, 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-des-Appro               active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Figure III.16 : Les clients VTP (Switch2-Distribution).

Voici les deux autres Client VTP de la couche Accès :

```
Switch1-Acces#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 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-des-Appro               active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch1-Acces#
```

Figure III.17 : Les clients VTP (Switch1-Accés).

```
Switch2-Acces#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 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-des-Appro               active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch2-Acces#
```

Figure III.18 : Les clients VTP (Switch2-Accés).

Les VLANs « DRH et Direction-des-Appro » sont bien arrivés aux clients comme vu dans les figures précédentes. Donc les trois switches sont correctement configurés avec le VTP.

La figure suivante illustre les VTPs crées sur l'architecture réseau :

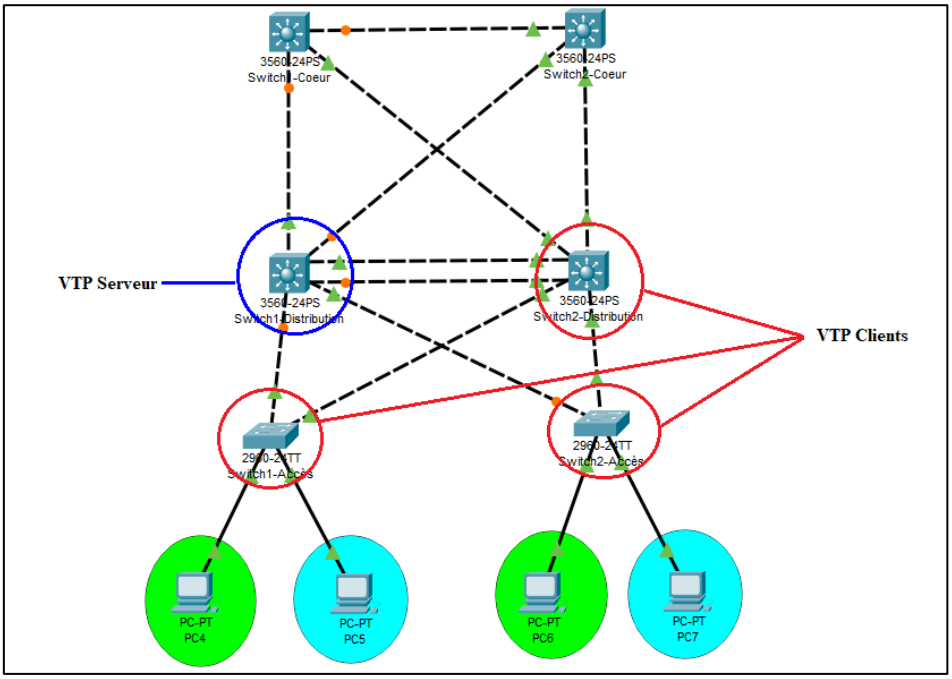


Figure III.19 : Représentation des VTPs sur L'architecture réseau.

- **Configuration de l'Etherchannel :**

Sur les commutateurs de la couche Distribution :

Pour configurer l'Etherchannel, sur le 'Switch1-Destribution', nous commençons d'abord par la création de groupe Channel 1 et nous le mettons en mode 'On' en utilisant cette commande :
« Channel-groupe 1 mode on », puis nous quittons ce mode et nous accédons aux interfaces du port Channel 1 et nous mettons toutes ces interfaces en mode trunk. Nous effectuons la même configuration sur le deuxième Switch qui est 'Switch2-Destribution'.

```
Switch1-Distribution#
Switch1-Distribution#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1-Distribution(config)#int range Fa0/3-4
Switch1-Distribution(config-if-range)#channel-group 1 mode on
Switch1-Distribution(config-if-range)#
%LINK-5-CHANGED: Interface Port-channel1, changed state to up

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

Switch1-Distribution(config-if-range)#exit
Switch1-Distribution(config)#int port-channel 1
Switch1-Distribution(config-if)#switchport mode trunk
Switch1-Distribution(config-if)#
```

Figure III.20 : Configuration de l'Etherchannel.

Enfin pour verifier le resultat de cette configuration nous tapons la commande «show running config ».

```
!
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
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
 channel-group 1 mode on
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode on
!
```

Figure III.21 : Verification de la configuration d'Etherchannel.

Donc nous voyons bien que le port channel 1 est en mode trunk ainsi les autres interfaces qui sont déjà aussi en mode trunk.

- **Configuration de STP :** dans notre architecture réseau, des boucles créent qui sont bloquées par le spanning tree et quelques interfaces de ces boucles sont mis en orange « éteints », la Figure suivante montre les interfaces éteints des boucles :

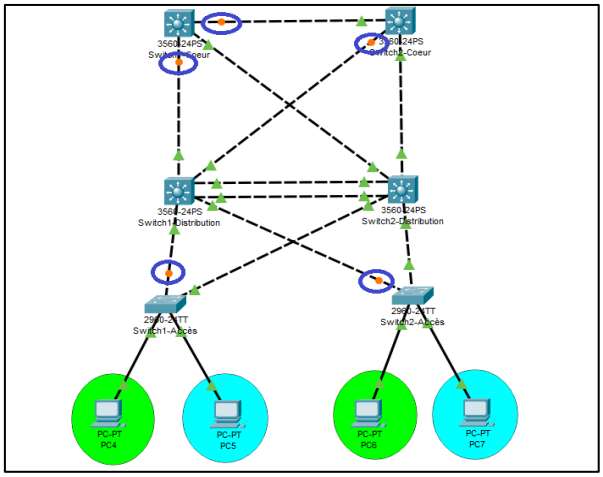


Figure III.22 : Les boucles bloqueés par le STP.

Afin de remédier ça nous configurons le STP au niveau des commutateurs de la couche Distriburion.

- La configuration de STP sur le switch1-Distribution :

```
Switch1-Distribution(config)#spanning-tree vlan 10 root primary
Switch1-Distribution(config)#spanning-tree vlan 11 root secondary
Switch1-Distribution(config)#
```

Figure III.23 : Configuration de STP au niveau de switch1-Distribution.

- La configuration de STP sur le switch2-Distribution : au niveau de ce switch nous mettons l'inverse de la configuration du switch1-Distribution :

```
Switch2-Distribution(config)#spanning-tree vlan 10 root secondary
Switch2-Distribution(config)#spanning-tree vlan 11 root primary
Switch2-Distribution(config)#
```

Figure III.24 : Configuration de STP au niveau de switch2-Distribution.

Voici le resultat de la configuration de STP :

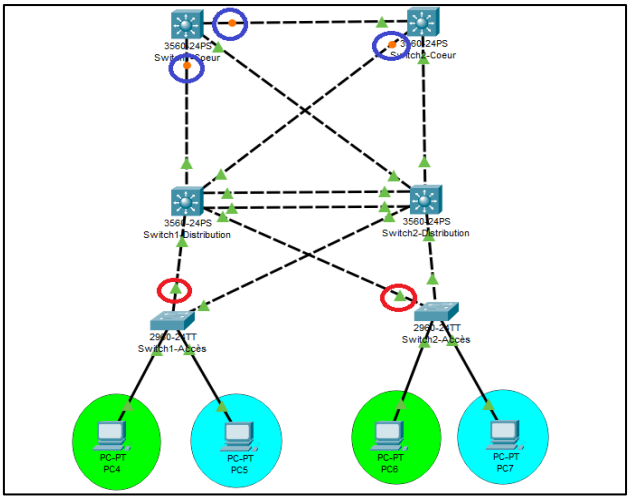


Figure III.25 : Resultat de la configuration de STP.

Dans la (FigureIII.25), les interfeces mis dans un cercle rouge sont devenu en vert « allumer » aprés avoir configurer le STP, par contre d'autres qui sont dans le cercle bleue restent toujours en orange «eteindre », car ces ports sont toujours de niveau 2 c'est aprés les configurations suivantes que nous les rendons comme interfaces et nous allons les passer de niveau 2 au niveau 3 pour que le STP ne va pas fonctionner sur ces ports, parce que le STP fonctionne seulement sur le niveau 2 (c'est un protocole de niveau 2).

- **Configuration de DHCP**

Sur les commutateurs de couche Distribution

Pour configurer le DHCP au niveau des switches de cette couche, nous devons créer deux serveurs DHCP, un au niveau de Switch1-Destribution et l'autre au niveau de Switch2-Destribution pour que le réseau reste toujours en fonctionnement si l'un de ces serveurs tombe en panne, et nous allons les configurer séparément (nous allons deviser les réseaux) pour ne pas avoir un conflit d'adresses.

Pour configurer le DHCP nous devons passer par des étapes qui sont :

- **Etape 01 :** nous commençons d'abord par exclure les adresses sur les deux Switches :

1) **Switch1-Distribution :**

```
Switch1-Distribution#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1-Distribution(config)#ip dhcp excluded-address 10.10.10.128 10.10.10.254
Switch1-Distribution(config)#ip dhcp excluded-address 10.10.11.128 10.10.11.254
Switch1-Distribution(config)#
```

Figure III.26 : Exclusion des adresses au niveau de Switch1-Distribution.

Nous tapons la commande « show running-config » :

```
Switch1-Distribution#show running-config
Building configuration...

Current configuration : 1720 bytes
!
version 12.2(37)SE1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch1-Distribution
!
!
!
ip dhcp excluded-address 10.10.10.128 10.10.10.254
ip dhcp excluded-address 10.10.11.128 10.10.11.254
!
```

Figure III.27 : Vérification des adresses exclure sur le Switch1-Distribution.

Nous avons exclure pour les réseaux 10.10.10.0 les adresses de 10.10.10.128 jusqu'à 10.10.10.254 et pour le réseau 10.10.11.0 les adresses de 10.10.11.128 jusqu'à 10.10.11.254, ça signifie que le serveur DHCP crée au niveau de ce Switch va distribuer que les adresses de 10.10.10.1 jusqu'à 10.10.10.127 pour le premier réseau et de 10.10.11.1 jusqu'à 10.10.11.127 pour le deuxième réseau.

1) Switch2-Distribution :

```
Switch2-Distribution#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch2-Distribution(config)#ip dhcp excluded-address 10.10.10.1 10.10.10.127
Switch2-Distribution(config)#ip dhcp excluded-address 10.10.11.1 10.10.11.127
Switch2-Distribution(config)#ip dhcp excluded-address 10.10.11.252 10.10.11.254
Switch2-Distribution(config)#ip dhcp excluded-address 10.10.10.252 10.10.10.254
Switch2-Distribution(config)#
```

Figure III.28 : Exclusion des adresses au niveau de Switch2-Distribution.

Nous tapons la commande « show running-config » :

```
Switch2-Distribution#show running-config
Building configuration...

Current configuration : 1818 bytes
!
version 12.2(37)SE1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch2-Distribution
!
!
!
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 10.10.10.252 10.10.10.254
ip dhcp excluded-address 10.10.11.252 10.10.11.254
!
```

Figure III.29 : Vérification des adresses exclure sur le Switch2-Distribution.

Même chose au niveau de ce Switch, nous effectuons des exclusions des adresses. Donc le serveur DHCP au niveau de ce Switch va distribuer les adresses qui ne sont pas exclure, dans un intervalle d'adresse de 10.10.10.128 jusqu'à 10.10.10.251 pour le réseau 10.10.10.0 et un intervalle d'adresse de 10.10.11.128 jusqu'à 10.10.11.251 pour le réseau 10.10.11.0.

- **Etape 02 :** après avoir exclure les adresses, maintenant nous pouvons donner les pools d'adresses pour les VLANs.

```
Switch1-Distribution(config)#ip dhcp pool vlan10
Switch1-Distribution(dhcp-config)#network 10.10.10.0 255.255.255.0
Switch1-Distribution(dhcp-config)#ip dhcp pool vlan11
Switch1-Distribution(dhcp-config)#network 10.10.11.0 255.255.255.0
Switch1-Distribution(dhcp-config)#
```

Figure III.30 : Les pools d'adresse pour les VLANs.

Nous effectuons la même configuration pour le deuxième switch qui est (Switch2-Destribution).

- **Etape 03 :** dans cette étape, lorsque nous configurons le DHCP nous devons donner les interfaces des VLANs et nous attribuons à chacune une adresse IP.

```
Switch1-Distribution(config)#interface vlan 10
Switch1-Distribution(config-if)#ip address 10.10.10.252 255.255.255.0
Switch1-Distribution(config-if)#exit
Switch1-Distribution(config)#interface vlan 11
Switch1-Distribution(config-if)#
%LINK-5-CHANGED: Interface Vlan11, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan11, changed state to up

Switch1-Distribution(config-if)#ip address 10.10.11.252 255.255.255.0
Switch1-Distribution(config-if)#
```

Figure III.31 : Attribution des adresses IP aux interfaces des VLANs.

Nous tapons la commande « show running-config » pour vérifier si les adresses sont bien attribuées :

```
!
interface Vlan10
 mac-address 0060.47db.d301
 ip address 10.10.10.252 255.255.255.0
!
interface Vlan11
 mac-address 0060.47db.d302
 ip address 10.10.11.252 255.255.255.0
!
```

Figure III.32 : Vérifications de l'arrivée des adresses.

Maintenant nous devons ajouter aussi les passerelles par défauts :

```
Switch1-Distribution(config)#ip dhcp pool vlan10
Switch1-Distribution(dhcp-config)#default-router 10.10.10.254
Switch1-Distribution(dhcp-config)#exit
Switch1-Distribution(config)#ip dhcp pool vlan11
Switch1-Distribution(dhcp-config)#default-router 10.10.11.254
```

Figure III.33 : L'ajout des passerelles par défauts.

Nous faisons la même configuration sur le deuxième switch qui est « Switch2-Destribution », sauf que les adresses des passerelles attribuées aux VLANs 10 et 11 ne seront

pas les mêmes que le Switch1-Distribution. Nous attribuons l'adresse 10.10.10.253 pour le vlan 10 et 10.10.11.253 pour le vlan 11 mais virtuellement ils vont partager la x.x.x.254.

Sur les commutateur de la couche Accès

- **Etape 01 :** sur les switch de cette couche nous devons attribuer pour chaque VLANs crées un port.

```
Switch2-Acces#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch2-Acces(config)#int Fa0/1
Switch2-Acces(config-if)#switchport mode access
Switch2-Acces(config-if)#switchport access vlan 10
Switch2-Acces(config-if)#int Fa/2
                         ^
% Invalid input detected at '^' marker.

Switch2-Acces(config-if)#int Fa0/2
Switch2-Acces(config-if)#switchport mode access
Switch2-Acces(config-if)#switchport access vlan 11
Switch2-Acces(config-if)#
```

Figure III.34 : Attribution des ports au VLANS.

Nous tapons la commande « show running-config » et nous voyons que les ports sont bien attribués aux VLANs.

```
Switch2-Acces#show running-config
Building configuration...

Current configuration : 1235 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch2-Acces
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 11
 switchport mode access
!
```

Figure III.35 : Verification de l'attribution des ports aux VLANs.

- **Etape 02 :** dans cette étape, les interfaces agrégées nous les mis en mode trunk, par la suite nous devons spécifier quel VLANs a le droit de passer (allocation des VLANS aux ports) :

```
Switch1-Acces(config)#int range Fa0/3-4
Switch1-Acces(config-if-range)#switchport mode trunk
Switch1-Acces(config-if-range)#switchport trunk allowed vlan all
Switch1-Acces(config-if-range)#
```

Figure III.36 : Le mode trunk et allocation des VLANs.

Avec la commande « show running-config », nous voyons que le mode trunk est activé sur les interfaces .

```
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport mode trunk
!
```

Figure III.37 : Verification de l'activation du mode trunk.

Le deuxieme switch sera configurer de la même manière.

Au final nous activons le DHCP sur les ordinateurs pour qu'ils reçoivent leurs adressses IP ainsi leurs default getway. Pour faire il suffit de cliquer sur le bouton DHCP sur leurs interfaces.

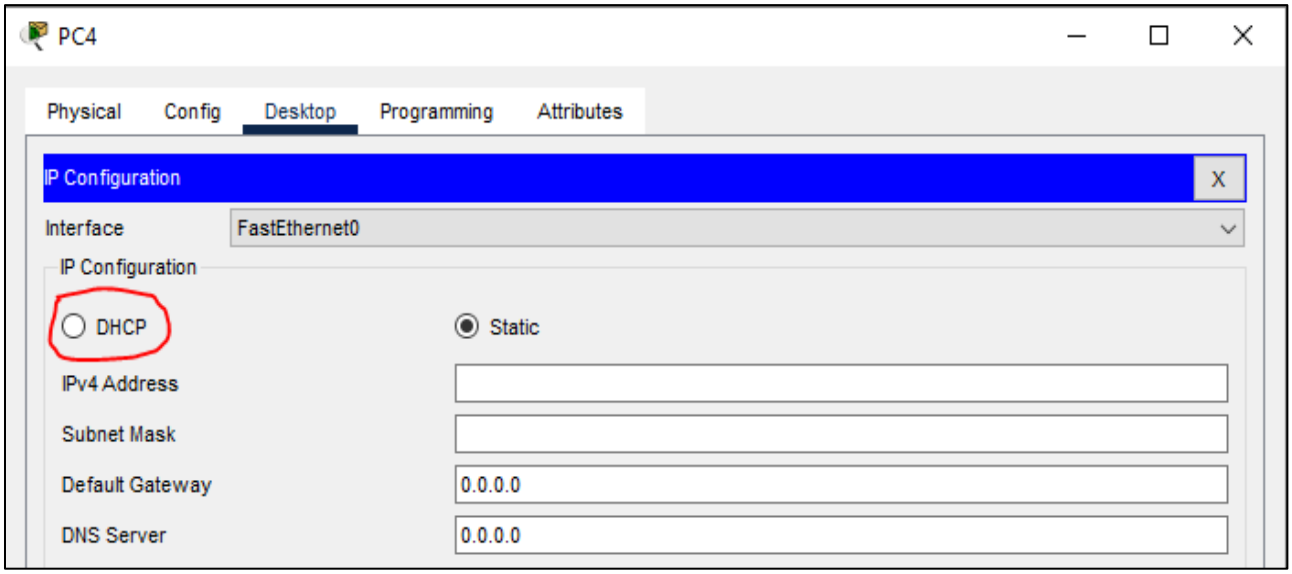


Figure III.38 : Interfaces de configuration du pc.

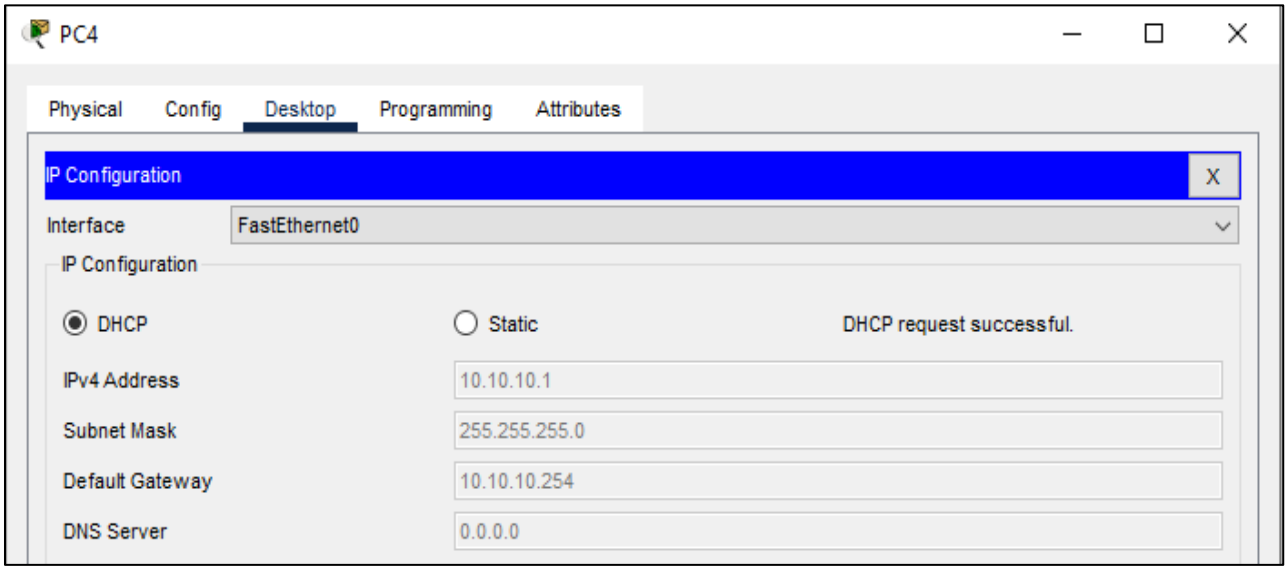


Figure III.39 : Activation de DHCP.

Nous effectuons la même operations pour les autres ordinateurs restants.

- **Configuration de HSRP**

- **Etape 01 : la configuration**

  Le HSRP sera configuré sur les commutateurs de la couche Distribution. Nous commençons d'abord par le Switch1-Distribution :

```
Switch1-Distribution(config)#interface vlan 10
Switch1-Distribution(config-if)#standby 10 ip 10.10.10.254
Switch1-Distribution(config-if)#standby 10 priority
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Standby -> Active
200
Switch1-Distribution(config-if)#standby 10 priority 200
Switch1-Distribution(config-if)#standby 10 preempt
Switch1-Distribution(config-if)#exit
Switch1-Distribution(config)#int vlan 11
Switch1-Distribution(config-if)#standby 11 ip 10.10.11.254
Switch1-Distribution(config-if)#standby 11 priority 150
Switch1-Distribution(config-if)#
%HSRP-6-STATECHANGE: Vlan11 Grp 11 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan11 Grp 11 state Standby -> Active

Switch1-Distribution(config-if)#standby 11 preempt
Switch1-Distribution(config-if)#
```

Figure III.40 : Configuration de HSRP au niveau du Switch1-Distribution.

La configuration au niveau de Switch2-Distribution sera :

```
Switch2-Distribution(config)#int vlan 10
Switch2-Distribution(config-if)#standby 10 ip 10.10.10.254
Switch2-Distribution(config-if)#
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby

Switch2-Distribution(config-if)#standby 10 priority 150
Switch2-Distribution(config-if)#standby 10 preempt
Switch2-Distribution(config-if)#exit
Switch2-Distribution(config)#int vlan 11
Switch2-Distribution(config-if)#standby 11 ip 10.10.11.254
Switch2-Distribution(config-if)#
%HSRP-6-STATECHANGE: Vlan11 Grp 11 state Speak -> Standby

Switch2-Distribution(config-if)#standby 11 priority 200
Switch2-Distribution(config-if)#standby 11 preempt
Switch2-Distribution(config-if)#
 %HSRP-6-STATECHANGE: Vlan11 Grp 11 state Standby -> Active
```

Figure III.41 : Configuration de HSRP au niveau du Switch2-Distribution.

- **Etape 02 : verification de fonctionnement de HSRP**

  1. Pour verifier si le HSRP fonctionne nous faisons un ping continue sur un pc , nous prenons par exemple le vlan 10 .

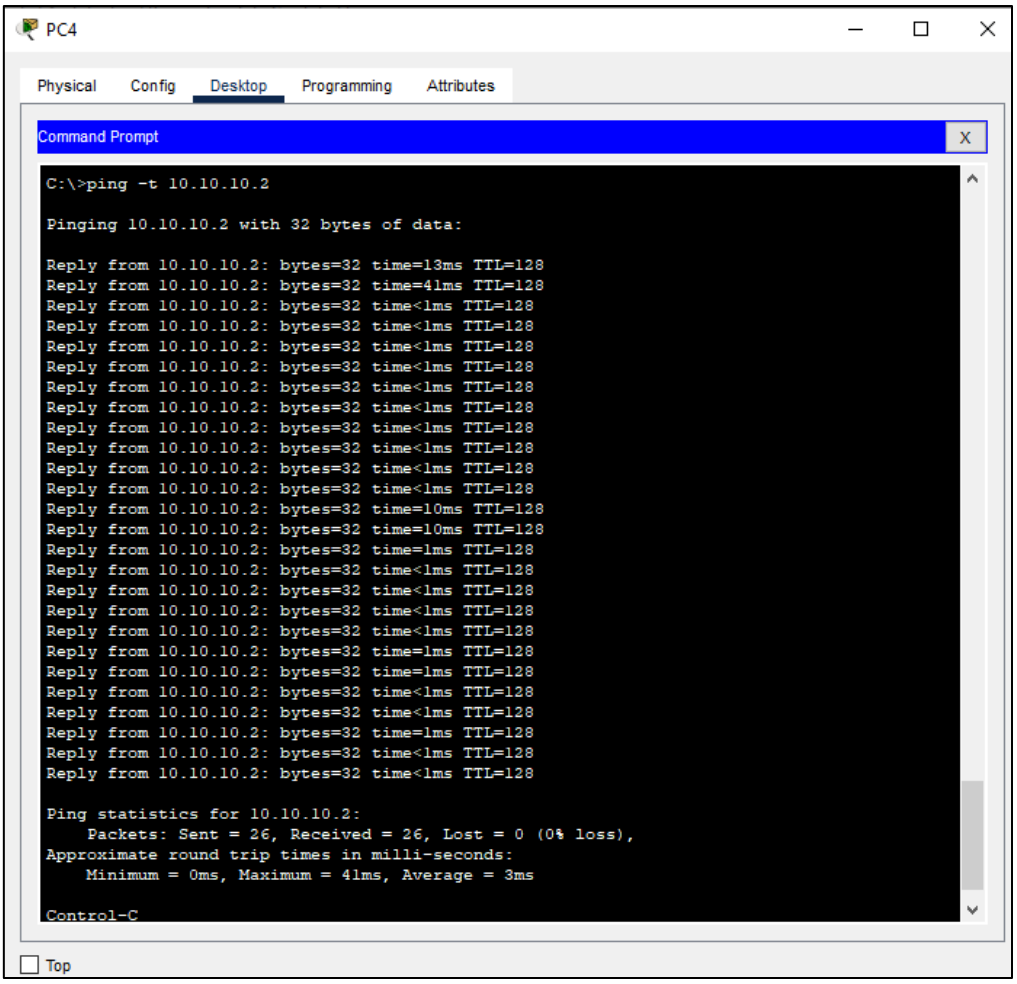


Figure III.42 : Ping continue.

Ici sur le vlan 10, son root-bridge est le Switch1-Destribution, donc les paquets transmis passent par la root-bridge1 vert la destination comme illustre la figure suivante :

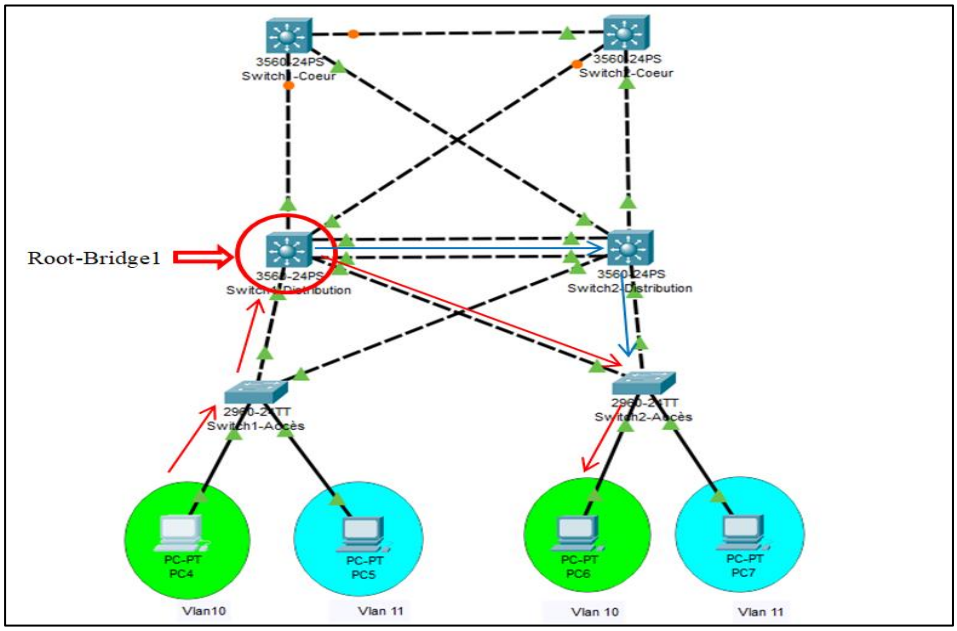


Figure III.43 : Représentation de passage de VLANs sur son root-bridge.

Les couleurs des flèches pour dire que le paquet peut empreinter soit le chemin qui est en flèches rouge ou un autre chemin qui est en bleue pour arriver à la destination.

2. Maintenant nous allons éteindre les interfaces de root-Bridge1 (cas d'une panne), donc ici le root-bridge2 va prendre la relève et le signal va passer. Alors le réseau reste toujours en fonctionnement.

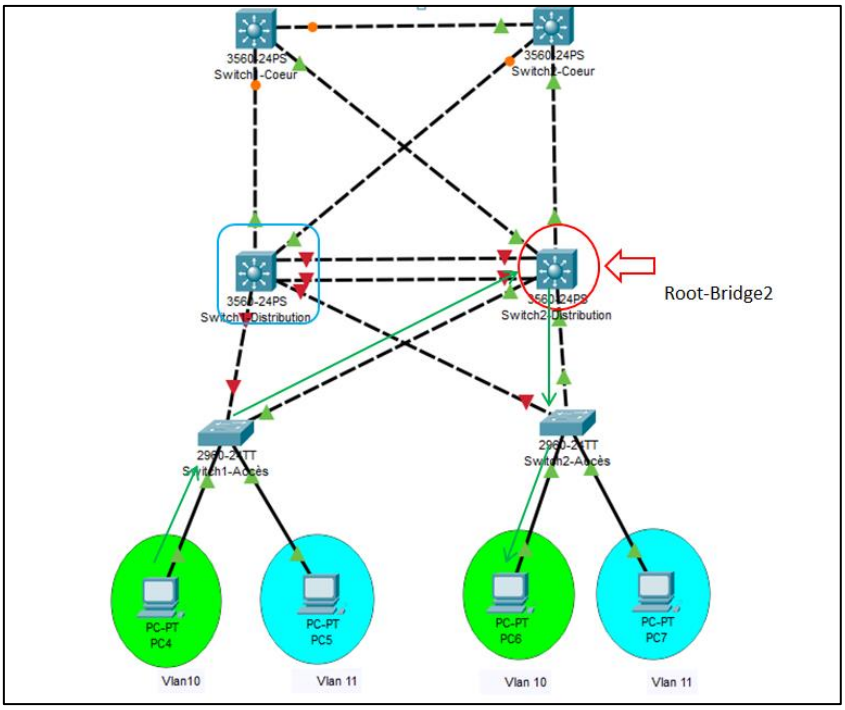


Figure III.44 : Fonctionnement de HSRP après avoir désactiver les ports.

Dans ce cas nous remarquons que le Ping va s'arrêter, il aura quelques paquets qui ne passent pas (le temps ou le root-bridge2 va commencer à fonctionner) et à partir du cinquième paquet le Ping va relancer (le signale passe).

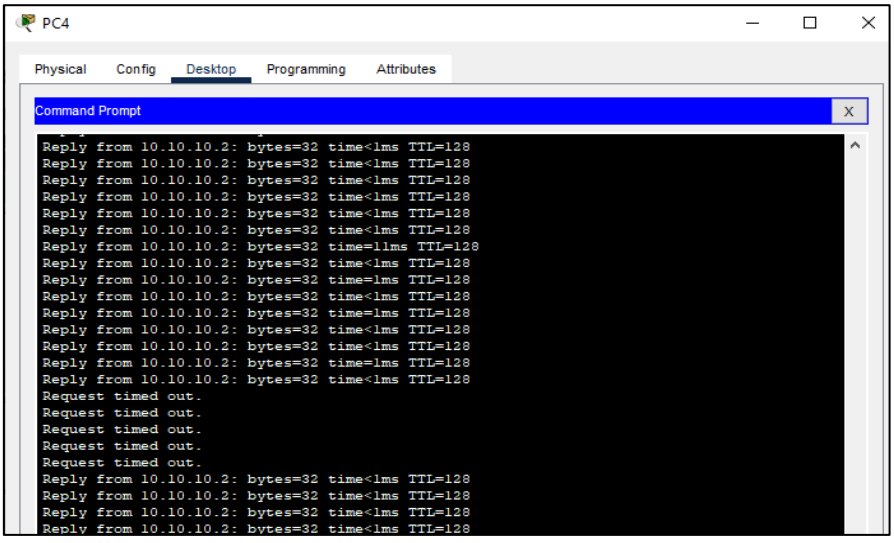


Figure III.45 : Le Ping après avoir désactiver les ports.

Maintenant, nous activons les interfaces du root-bridge1 (réparation de la panne). Nous remarquons que quelques paquets arrêtent de circuler en attendant que la root-bridge1 reprenne son fonctionnement, et elle fait passer les paquets.

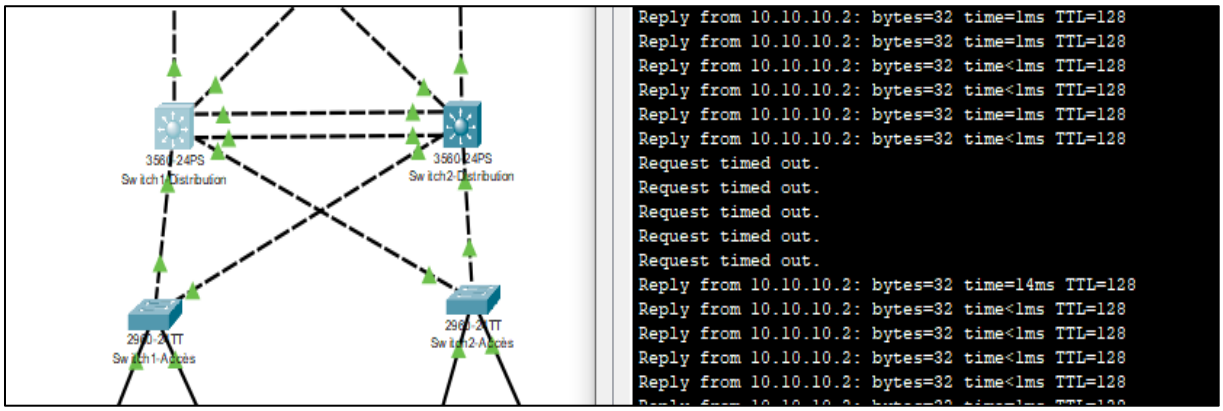


Figure III.46 : Ping après la reprise de Switch1-Destribution.

- **Configuration de l'OSPF**

Pour configurer l'OSPF nous passons par plusieurs étapes qui sont :

- **Etape 01 :** d'abord nous devons passer les ports des commutateurs de la couche Distribution et Cœur de niveau 2 au niveau 3 pour qu'ils devenir des interfaces et pour que nous pouvons attribuer des adresses. La figure suivante illustre les ports que nous devons passer de niveau 2 au niveau 3 :

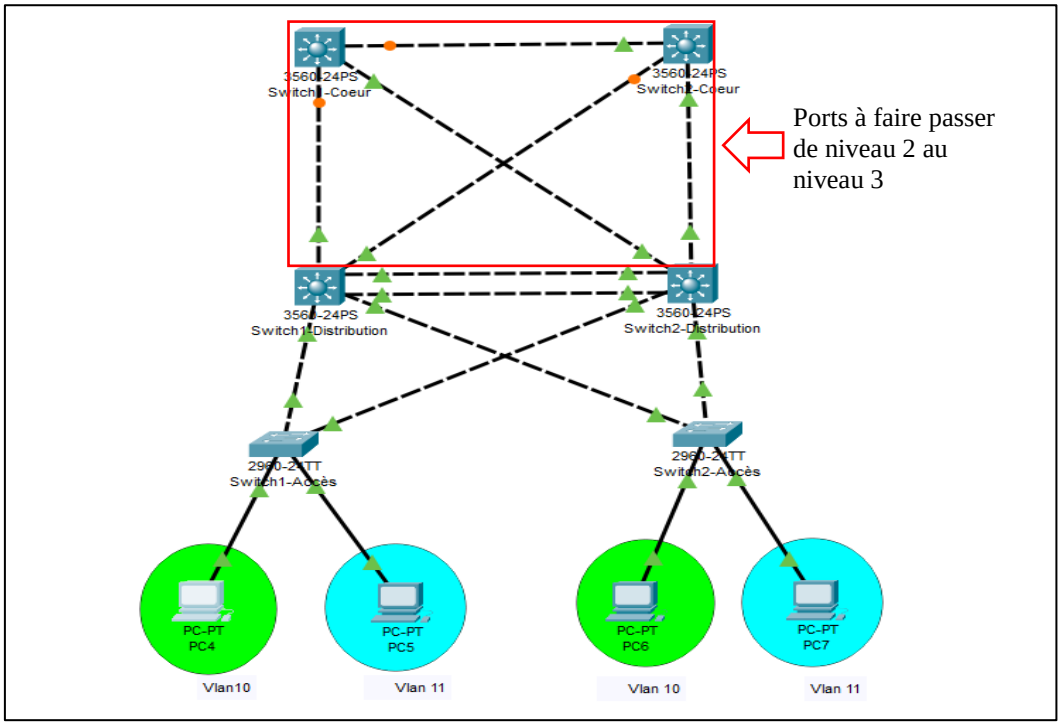


Figure III.47 : Les ports de niveau 2 qu'on doit passer au niveau 3.

La commande « no switchport » permet de faire passer les ports de niveau 2 aux interfaces de niveau 3 et nous les configurons :

```
Switch1-Distribution(config)#int Fa0/5
Switch1-Distribution(config-if)#no switchport
Switch1-Distribution(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

Switch1-Distribution(config-if)#ip address 10.10.12.1 255.255.255.252
```

Figure III.48 : Configuration des ports de niveau 2.

Nous vérifions les adresses des interfaces qu'ils sont bien attribuées :

```
!
interface FastEthernet0/5
 no switchport
 ip address 10.10.12.1 255.255.255.252
 duplex auto
 speed auto
!
```

Figure III.49 : Montrer la configuration des ports.

Et nous configurons toutes les autres interfaces de la même manière.

- **Etape 02 :** dans cette étape nous activons le routage :

Sur les commutateurs de couche cœur : nous configurons tous les réseaux qui sont directement connectés de cette façon :

```
Switch1-Coeur(config)#ip routing
Switch1-Coeur(config)#router ospf 1
Switch1-Coeur(config-router)#network 10.10.16.0 0.0.0.3
% Incomplete command.
Switch1-Coeur(config-router)#network 10.10.16.0 0.0.0.3 area 0
Switch1-Coeur(config-router)#network 10.10.15.0 0.0.0.3 area 0
Switch1-Coeur(config-router)#network 10.10.12.0 0.0.0.3 area 0
Switch1-Coeur(config-router)#
```

Figure III.50 : Configuration de l'OSPF dans la couche Cœur.

Confirmer « show running-config » si les réseaux qui sont directement connectés qu'ils sont bien configurer :

```
!
router ospf 1
 log-adjacency-changes
 network 10.10.16.0 0.0.0.3 area 0
 network 10.10.15.0 0.0.0.3 area 0
 network 10.10.12.0 0.0.0.3 area 0
!
ip classless
!
```

Figure III.51 : Vérifié la configuration de l'OSPF.

Et nous effectuons la configuration sur le deuxième switch2-cœur.

Sur les commutateurs de la couche Distribution : nous configurons tous les réseaux qui sont directement connectés et les autres réseaux virtuels de cette façon :

```
Switch1-Distribution(config)#ip routing
Switch1-Distribution(config)#router ospf 1
Switch1-Distribution(config-router)#network 10.10.10.0 0.0.0.255 area 0
Switch1-Distribution(config-router)#network 10.10.11.0 0.0.0.255 area 0
Switch1-Distribution(config-router)#network 10.10.12.0 0.0.0.3 area 0
Switch1-Distribution(config-router)#network 10.10.13.0 0.0.0.3 area 0
Switch1-Distribution(config-router)#
```

Figure III.52 : Configuration de l'OSPF dans la couche Distribution.

Confirmer avec « show running-config » si les réseaux qui sont directement connectés et les réseaux virtuels qu'ils sont bien configurer :

```
!
router ospf 1
 log-adjacency-changes
 network 10.10.12.0 0.0.0.3 area 0
 network 10.10.13.0 0.0.0.3 area 0
 network 10.10.10.0 0.0.0.255 area 0
 network 10.10.11.0 0.0.0.255 area 0
!
```

Figure III.53 : Vérifié la configuration de l'OSPF.

- **<u>Etape 03 :</u>** nous testons la connectivité de deux réseaux déférent, nous prenons par exemple deux vlan défèrent et nous lançons un Ping continue.la figure suivante montre le teste de connectivité :

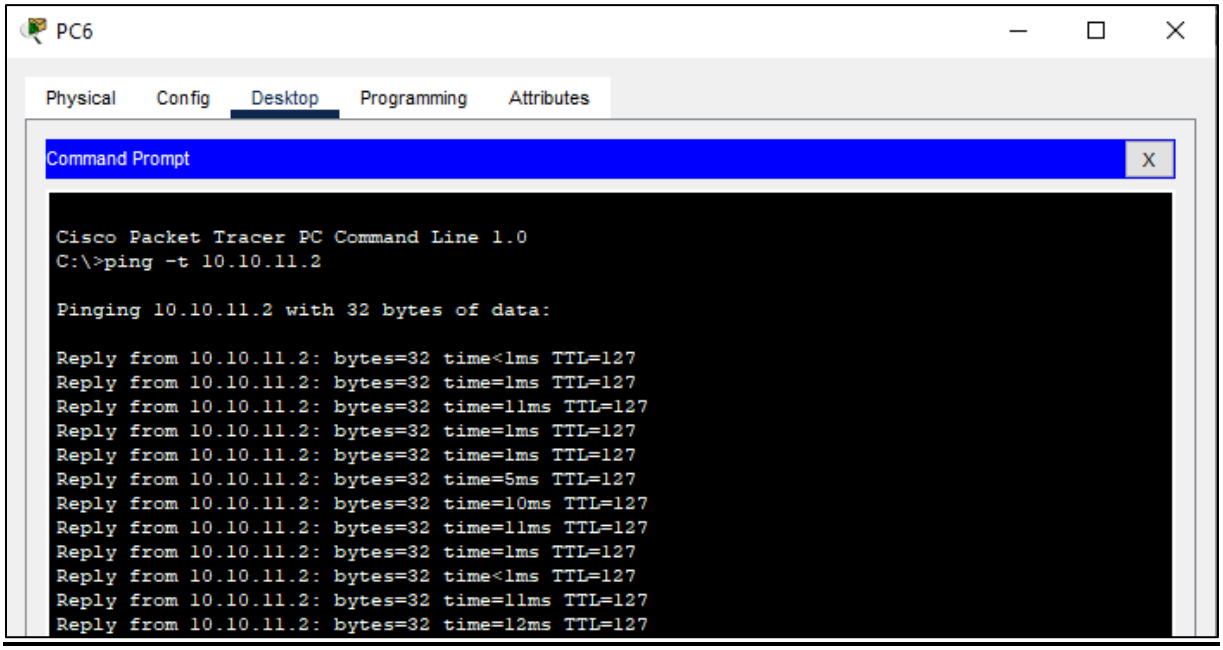


Figure III.54 : Testé la connectivité des deux réseaux avec le Ping.

Donc l'OSPF fonctionne très bien sur le réseau.

III.3.2.2. Sécuriser le réseau

Nous passons maintenant à l'application de la sécurité sur le réseau local, pour faire nous devons passer par plusieurs étapes de sécurité.

- **Configurations des mots de passe**

- **Etape 01 :** nous commençons par sécuriser l'exécution privilégie, pour faire nous mettons cette configuration :

```
Switch2-Acces>enable
Switch2-Acces#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch2-Acces(config)#enable password Cevital&Arab.stage/2022
Switch2-Acces(config)#
```

Figure III.55 : Configuration de la sécurité d'exécution privilégiée.

Avec la commande « show running config » nous vérifions cette configuration :

```
hostname Switch2-Acces
!
enable password Cevital&Arab.stage/2022
!
```

Figure III.56 : Vérification de la configuration.

Dans la configuration précédente nous remarquons que le mot de passe est toujours en clair, donc ce n'est pas une meilleur sécurité, pour la renforcer nous définissons un mot de passe chiffré par la configuration suivante :

```
Switch2-Acces(config)#enable secret Cevital&Arab.stage/2022
Switch2-Acces(config)#
```

Figure III.57 : Configuration chiffrée.

Nous vérifions le mot de passe chiffré :

```
!
hostname Switch2-Acces
!
enable secret 5 $1$mERr$okfMue4UoY0i7e.cJE3nQ0
!
```

Figure III.58 : Vérification de la configuration.

Nous effectuons la même configuration pour le reste de tous équipements du réseau.

- **Etape 02 :** par la suite nous configurons les lignes consoles :

```
Switch2-Acces(config)#line consol 0
Switch2-Acces(config-line)#password Cevital&Arab.stage/2022
Switch2-Acces(config-line)#login
Switch2-Acces(config-line)#
```

Figure III.59 : Configuration des lignes consoles.

Nous vérifions cette configuration avec la commande « show-running config » :

```
!
line con 0
 password Cevital&Arab.stage/2022
 login
!
```

Figure III.60 : Vérifie la configuration des lignes consoles.

Nous effectuons la même configuration pour le reste de tous équipements du réseau.

- **Etape 03 :** sécuriser les lignes virtuelles après avoir définir un mot de passe et activer la connexion :

```
Switch2-Acces(config)#line vty 0 4
Switch2-Acces(config-line)#password Cevital&Arab.stage/2022
Switch2-Acces(config-line)#login
Switch2-Acces(config-line)#
```

Figure III.61 : Configuration des lignes virtuelles.

Nous vérifions cette configuration avec la commande « show-running config » :

```
!
line vty 0 4
 password Cevital&Arab.stage/2022
 login
line vty 5 15
 login
!
```

Figure III.62 : Vérifie la configuration des lignes virtuelles.

Dans cette étape nous avons configurés l'accès à distance avec Telnet, et nous l'avons sécurisés avec l'attribution du mot de passe, nous montrons ça sur la figure suivante :

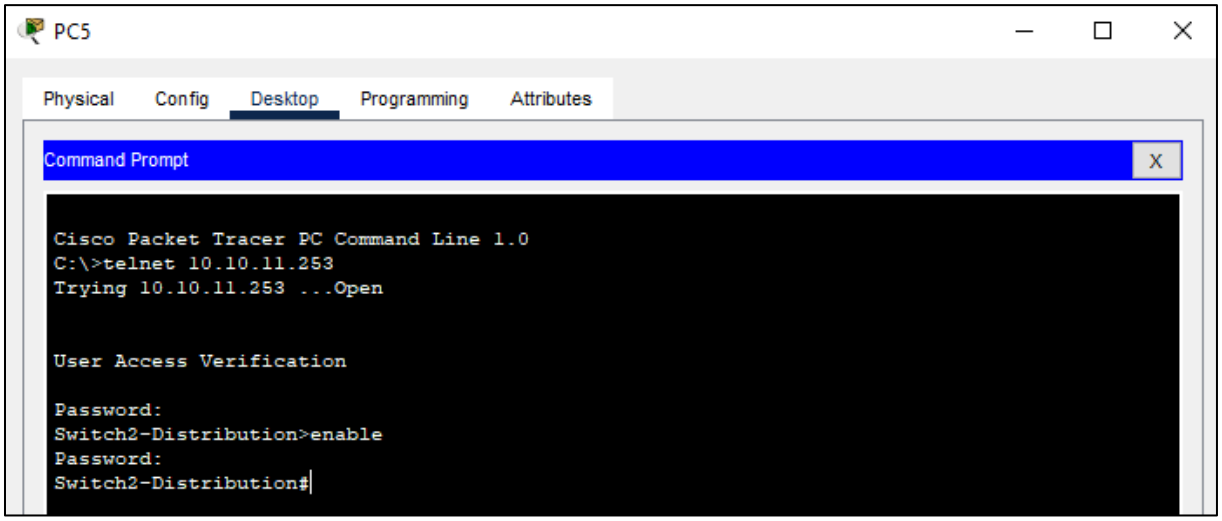


Figure III.63 : Accéder à distance via le PC5 avec Telnet.

- **Etape 04 :** les configurations précédentes des mots passes sont en clair, alors nous devons les chiffrés par cette configuration :

```
Switch2-Acces#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch2-Acces(config)#service password-encryption
Switch2-Acces(config)#
```

Figure III.64 : Chiffrés les mots de passes.

La figure suivante illustre les mots de passe chiffrés :

```
!
line con 0
 password 7 08024958000D041B542A1E052865373C3232275C55465153
 login
!
line vty 0 4
 password 7 08024958000D041B542A1E052865373C3232275C55465153
 login
```

Figure III.65 : Les mots de passe cryptés.

- **Configuration de L'SSH :** Vu que Telnet ne chiffre pas les informations entre le client et le serveur, cela permet à un analyseur de réseau d'intercepter les mots de passe et les données de configuration. Pour cella nous configurons le protocole SSH qui permet de chiffrer les informations et assurer l'authentification de l'ordinateur distant.

- **Etape 01 :** nous commençons par configurer le SSH de cette manière :

```
Switch2-Distribution#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch2-Distribution(config)#ip domain-name Cevital.com
Switch2-Distribution(config)#crypto key generate rsa
The name for the keys will be: Switch2-Distribution.Cevital.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]

Switch2-Distribution(config)#ip ssh version 2
*Mar 1 2:5:47.323: %SSH-5-ENABLED: SSH 1.99 has been enabled
Switch2-Distribution(config)#line vty 0 4
Switch2-Distribution(config-line)#transport input ssh
Switch2-Distribution(config-line)#login local
Switch2-Distribution(config-line)#exit
Switch2-Distribution(config)#username Cevital password Cevital&Arab.stage/2022
Switch2-Distribution(config)#exit
Switch2-Distribution#
%SYS-5-CONFIG_I: Configured from console by console

Switch2-Distribution#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch2-Distribution#
```

Figure III.66 : Configuration de l'SSH.

Nous vérifions cette configuration en tapant la commande « show running config » :

```
!
ip ssh version 2
ip domain-name Cevital.com
!
username Cevital privilege 1 password 7 08024958000D041B542A1E052865373C3232275C55465153
!
```

Figure III.67 : Vérification de la configuration de l'SSH.

- **Etape 02 :** maintenant nous montrons comment accéder à distance avec l'SSH :

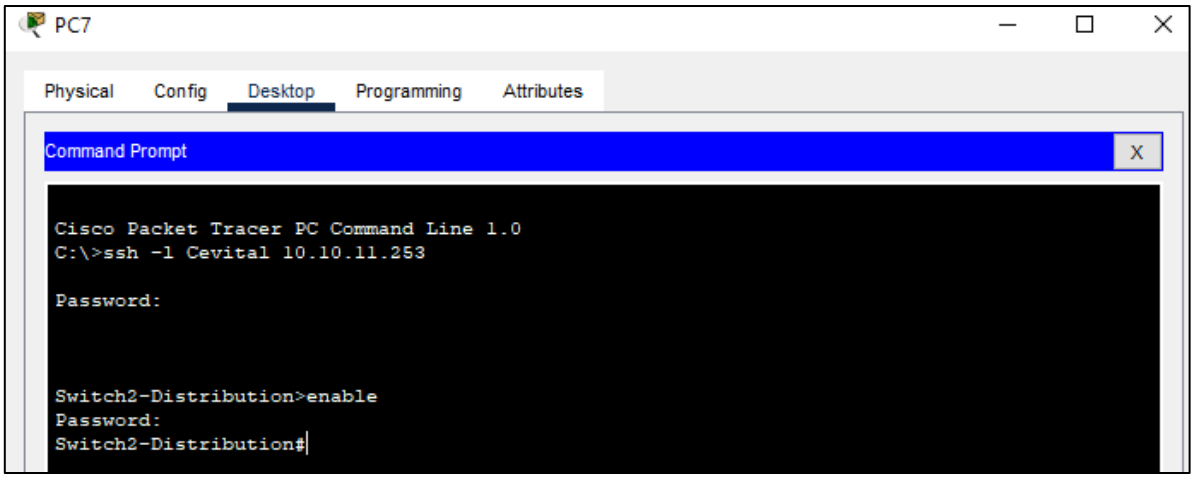


Figure III.68 : Accéder à distance via le PC7 avec SSH.

- **STP BPDUGUARD**

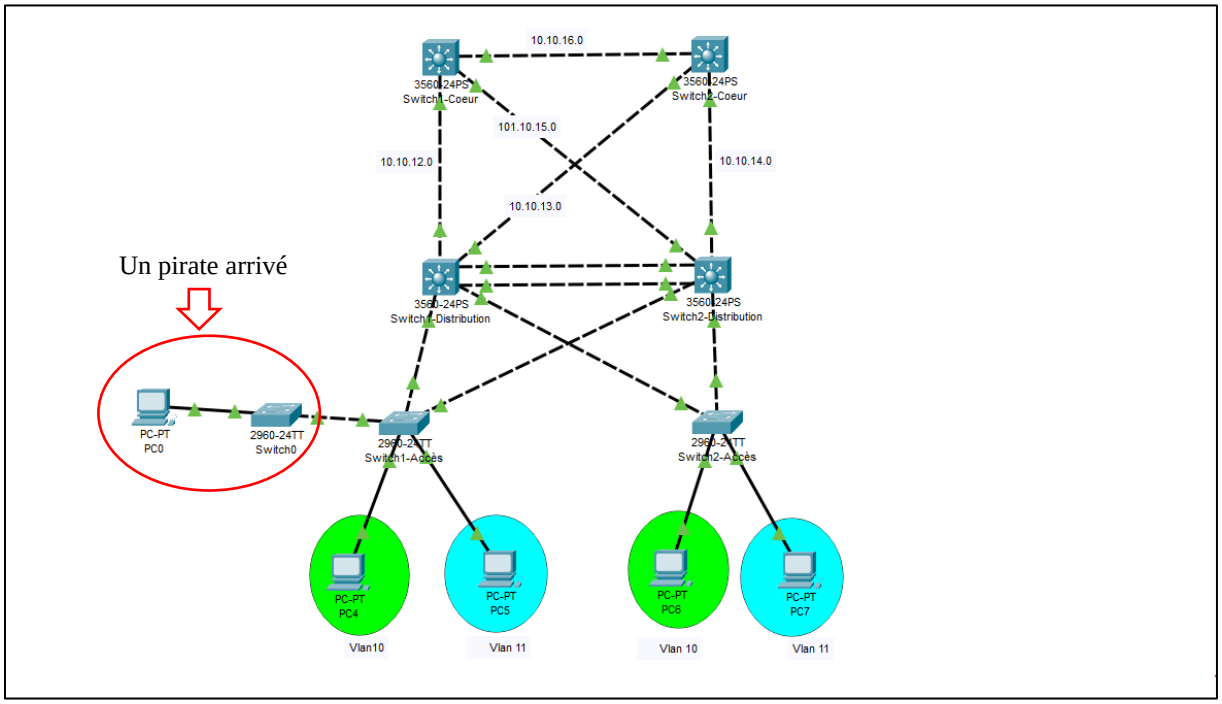


Figure III.69 : L'architecteur réseau avant la configuration de STP BPDUGUARD.

Sur notre réseau nous voyons que a l'arrivé d'un pirate, son but est de forcé le switch au il a connecté son pc d'être la root-bridge par donner la plus petite priority à ce switch, afin que toutes les communications du réseau passe par lui, donc l'altération et la modification des informations sur le réseau est une faille de sécurité.

Pour empêcher ce pirate de ne pas avoir accès, nous faisons cette configuration :

```
Switch1-Acces(config)#in range Fa0/5-24
Switch1-Acces(config-if-range)#spanning-tree bpduguard enable
Switch1-Acces(config-if-range)#%SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port
FastEthernet0/5 with BPDU Guard enabled. Disabling port.

%PM-4-ERR_DISABLE: bpduguard error detected on 0/5, putting 0/5 in err-disable state


%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down

Switch1-Acces(config-if-range)#
```

Figure III.70 : Configuration du STP BPDUGUARD.

Apres avoir mettre la configuration du STP BPDUGUARD nous voyons que le pirate ne peut pas avoir accès tant que les ports non utiliser sur le réseau sont bloquées par la configuration précédente :

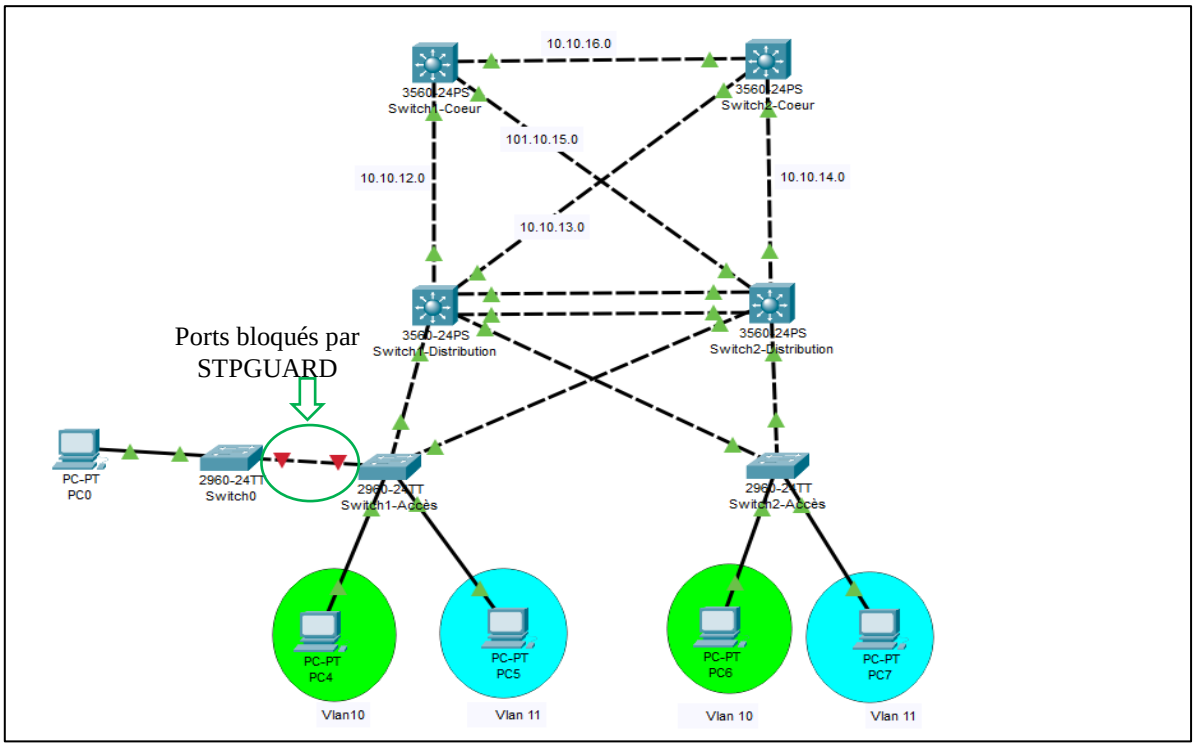


Figure III.71 : L'architecture réseau avant la configuration de STP GUARD.

- **Sécurisation de port :** sur un réseau d'entreprise par exemple, une personne mal-attentionner pourrait très bien se connecter sur un des ports non utilises du switch et accéder au réseau !

Alors pour sécuriser les ports des commutateurs de notre réseau, nous passons par ces étapes :

- **Etape01 :** dans cette étape nous désactivons tous les ports, qui ne sont pas utilisés, pour faire nous mettons cette configuration :

```
Switch2-Acces(config)#int range Fa0/5-24
Switch2-Acces(config-if-range)# shutdown

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down
```

Figure III.72 : Désactivation des ports.

Pour ajouter en plus, un niveau de sécurité en plaçant tous les interfaces désactiver dans un VLAN qui n'est pas utilisé :

```
Switch2-Acces(config)#int range Fa0/5-24
Switch2-Acces(config-if-range)#switchport access vlan 45
Switch2-Acces(config-if-range)#
```

Figure III.73 : Placement des interfaces désactivés dans un vlan non utilisé.

Nous faisons un «show-running config », nous voyons bien que nos interfaces sont désactivées :

```
!
interface FastEthernet0/5
 switchport access vlan 45
 spanning-tree bpduguard enable
 shutdown
!
interface FastEthernet0/6
 switchport access vlan 45
 spanning-tree bpduguard enable
 shutdown
!
```

Figure III.74 : Montrer les interfaces désactivées.

- **<u>Etape 02 :</u>** maintenant nous configurons le « port-Security », en limitants l'accès à certaines adresses MAC. Nous faisons cette limitation avec le mode « sticky ».

```
Switch1-Acces(config)#int Fa0/1
Switch1-Acces(config-if)#switchport mode access
Switch1-Acces(config-if)#switchport port-security
Switch1-Acces(config-if)#switchport port-security maximum 1
Switch1-Acces(config-if)#switchport mac-address sticky
                                   ^
% Invalid input detected at '^' marker.

Switch1-Acces(config-if)#switchport port-security mac-address sticky
Switch1-Acces(config-if)#switchport port-security violation shutdown
Switch1-Acces(config-if)#
```

Figure III.75 : La configuration de port-Security.

Ici nous avons autorisé qu'une seule adresse MAC qui peut se connecter sur le port Fa0/1 avec la commande « switchport port-security maximum 1 », et aucunes autres adresses ne pourra se connecter sur ce port sauf la première adresse prés avec «switchport port-security mac-address sticky ». Pour terminer la configuration, nous avons choisi le mode violation « switchport port-security violation shutdown », qui désactivera l'interface dès qu'une violation de sécurité interviendra.

Maintenant que nous avons bien configuré la sécurité sur le port 1 du switch, nous allons vérifier son fonctionnement avec la commande « show port security interface FastEthernet 0/1 » :

```
Switch1-Acces#show port-security interface fastEthernet 0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000A.F3D4.86A4:10
Security Violation Count   : 0
```

Figure III.76 : Vérification le fonctionnement de la configuration.

Nous effectuons cette configuration sur le deuxième port de ce Switch, et les configurations précédentes (sécurisation de port) sur le deuxième switch (Switch2-Accès) de la couche Accès.

- **DHCP snooping :** nous configurons le DHCP snooping sur les commutateurs de la couche Accès, pour écouter le trafic DHCP et arrêter tous les paquets malveillants qui se font passer le DHCP, pour faire nous mettons cette configuration :

```
Switch2-Acces(config)#ip dhcp snooping
Switch2-Acces(config)#no ip dhcp snooping information option
Switch2-Acces(config)#ip dhcp vlan 10
                             ^
% Invalid input detected at '^' marker.

Switch2-Acces(config)#ip dhcp snooping vlan 10
Switch2-Acces(config)#int range Fa0/3-4
Switch2-Acces(config-if-range)#ip dhcp snooping trust
Switch2-Acces(config-if-range)#exit
Switch2-Acces(config)#int Fa0/1
Switch2-Acces(config-if)#ip dhcp snooping limit rate 10
```

Figure III.77 : Configuration du DHCP Snooping.

Pour vérifier la configuration de surveillance avec la commande « show ip dhcp snooping » :

```
Switch2-Acces#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
Insertion of option 82 is disabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/3            yes        unlimited
FastEthernet0/1            no         10
FastEthernet0/4            yes        unlimited
Switch2-Acces#
```

Figure III.78 : Vérification de la configuration d DHCP Snooping.

La commande suivante « show ip dhcp snooping binding », permet d'assurer le suive de l'adresse MAC avec les adresses IP.

```
Switch2-Acces#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ------------------
00:01:42:12:5A:59   10.10.10.129     0           dhcp-snooping  10    FastEthernet0/1
00:30:A3:09:D6:06   10.10.11.129     0           dhcp-snooping  11    FastEthernet0/2
Total number of bindings: 2
Switch2-Acces#
```

Figure III.79 : Afficher les clients DHCP avec leurs adresses.

Donc nous voyons ici que les deux clients légitimes ont bien reçu les adresses IP du vrai serveur DHCP.

Conclusion

Pour conclure notre projet, nous avons d'abord mis en place le réseau local fourni par l'entreprise Cevital à l'aide du logiciel de simulation « Cisco Paket Tracer », que nous avons par la suite utilisé pour la configuration de notre architecture. Nous avons donc configuré entièrement le réseau pour qu'il fonctionne correctement puis nous avons sécurisé le réseau en appliquant certains protocoles de sécurité. Nous avons également testé et validé notre conception et réalisation, et sur la base des captures d'écran que nous avons fait nous avons clairement pu voir que notre théorie et nos besoin correspondaient très bien à ce que nous avons réalisés de ce fait nous validons notre configuration.

Conclusion Générale

Le travail présenté dans ce mémoire consiste à proposer une configuration pour un réseau local de l'entreprise Cevital dont le but est d'améliore une sécurité de celui-ci. Cette configuration inclut la protection de tous les équipements d'interconnexions qui composent le réseau.

Pour mener à bien notre projet on l'a devisé en deux parties :

- ✓ l'approche théorique qui est devisé en deux chapitres, le premier porte sur les généralités des réseaux informatiques où on a donné un aperçue de ces concepts de base et la classification des réseaux informatiques, les dispositifs d'interconnexion, les supports de transmission outre le model de communication, leurs adressages et certains protocoles réseau. Par la suite on a passé au deuxième chapitre où on a présenté des généralités sur la sécurité d'un réseau informatique, qu'on a défini, montrer ces objectifs et les domaines de l'application, suivi des protocoles pour se défendre contre les attaques et les menaces.
- ✓ La deuxième approche elle-même est devisée en deux sous parties, la première consiste à présenter l'organisation de l'entreprise où on fait le stage, la deuxième qui est la dernière partie est dédiée la réalisation du projet, on simule l'architecture proposée via le logiciel « Cisco Packet Tracer », puis tous les équipements sont entièrement configurés pour faire fonctionner le réseau, et enfin on a appliqué des protocoles pour sécuriser également le réseau.

Ce travail nous a permet d'acquérir, d'enrichir et d'approfondir nos connaissances et nos compétences dans de nombreux domaines, ainsi il nous a fait découvrir le monde de la recherche sur les réseaux, notamment leur sécurisation.

Références Bibliographiques

[1] Michèle Germain, Introduction aux réseaux, Livre blanc Forum ATENA.

[2] Haimoudi El Khatir, cours Informatique, filière SEG, Semestre S3, https://docplayer.fr/8089535-Cours-informatique-filiere-seg-semestre-s3-professeur-haimoudi-el-khatir-page-1.html, dernier accès Avril 2022.

[3] Guy Pujolle, Les réseaux, 8eme édition, Eyrolles Paris, 2014.

[4] Patrick Hautrive, La théorie des réseaux locaux et étendus, Publié le 7 octobre 2006 - Mis à jour le 18 avril 2020. https://hautrive.developpez.com/reseaux/?page=les-types-d-organisation-des-reseaux, dernier accès Mai 2022.

[5] https://www.commentcamarche.net/contents/512-topologie-des-reseaux, Dernière modification le vendredi 2 juin 2017 à 15:45 par smarques, dernier accès Mai 2022.

[6] https://www.samomoi.com/reseauxinformatiques/les_topologies_des_reseaux.php, dernier accès Mai 2022.

[7] Jean-Pierre ARNAUD, Réseaux & télécoms, Dunod, 4e édition, ISBN 978-2-10-059259-3.

[8] Vince, Les réseaux de zéro, Zeste de savoir, Le 08 février 2022.

[9] Stéphane Lohier et Dominique Présent, Réseaux et transmissions (Protocoles, infrastructures et services), Dunod, 7e édition, ISBN 978-2-10-081183-0.

[10] Danièle DROMARD et Dominique SERET, Architecture des réseaux, Pearson Education France, Paris, 2e édition, ISBN 978-2-7440-7480-6.

[11] Stéphane Lohier, Dominique Présent, Réseaux et transmission (protocoles, infrastructures et services), Dunod, 6e édition, ISBN 978-2-10-074475-6.

[12] Pierre Jaquet, Les réseaux informatiques, http://www.jaquet.org, mai 2015.

[13] Jean-François Pillou, Tout sur les Réseaux et Internet, Dunod, 4e édition, ISBN 978-2-10-072229-7.

[14] Stéphane Lohier et Dominique Présent et Guy Pujolle, Transmissions et Réseaux, Dunod, 3e édition, ISBN 2 10 007221 8.

[15] José DORDOIGNE, Réseaux informatiques Notions fondamentales (Protocoles, Architecture, Réseaux sans fil, Virtualisation, Sécurité, IP v6…), ENI, 6e édition, ISBN 978-2-7460-9392-8.

[16] Aurélien ROUX, Cisco configurer routeurs et commutateurs, ENI, 4e édition, ISBN 978-2-7460-8855-9.

[17] Romain LEGRAND et André VAUCAMPS, Cisco Notions de base sur les réseaux, ENI, Nouvelle Edition, ISBN 978-7460-9213-6.

[18] Elie MABO, La sécurité des systèmes informatiques (Théorie), support de cours, 2010, consulté le 18/05/22.

[19] Dr. YENDE RAPHAEL Grevisse, Support de cours de Sécurité Informatique & Crypto. PhD, Docteur en Télécoms et Réseaux Inf. Master. Congo-Kinshasa 2018. ffcel-01965300f. (https://hal.archives-ouvertes.fr/cel-01965300).

[20] Solange Ghernaouti, Sécurité informatique et réseaux, Dunod, 4e édition, ISBN 978-2-10-059912-7.

Références Bibliographiques

[21] https://web.maths.unsw.edu.au/~lafaye/CCM/attaques/attaques.htm, consulté le 27/04.2022.

[22] Mme Labraoui N, Sécurité Informatique, Master 1 Réseaux et systèmes distribués 2019-2020, Université Abou Bakr Belkaid, dernier accès Avril 2022.

[23] José DORDOIGNE, Réseaux informatiques, Notions fondamentales (protocoles, architectures, Réseaux sans fils, virtualisation, Sécurité, IP v6, …), Edition ENI, Février 2011, 4e édition, ISBN : 978-2-7460-6145-3, ISSN : 1627-8224.

[24] https://cisco.goffinet.org/ccna/vlans/concepts-vlan-cisco/#15-d%C3%A9finition, Dernier accès Mai 2022.

[25] ANSSI, Recommandations pour la sécurisation d'un commutateur de desserte, Paris, le 24 juin 2016. (https://www.ssi.gouv.fr/uploads/2016/07/nt_commutateurs.pdf).

[26] https://www.connecthostproject.com/vtp.html , dernier accès juin 2022.

[27] Cisco, https://www.cisco.com/c/fr_fr/products/security/firewalls/what-is-a-firewall.html, Dernier accès Mai 2022.

[28] DI GALLO Frédéric, COURS DE RESEAUX ET SYSTEMES, Cycle Probatoire, CNAM BORDEAUX, dernier accès Mai 2022.

[29] https://cisco.goffinet.org/ccna/filtrage/concept-ids-ips/ , derniers accès Juin 2022.

[30] Plate-forme de cours sur l'administration systèmes et réseau pour les professionnels de l'informatique, https://www.it-connect.fr/informatique-cest-quoi-une-dmz/, dernier accès Mai 2022.

[31] Jean-PAUL ARCHIER, Les VPN (Fonctionnement, mise en œuvre et maintenance des Réseaux Privées Virtuel), Edition ENI, ISBN 978-2-7460-5522-3.

[32] Laurent Bloch & Christophe Wolfhugel, Sécurité informatique (Principes et méthode a l'usage des DSI, RSSI et administrateurs, EYROLLES, 2e édition, ISBN 978-2-212-12525-2.

[33] GUY PUJOLLE, LES RESEAUX, EYROLLES, 9e édition, ISBN 978-2-212-67535-1.

[34] Pierre CABANTOUS, Les réseaux informatiques (guide pratique pour l'administration et la supervision), Edition ENI, ISBN 978-2-409-01920-3.

[35] https://cisco.goffinet.org/ccna/ethernet/switchport-port-security-cisco-ios/, dernier accès Juin 2022.

[36] https://www.cisco.com/c/en/us/tech/lan-switching/spanning-tree-protocol/index.html, dernier accès Juin 2022.

[37] https://docs.ruckuswireless.com/fastiron/08.0.60/fastiron-08060-l2guide/GUID-8BA224A2-0D22-4638-B8A3-D09CBCE2EC36.html, dernier accès Juin 2022.

[38] Laurent SCHALKWIJK et André VAUCAMPS, CISCO routage et commutation, Edition ENI, ISNB 978-7460-9785-8.

Résumé

La sécurité des réseaux est une priorité absolue pour les entreprises. Sans une sécurité adéquate, les données d'une entreprise peuvent être compromises, avec des conséquences potentiellement catastrophiques. Aujourd'hui, de nombreuses entreprises sont victimes de plusieurs attaques et piratées en raison d'un manque de sécurité. Pour se protéger de ces attaques, les administrateurs réseau doivent mettre en place des stratégies et des mécanismes de sécurité plus solides dans leurs réseaux. Dans notre travail, nous avons intéressés par une proposition d'une configuration sécurisée basée sur le regroupement des VLANs, la sécurisation des ports (port-Security), ainsi protéger le domaine STP et empêcher les serveurs DHCP indésirables de se connecter sur notre réseau afin de pouvoir maximiser la protection du réseau de l'entreprise Cevital contre les menaces et les attaques possibles de l'atteindre.

Mots clés:

VLANs, Port-Security, STP, DHCP.

Abstract

Network security is a top priority for businesses. Without adequate security, a company's data can be compromised, with potentially catastrophic consequences. Many businesses today are the victims of multiple attacks and hacks due to a lack of security. To protect against these attacks, network administrators need to implement stronger security strategies and mechanisms in their networks. In our work, we are interested in a proposal for a secure configuration based on the grouping of VLANs, securing ports, thus protecting the STP domain and preventing unwanted DHCP servers from connecting to our network in order to be able to maximize protection. Of the Cevital company network against threats and possible attacks to reach it.

Keywords:

VLANs, Port-Security, STP, DHCP.