Université Abderrahmane MIRA de Béjaïa

Faculté Des Sciences Exactes

Département Informatique

Memoire de fin de cycle

En vue de l'obtention du diplôme Master professionnel en informatique

Option : Administration et Sécurité des Réseaux

Sous le thème

Etude et mise en place des réseaux locaux virtuels

Cas d'étude : Entreprise Portuaire de Béjaia

Réalisé par :

M^lle^ *BOUIMEDJ Lynda*

Encadrée par :

M^me^ *ADEL Karima*

Devant le jury composé de :

Président : Mr SBAA.A

Examinatrice :* M^me^ *METIDJI.R

Examinateur : Mr KDJOUH.N

Promotion : 2016/2017

Remerciements

C’est avec joie que je rends ce travail si passionnant et épuisant.

Je remercie tout d'abord Dieu le tout puissant de m'avoir donné le courage, la force et la patience d'achever ce modeste travail.

Mes remerciements les plus sincères s’adressent aux personnes qui m'ont apporté leur aide et qui ont contribué à l'élaboration de ce travail ainsi qu'à la réussite de cette formidable année académique.

Je tiens à remercier grandement mon encadrante Madame ADEL Karima et Monsieur TOUATI Baderddine, qui, entant que mon encadrant au sein de l’entreprise portuaire de Béjaia s'est toujours montré à l'écoute et très disponible tout au long de la réalisation de ce travail malgré ses charges professionnelles.

Je remercie tout particulièrement mon cher futur mari pour l'inspiration, l'aide et le temps qu'il a bien voulu me consacrer et sans qui ce mémoire n'aurait jamais vu le jour.

Les mots me manquent pour exprimer ma profonde reconnaissance à ma tendre famille dont l'amour, la patience et le sacrifice s'inscrivent à chaque page de ce document.

Dédicaces

Je dédie ce mémoire à :

· Mes parents :

Ma mère, qui a œuvré pour ma réussite, de par son amour, son soutien, et tous les sacrifices consentis, pour toute son assistance et sa présence dans ma vie, reçois à travers ce travail aussi modeste soit-il, l'expression de mes sentiments et de mon éternelle gratitude.

Mon père, qui peut être fier et trouver ici le résultat de longues années de sacrifices et de privations pour m'aider à avancer dans la vie. Merci pour les valeurs nobles, l'éducation et le soutient permanent venu de toi.

· Mes sœurs et mon frère :

Ma grande et chère sœur Rym et son époux Yassine à qui je souhaite tout le bonheur du monde

Mes douces et petites sœurs Saby et Mina

Mon frère Wafi à qui je souhaite de la réussite dans ses études et sa carrière sportive.

· Mon oncle, ma tante, mes cousines et mon cousin :

Tonton Moho et Tata Dida qui m'ont toujours accueillie dans leur chaleureuse maison

Mes cousines adorées Kenza et Mira, les plus belles cousines du monde

Mon cousin Mohande en qui je vois beaucoup d'enthousiasme que j'espère te guidera vers beaucoup de succès.

·Mes défuntes grand-mères :

Imma et setti, des grand-mères qui ont fait preuve d'une immense générosité avant de quitter ce bas monde.

Dédicaces spéciale :

Ilyes mon homme, mon pote, mon tout

Sony mon amie, ma sœur, ma meilleure.

Table des matières

Table des figures

Table des figures

La liste des abréviations

A

ACL : Access Control List (liste de contrôle d'accès)

C

CLI: Commande Langage Interface

D

DC1: Direct Connect Interface

DZM: Zone démilitarisée

DDOS : Distributed Denial Of Service attack *(*attaque par déni de service)

DHCP: Dynamic Host Configuration Protocol (protocole de configuration dynamique des hôtes)

F

FDDI: Fiber Distributed Data Interface

I

IDS: Intrusion Detection System

ISO: Organisation internationale de normalisation

IPX: Internetwork Packet Exchange

IEEE: Institute of Electrical and Electronic Engineers

IP: Internet Protocol

L

LAN: Local Area Network

LLC: Logical Link Contro (Contrôle de la liaison logique)

Liste des abréviations

M

MAC: Media Access Control

O

OSI: Open Systems Interconnection

P

PHP: Hypertext Preprocessor

PC: Personal Computer

S

STP: Spanning Tree Protocol

T

TPID: Tag protocol identifier

TCP: Transmission Control Protocol

V

VLAN: Virtual Protocol Area Network

VPN: Virtual Private Network

VTP: VLAN Trunking Protocol

VMPS: VLAN Membership Policy Servee

VACL: VLAN access control list

Introduction Générale

L'apparition de l'informatique dans tous les secteurs d'activité a permis de rendre facile bon nombre de tâches. La plupart des entreprises aujourd'hui sont informatisées, et il est impensable, à notre époque, de ne pas disposer de cet outil pour les gérer. La performance du système d'information d'une entreprise est d'une importance capitale pour son efficacité et son bon fonctionnement.
Le réseau informatique permet aux entreprises de centraliser leurs données, de travailler en équipe de manière productive et de limiter l'utilisation du papier (impression, déplacement) afin de faciliter le transfert d'informations. Chose qui est devenue de plus en plus nécessaire, voire même primordiale pour les entreprises.

De nos jours l'Algérie suit ces tendances technologiques contemporaines, les entreprises disposent d'un système d'information centralisé, chacune a son propre réseau informatique. C'est dans cette optique que l'EPB (Entreprise Portuaire de Béjaia) s'en est elle aussi conçue un. Ce système lui permet aujourd'hui d'accomplir plus efficacement ses missions. Généralement, un réseau local (LAN) est défini par un domaine de diffusion, c'est-à-dire toutes les stations d'un réseau local reçoivent les messages de diffusion émis par n'importe quelle autre station de ce réseau. Plus l'entreprise prend de l'amplitude (nombre de stations) plus elle fait face à des contraintes causant une réduction de performance telle que l'augmentation du trafic du réseau et l'affaiblissement de la sécurité des données.

Nous avons axé notre travail sur la limitation de l'étendue de chaque domaine de diffusion sur le réseau local grâce à la segmentation VLAN qui permet d'améliorer les performances et la sécurité sur le réseau, qui est l'objectif de cette étude.

L'objectif de notre mémoire de fin d'études est l'amélioration de la sécurité et des performances du réseau contre les surcharges rencontrées par les utilisateurs de l'EPB avec l'implémentation d'une solution basée sur les VLANs (Virtual Local Area Network). Pour cela nous allons organiser l'ensemble des utilisateurs dans des réseaux virtuels en procédant à la segmentation logique du réseau en mettant bien sûr en évidence l'aspect sécuritaire de l'opération par le choix de la bonne segmentation logique, de la bonne configuration et des outils utilisés.

Introduction générale

Dans notre développement nous allons présenter tout d'abord la structure qui nous a accueillis, à savoir l'EPB. Ensuite nous allons faire une étude technique qui va nous permettre de critiquer objectivement le réseau local de l'entreprise et d'apporter les solutions adéquates aux différentes insuffisances descellées. Puis, dans le second chapitre nous allons présenter les concepts fondamentaux ainsi que le fonctionnement des réseaux locaux, et nous allons parler de l'impacte de la sécurité informatique sur les réseaux en exposant les objectifs ainsi que les stratégies de sécurité. Dans le troisième chapitre, nous allons focaliser notre attention sur les concepts de base des réseaux virtuels, nous allons mettre en outre l'accent sur la norme 802.1Q ainsi que les protocoles utilisés pour la configuration et l'administration des VLANs. Dans le quatrième et dernier chapitre, nous allons organiser l'ensemble du personnel de l'entreprise dans des réseaux virtuels en procédant à la segmentation logique du réseau intranet, c'est-a-dire l'implémentation de notre solution.

CHAPITRE 1 : PRESENTATION DE L'ORGANISME D'ACCUEIL

1.1 Introduction

Ce chapitre sera réservé à l'étude du réseau existant dans l'EPB et aux améliorations proposées. En première étape, nous allons évoquer un bref aperçu de l'entreprise pour connaitre son historique de création, son rôle par rapport aux autres entreprises portuaires nationales, sa situation graphique, sa structure, ses missions et activités, sa direction informatique et ses objectifs. Ensuite, nous allons étudier le réseau informatique mis en place dans cette entreprise et ses composants afin de pouvoir proposer d'éventuelles améliorations.

1.2 Présentation générale de l'organisme d'accueil

Le port de Bejaia joue un rôle très important dans les transactions internationales vu sa place et sa position géographique.
Aujourd'hui, il est classé 2ème port d'Algérie en marchandises générales et 3ème port pétrolier. Il est également le 1er port du bassin méditerranéen certifié ISO 9001.2000 pour l'ensemble de ses prestations, et à avoir ainsi installé un système de management de la qualité. Cela constitue une étape dans le processus d'amélioration continue de ses prestations au grand bénéfice de ses clients. L'Entreprise Portuaire a connu d'autres succès depuis, elle est notamment certifiée à la Norme ISO 14001 :2004 et au référentiel OHSAS 18001 :2007, respectivement pour l'environnement et l'hygiène et sécurité au travail.

1.3 Historique

Bejaia, une ville, un port,

Au cœur de l'espace méditerranéen, la ville de Bejaia possède de nombreux sites naturels et vestiges historiques datant de plus de 10 000 ans, ainsi que de nombreux sites archéologiques recelant des objets d'origine remontant à l'époque néolithique.
Bejaia joua un grand rôle dans la transmission du savoir dans le bassin méditerranéen, grâce au dynamisme de son port, la sécurité de la région, la bonne politique et les avantages douaniers. Bougie a su attirer beaucoup de puissants marchands.

La *Saldae* romaine devient un port d'embarquement de blé du grenier de Rome, ce n'est qu'aux *XIéme* siècle, que *Bgaieth*, devenue *Ennaceria*, pris une place très importante dans le monde de l'époque ; le port de Bejaia devient l'un des plus importants de la méditerranée.
La réalisation des ouvrages actuels débuta en 1834, elle fut achevée en 1987. C'est en 1960 qu'a été chargé le premier pétrolier d'Algérie.

1.4 Création de l'EPB

Le décret n°82-285 du 14 Août 1982 publié dans le journal officiel n° 33 porta création de l'Entreprise Portuaire de *Béjaïa* ; entreprise socialiste à caractère économique ; conformément aux principes de la charte de l'organisation des entreprises, aux dispositions de l'ordonnance n° 71-74 du 16 Novembre 1971 relative à la gestion socialiste des entreprises et les textes pris pour son application à l'endroit des ports maritimes.
L'entreprise, réputée commerçante dans ses relations avec les tiers, fut régie par la législation en vigueur et soumise aux règles édictées par le sus mentionné décret.
Pour accomplir ses missions, l'entreprise est substituée à l'Office National des Ports (ONP), à la Société Nationale de Manutention (SO.NA.MA) et pour partie à la Compagnie Nationale Algérienne de Navigation (CNAN).
Elle fut dotée par l'Etat, du patrimoine, des activités, des structures et des moyens détenus par l'ONP, la SO.NA.MA et de l'activité Remorquage, précédemment dévolue à la CNAN, ainsi que des personnels liés à la gestion et au fonctionnement de celles-ci.
En exécution des lois n° 88.01, 88.03 et 88.04 du 02 Janvier 1988 s'inscrivant dans le cadre des réformes économiques et portant sur l'autonomie des entreprises, et suivant les prescriptions des décrets n°88.101 du 16 Mai 1988, n°88.199 du 21 Juin 1988 et n°88.177 du 28 Septembre 1988.
L'Entreprise Portuaire de *Béjaïa* ; entreprise socialiste ; est transformée en Entreprise Publique Economique, Société par Actions (EPE-SPA) depuis le 15 Février 1989, son capital social fut fixé à Dix millions (10.000.000) de dinars algériens par décision du conseil de la planification n°191/SP/DP du 09 Novembre 1988. Actuellement, le capital social de l'entreprise a été ramené à 1.700.000.000 Da, détenues à 100% par la Société de Gestion des Participations de l'Etat «Ports », par abréviation « SOGEPORTS ».

1.5 Situation graphique

Le port de *Béjaïa*, est délimité par :

- Au nord par la route nationale N°9.
- Au sud par les jetées de fermeture et du large sur une largeur de 2 750m.
- A l'est par la jetée Est.
- A l'ouest par la zone industrielle de Bejaia

1.6 Missions et activités de l'EPB

➢ Ses Missions

La gestion, l'exploitation et le développement du domaine portuaire sont les charges essentielles de la gestion de l'EPB, c'est dans le but de promouvoir les échanges extérieurs du pays. Elle se doit d'assumer la police et la sécurité au sein du pays.

Elle est chargée des travaux d'entretien, d'aménagement, de renouvellement et de création d'infrastructures.

L'EPB assure également des prestations à caractère commercial, à savoir ; le remorquage, la manutention et l'acconage.

➢ Ses Activités

Les principales activités de l'entreprise sont :

- L'exploitation de l'outillage et des installations portuaires.

- L'exécution des travaux d'entretien, d'aménagement et de renouvellement de la super structure portuaire.

- L'exercice du monopole des opérations d'acconage et de manutention portuaire.

- L'exercice du monopole des opérations de remorquage, de pilotage et d'amarrage.

- La police et la sécurité portuaire dans la limite géographique du domaine public portuaire.

1.7 Présentations des différentes structures de l'EPB

L'EPB est organisée selon des directions fonctionnelles et opérationnelles dirigées par une Direction Générale qui est chargée de concevoir, coordonner et contrôler les actions liées à la gestion et au développement de l'entreprise (voir figure 1.1).

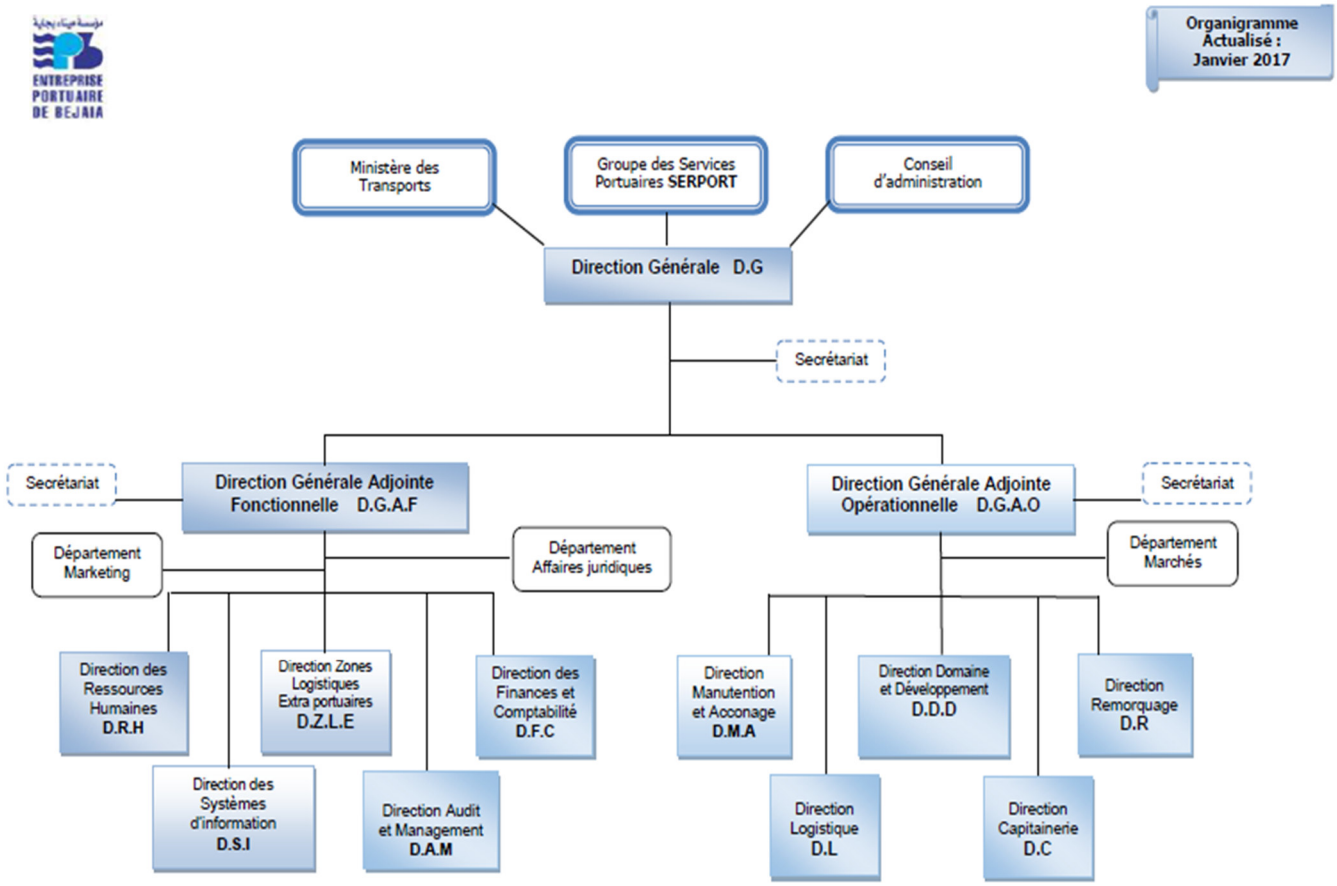


Figure 1.1. *Organigramme général de l'EPB*

1.8 Présentation de la direction informatique :

La structure informatique de l'EPB est un département rattaché à la direction générale adjointe ; il a été créé en 1989 et c'est à cette époque que les premières applications de l'entreprise ont vu le jour.

En 1995 la micro-informatique a été introduite à l'EPB et les premières applications sont écrites sous DBASE 5. A partir de 2001 l'entreprise portuaire a lancé un plan pour développer les applications métiers sous PHP et DELPHI 5 et comme système de gestion de bases de données MYSQL.

1.8.1 Les missions de la direction informatique :

- L'informatique a pour mission l'automatisation des métiers de l'Entreprise Portuaire de Bejaia, et cela en mettant en place les logiciels et l'infrastructure nécessaires pour la gestion du système d'information.
- L'EPB déploie des systèmes d'informations pour accroitre la productivité, automatiser les processus métiers et fournir un meilleur service aux clients. Ces systèmes intègrent de plus en plus des fonctionnalités réseau pour relier tous les utilisateurs à l'entreprise ou établir des liens avec la clientèle et les fournisseurs.
- Le réseau apporte aujourd'hui une réelle valeur ajoutée en permettant d'intégrer de nouveaux partenaires, fournisseurs et clients.

1.8.2 Organisation humaine de la direction informatique :

La figure 1.2 représente l'organisation humaine du département informatique.

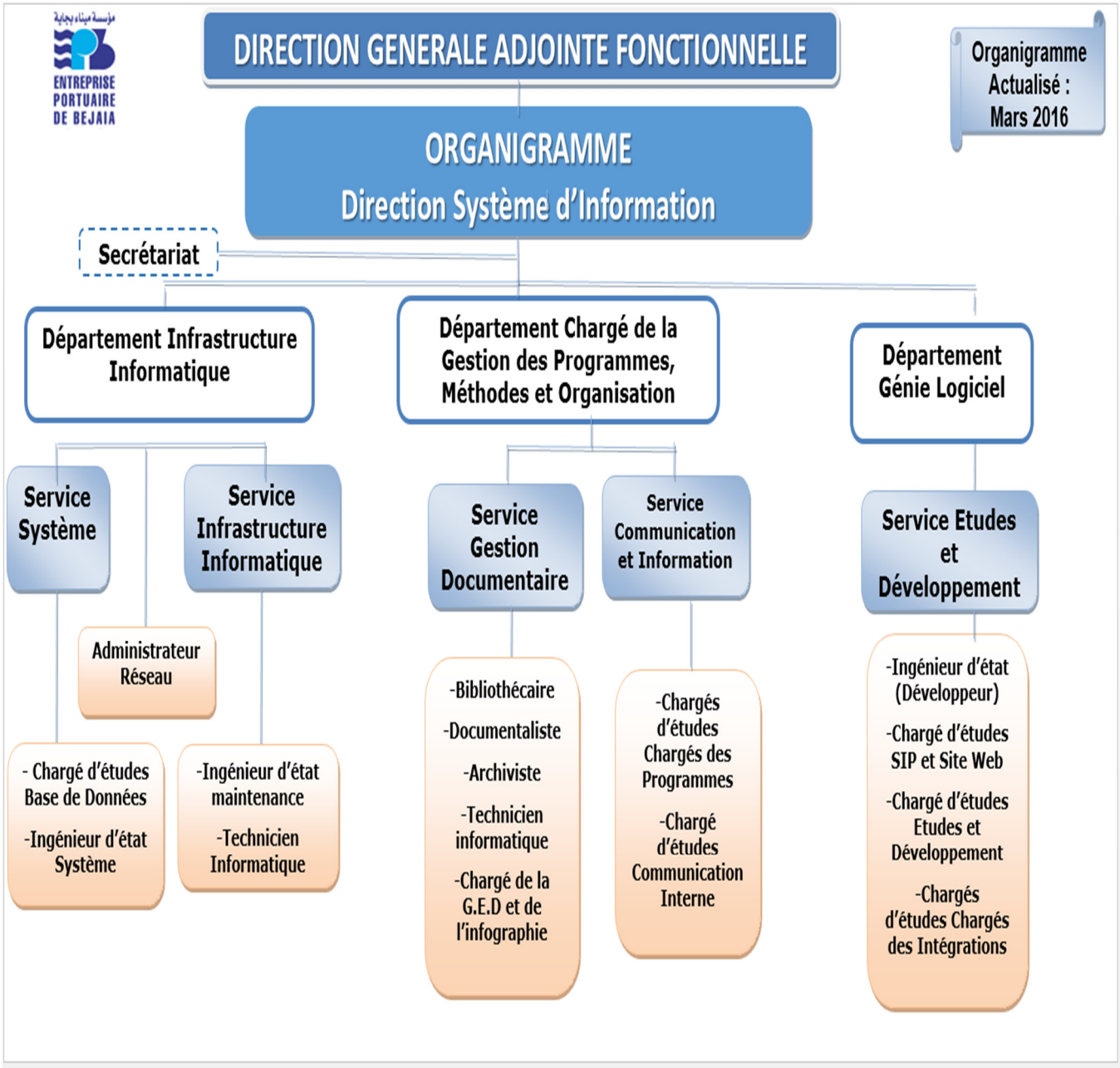


***Figure 1.2**. L'organigramme de la structure informatique*

1.8.3 L'infrastructure informatique

Le réseau informatique de l'EPB :

Le réseau du port de Bejaia s'étend du port pétrolier (n°16) aux ports 13 et 16 (port à bois). La salle machine du réseau local de l'EPB contient principalement une armoire de brassage et une autre armoire optique de grande taille, éventuellement l'ensemble des serveurs, ces deux armoires servent à relier les différents sites de l'entreprise avec le département informatique par des fibres optiques de type 4, 6, 8 et 12 brins. Chaque site a une armoire de brassage contenant un ou plusieurs convertisseur(s) media, un ou plusieurs Switch où sont reliés les différents équipements par des câbles informatiques.

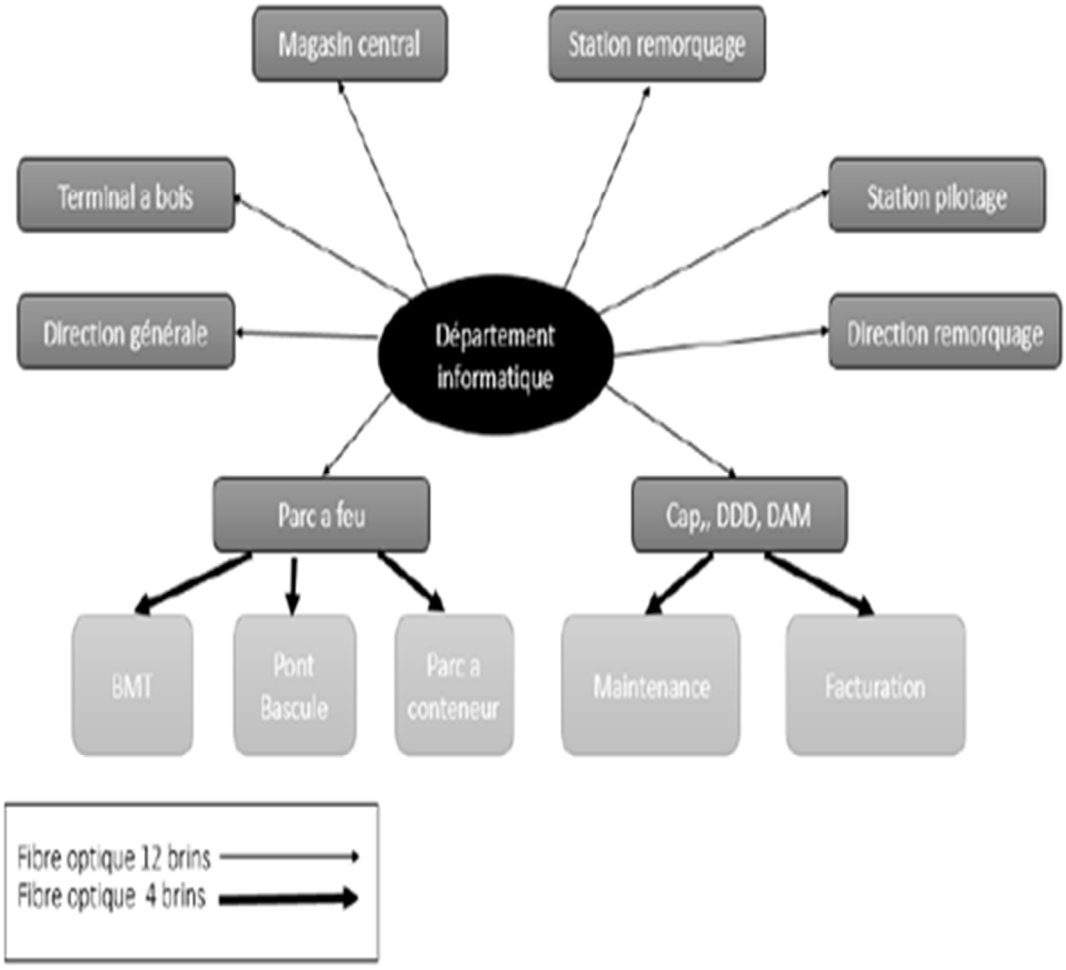


Figure 1.3. *Réseau fibre optique de l'EPB*

1.8.4 Présentation de l'architecture réseau de l'EPB :

Dans cette partie nous allons décrire les différents composants de l'architecture réseau de l'EPB (figure 1. 4)

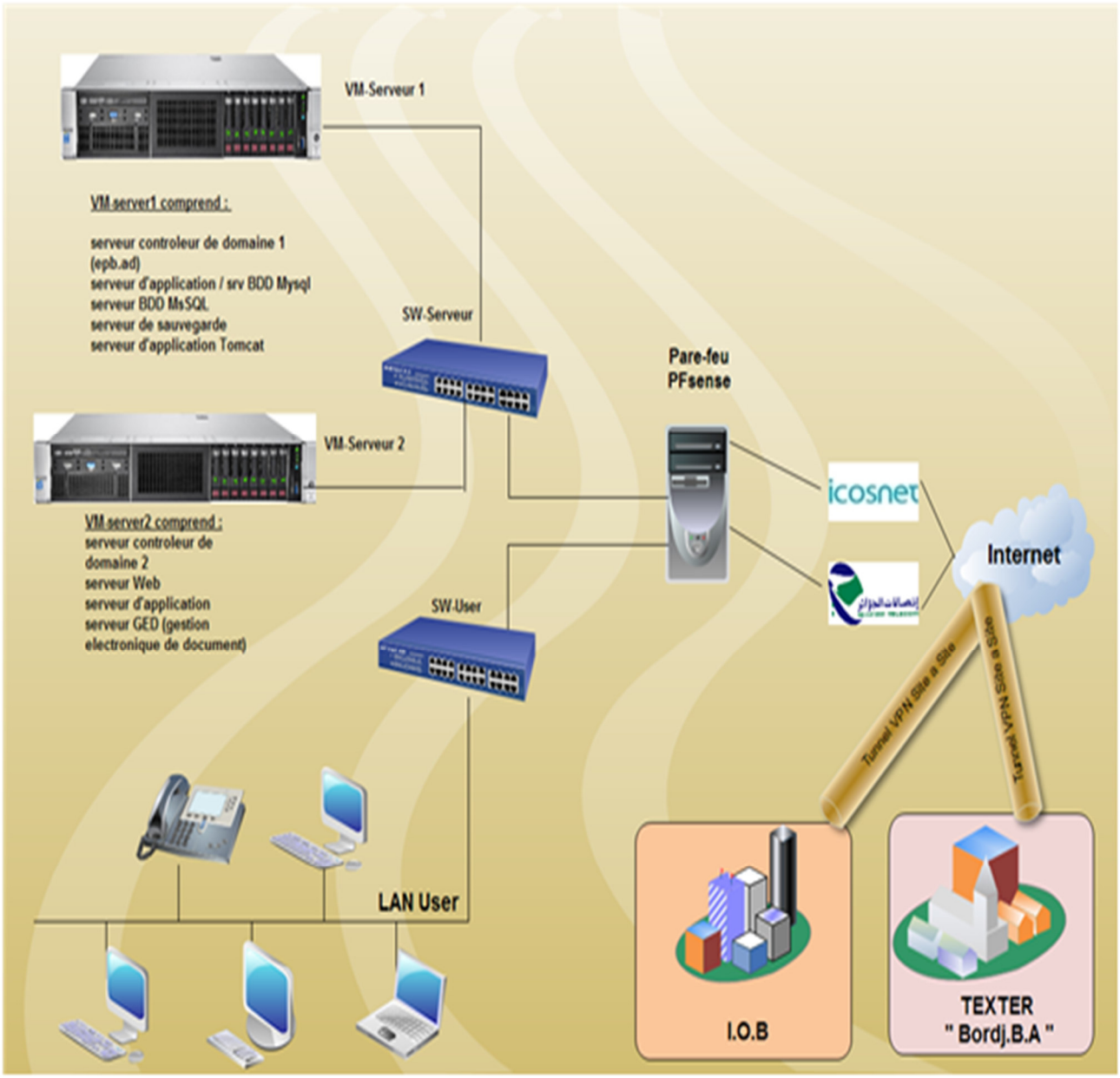


Figure 1.4. *Architecture réseau de l'EPB*

a) Etude de l'architecture :

➢ **Connexion Internet :**

L'entreprise portuaire de Bejaia s'est dotée de deux connexions *Wimax* à savoir *icosnet* et Algérie télécom. Ce type de connexions permet de se connecter à Internet haut débit grâce à une antenne *outdoor* qui communique par des ondes hertziennes via une station de base située au mont *Gouraya*, d'une très grande fiabilité permettant ainsi d'éviter l'usage du câble et le risque d'une panne physique par conséquent.

➢ **Sécurité :**

La sécurité est assurée par un pare-feu pour appliquer les stratégies d'accès et les règles de routages déterminant la manière dont les clients accèdent à Internet.

➢ **Salle machine** :

La salle machine est le cœur du réseau toutes les activités du port reposent sur cette salle, elle regroupe en un seul endroit les ressources nécessaires au bon fonctionnement du LAN, en plus des *Switchs* elle comporte les différentes machines serveurs :

- **Serveur de base de données (SQL server 2008 and My SQL**) :

Un serveur de base de données répond à des demandes de manipulation de données stockées dans une ou plusieurs bases de données. Il s'agit de demande de recherche, de tri, d'ajout, de modification ou de suppression de données. Ces données sont utilisées par des serveurs web et des utilisateurs.

- **Serveur de contrôleur de domaine DC1 (Active Directory)** :

Sous Windows Server 2012 R2 l'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateur utilisant le système Windows. Il répertorie les éléments de ce réseau administré tel que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc.

- **Serveur de contrôleur de domaine redondant DC2 (Active Directory) :**

Il permet de conserver des réplicas de données de l'annuaire sur un autre contrôleur de domaine, cela garantie la disponibilité et la continuité.

- **Serveur application/fichier :**

C'est un serveur sur lequel sont installées les applications utilisées par les usagers. Ces applications sont chargées sur le serveur d'application pour y accéder à distance. Un serveur d'application peut être un serveur qui centralise toutes les applications utilisées par les postes clients.

- **Serveur de sauvegarde :**

Il a pour rôle de sauvegarder en continue les données générées par l'entreprise. Si un employé efface par erreur un document, ou qu'il y a un dysfonctionnement d'un ordinateur, le serveur est en mesure de récupérer le fichier perdu.

b) Diagnostique de l'architecture de l'EPB :

L'étude que nous avons menée sur l'architecture nous a permis de retirer des faiblesses réseaux et qui sont les suivantes :

- **Absence de serveurs en redondances pour assurer la tolérance aux pannes :**

✓ Pour assurer la disponibilité et la continuité des données et des ressources dans une entreprise un serveur en redondance est important.
✓ Le serveur en redondance prend en charge tous les services défectueux du premier serveur.

- **Un seul domaine de diffusion :**

✓ Un seul et unique domaine de diffusion ce qui implique une surcharge du réseau de l'entreprise, les machines communiquent sans cesse entre elles, le trafic réseaux devient lourd,

ce qui ralenti nettement la communication sur le réseau et engendre une lourdeur mêmes sur les applications et machines clients.

- **Architecture plate** :

✓ Besoin de segmentation du réseau en plusieurs VLAN.

✓ Changements et Configuration des Switch au niveau des armoires pour mettre à niveau le réseau VLAN de l'entreprise.

1.8.4 Les objectifs de la direction informatique :

Afin d'assurer les besoins de l'entreprise il est nécessaire d'améliorer les performances du réseau, et pour cela il faudra passer en revue tous les aspects intervenant dans ce système, notamment :

1. Amélioration de la sécurité, de la disponibilité et des performances réseau.
2. Amélioration du câblage interne.
3. Amélioration du plan d'adressage IP.
4. Mise à niveau des systèmes d'exploitation.
5. Amélioration de la qualité du matériel (serveurs, commutateurs et hôtes).
6. Maitrise de l'impact des trafics générés par les serveurs d'authentification - des médias d'interconnexion.

Notre travail consiste à mettre en œuvre d'autres améliorations à cette architecture afin d'optimiser le fonctionnement et assurer la continuité de quelques services.

1.8.5 Proposition :

- Mettre en place une solution d'amélioration de la sécurité et d'optimisation de la bande passante du réseau par la segmentation des domaines de *broadcast* de l'EPB.

La solution VLAN reste toutefois la première étape du processus d'améliorer les performances, la gestion et la sécurité du réseau de l'entreprise contre les surcharges rencontrées par les utilisateurs de l'EPB.

1.9 Conclusion

L'étude de l'existant nous a permis de se familiariser avec le réseau actuel de l'EPB, et de savoir l'utilité des différents détails, chose qui nous a fait découvrir les lacunes et les faiblesses du réseau. L'étude approfondie de ces lacunes nous a conduit à proposer une solution afin d'apporter des améliorations. Après avoir choisi la solution à adopter, nous avons tracé nos objectifs, ensuite, nous avons défini un plan de travail pour mettre en œuvre cette solution.

CHAPITRE 2 : GENERALITES SUR LES RESEAUX LOCAUX INFORMATIQUES ET LA SECURITE INFORMATIQUE

2.1 Introduction

Avec l'arrivée de l'internet dans nos réseaux locaux, de nombreux problèmes surgissent concernant la sécurité des données des utilisateurs. Donc, assurer la confidentialité de la transmission d'informations est devenu un point primordial dans la mise en place des réseaux informatiques.

L'objectif de ce chapitre est de présenter les concepts de base des réseaux locaux et de la sécurité informatique. Pour cela, nous commencerons par une brève présentation des réseaux locaux, nous parlerons en outre sur les topologies et les équipements d'interconnexion des réseaux locaux ainsi que d'autres caractéristiques de ces derniers, comme on parlera sur le modèle de référence OSI qui est le socle de référence pour les réseaux informatiques ainsi que le modèle TCP/IP.

Après avoir présenté quelques concepts des réseaux locaux, on va définir et exposer les objectifs de la sécurité informatique, comme nous exposerons quelques attaques qui exploitent les faiblesses de notre réseau, nous bouclerons ce chapitre par une présentation de quelques stratégies de la sécurité informatique telles que les pare-feux, les DZM et les VLANs

2.2 Généralités sur les réseaux locaux (LANs)

Un réseau local ou LAN, de l'anglais (Local Area Network) permet la connexion d'un ensemble de postes afin d'échanger ou de partager des informations. Il permet aussi le partage de ressource (disque, imprimante, etc.) Ces postes sont circoncis dans une zone géographique d'environ 10 km de rayon [1]

Les objectifs d'un réseau local :

- Le transfert rapide des données ;
- L'accès au réseau doit être équitable, personne ne doit être privilégié sur le réseau ;
- L'évolution du réseau et la possibilité d'être étendu.

2.2.1 Topologie des réseaux

La topologie caractérise la façon dont les différents équipements sont interconnectés.
Il convient de distinguer :

- **La topologie logique** : Elle représente la façon dont laquelle les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token ring et FDDI2 [2].

- **La topologie physique** : C'est le chemin de câblage apparent, c'est à dire ce que voit l'utilisateur. Il existe trois grands types de topologies physiques dans les réseaux locaux, la topologie en étoile, en anneau et en bus. Des topologies plus complexes peuvent être obtenues en combinant ou en dérivant ces topologies de base [3]

a. **La topologie en étoile** : Dans cette topologie chaque périphérique (ordinateur ou imprimante) est relié au nœud central. Les performances d'un réseau Ethernet dépendent principalement du nœud central (**Figure 2.1**).

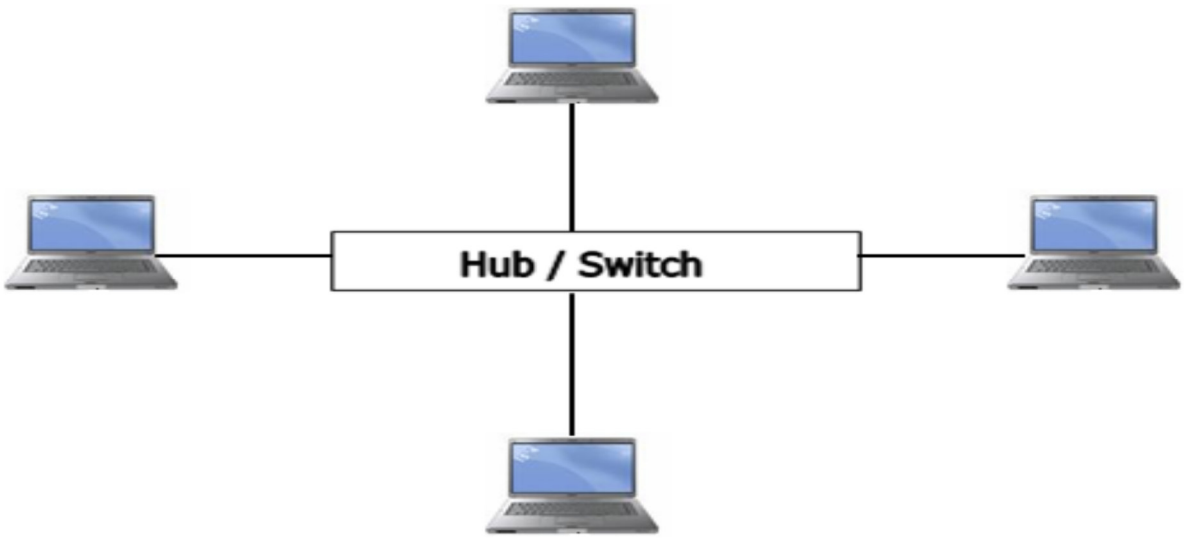


Figure 2.1. *Topologie en étoile*

C'est un type de réseau relativement efficace et économique. La plupart des petits réseaux locaux fonctionne sur ce principe, en utilisant un *Switch* central reliant tous les périphériques sur un même nœud.

b. La topologie en anneau : Dans la topologie en anneau, les postes sont reliés entre eux pour former une boucle. L'ordre d'accès au réseau se fait grâce à un unique jeton qui passe d'un post à un autre tout autour de l'anneau en bouclant sans cesse. Un poste ne peut transmettre une information sur le réseau que lorsqu'il a le jeton. Chaque nœud du réseau a ainsi la même possibilité de communiquer. Le plus gros problème est que si l'un des nœuds connait une avarie tout le réseau en pâtit. La technologie de réseau en anneau la plus connue est la technologie Token Ring (Figure 2.2).

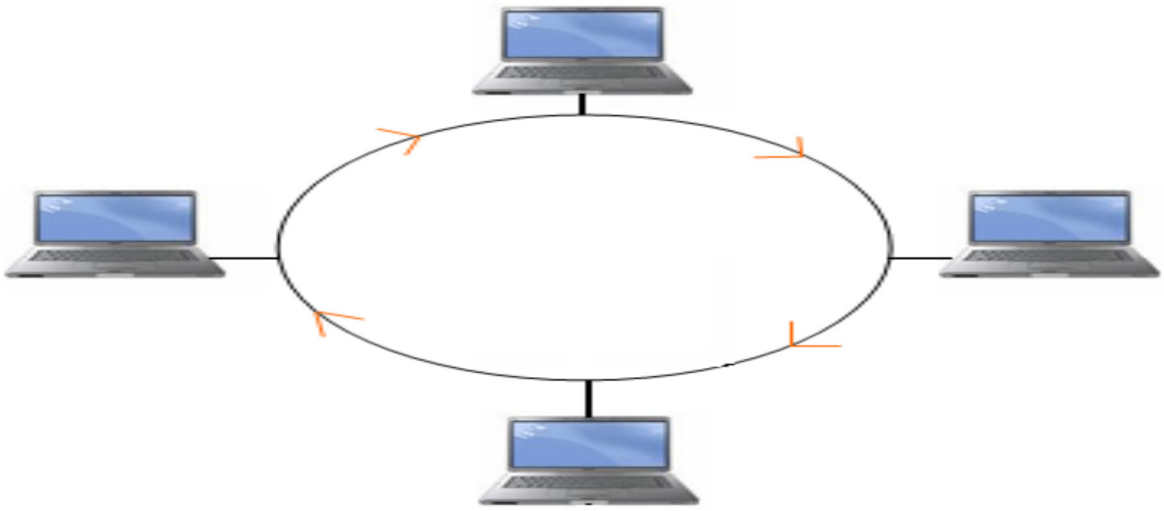


Figure 2.2. *Topologie en anneau*

c. La topologie en bus : La topologie en bus est probablement la plus utilisée, elle utilise un seul médium de transmission (par exemple un seul câble). Tous les postes partagent le même bus et les mêmes communications (Figure 2.3).

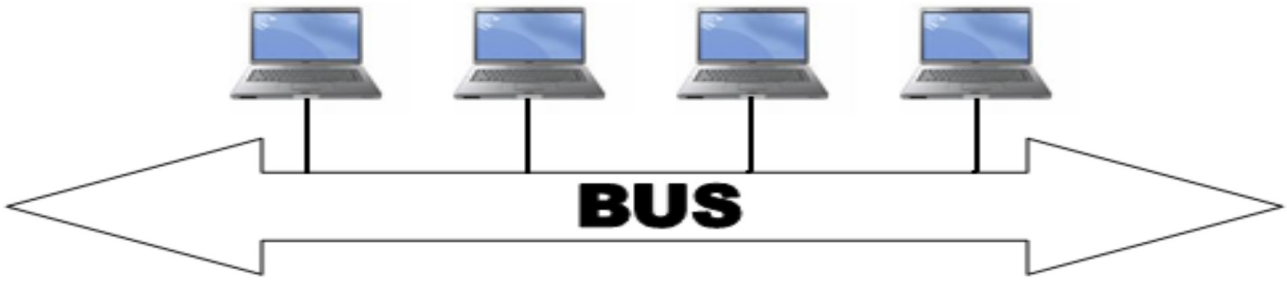


Figure 2.3. *Topologie en bus*

Elle a pour avantages d'être facile à mettre en œuvre, par contre elle est extrêmement vulnérable étant donné que si un des coupleurs est défectueux, c'est l'ensemble du réseau qui est affecté.

2.2.2 L'interconnexion d'un réseau locale

La mise en place d'un réseau soulève de nombreuses questions sur les contraintes d'utilisation. Comment faire si le réseau à créer dépasse les distances maximales imposées par le type de câble utilisé ? Comment faire parvenir les informations à d'autres réseaux que le sien ? Comment relier des réseaux utilisant des protocoles de communication différents? Toutes ces questions peuvent être résolues grâce à différents types de matériels qui sont [4] :

- Répéteur : dispositif permettant d'étendre la distance de câblage d'un réseau local.

Il amplifie et répète les signaux qui lui parviennent.

- Pont : Un pont *(bridge)* est un dispositif permettant de relier des réseaux de même nature.
- Routeur : Un routeur *(router)* est un dispositif permettant de relier des réseaux locaux de telle façon à permettre la circulation de données d'un réseau à un autre de façon optimale.

- Passerelle : Une passerelle *(gateway)* est un dispositif permettant d'interconnecter des différents réseaux. Elle assure la traduction d'un protocole d'un haut niveau vers un autre.

- Concentrateur : Un concentrateur *(hub)* est un dispositif permettant de connecter divers éléments de réseau.

- Commutateur : Un commutateur *(Switch)* est un dispositif permettant de relier divers éléments tout en segmentant le réseau.

- Adaptateur : Un Adaptateur *(adapter)* est destiné à être inséré dans un poste de travail ou un serveur afin de le connecter à un système de câblage.

2.2.3 Supports de transmission

Le choix du support est en fonction de critères interdépendants, parmi lesquels :
La distance maximale entre les stations, les débits minimum et maximum, le type de transmission (numérique ou analogique), la nature des informations échangées (donnée, voix, vidéo, etc.), la connectique, la fiabilité, le coût, etc. [5]

Types	**Caractéristiques**
Paire torsadée	Débits pouvant atteindre 100 Mbit/s. Affaiblissement important. Sensibilité aux parasites d'origine électromagnétique
Câble coaxial	Bande passante pouvant atteindre 300 à 400 MHz. Peu sensible aux inductions.
Fibre optique	Bande passante supérieure au GHz. Affaiblissement léger. Insensibilité aux parasites d'origine électromagnétique

Tableau 2.1. *Types de supports de transmission*

2.2.4 Modèles de référence

Sur un réseau, la communication entre les différents éléments implique une logique dans leur façon d'interagir, et le respect d'un certain nombre de conventions et de règles afin d'assurer le bon déroulement du processus de transfert et de vérification des données reçues. L'ensemble de ces règles et conventions s'appelle un protocole, il en existe un grand nombre. Afin que tous ces protocoles puissent cohabiter et faciliter la conception de nouveaux matériels compatibles avec les appareils existants, il est souhaitable que tous ces protocoles utilisent un langage commun [6].

2.2.4.1 le modèle de référence OSI

Le modèle de référence OSI (Open System Interconnexion) définit une sorte de langage commun. Ce modèle a été mis au point par l'ISO (Organisation Internationale des Standards) et est devenu le socle de référence pour tout système de traitement de communications. Il répartit les questions relatives au domaine des communications informatiques selon sept couches classées par ordre d'abstraction croissant. Son objectif est d'assurer que les protocoles spécifiques utilisés dans chacune des couches coopèrent pour assurer une communication efficace. Décrivons succinctement le rôle de chaque couche [6] :

1. **Physique** : Elle convertit les signaux électriques en bits de données et vice versa, selon la réception ou la transmission des informations à la couche liaison.

2. **Liaison** : Elle est divisée en deux sous-couches :
   - La couche MAC qui structure les bits de données en trames et gère l'adressage des cartes réseaux.
   - La couche LLC qui assure le transport des trames et gère l'adressage des utilisateurs, c'est à dire des logiciels de couches supérieures.

3. **Réseau** : Elle traite la partie donnée utile contenue dans la trame. Elle connait l'adresse de tous les destinataires et choisit le meilleur itinéraire pour l'acheminement. Elle gère donc l'adressage logique et le routage.

4. **Transport** : Elle segmente les données de la couche session, prépare et contrôle les tâches de la couche réseau. Elle peut multiplier les voies d'accès et corriger les erreurs de transport.

5. **Session** : Son unité d'information est la transaction. Elle s'occupe de la gestion et la sécurisation du dialogue entre les machines connectées, les applications et les utilisateurs (noms d'utilisateurs, mots de passe, etc.)

6. **Présentation** : Elle convertit les données en information compréhensible par les applications et les utilisateurs, syntaxe, sémantique, conversion des caractères graphiques, format des fichiers, cryptage et la compression.

7. **Application** : C'est l'interface entre l'utilisateur ou les applications et le réseau. Elle concerne la messagerie, les transferts et partages de fichiers et l'émulation de terminaux.

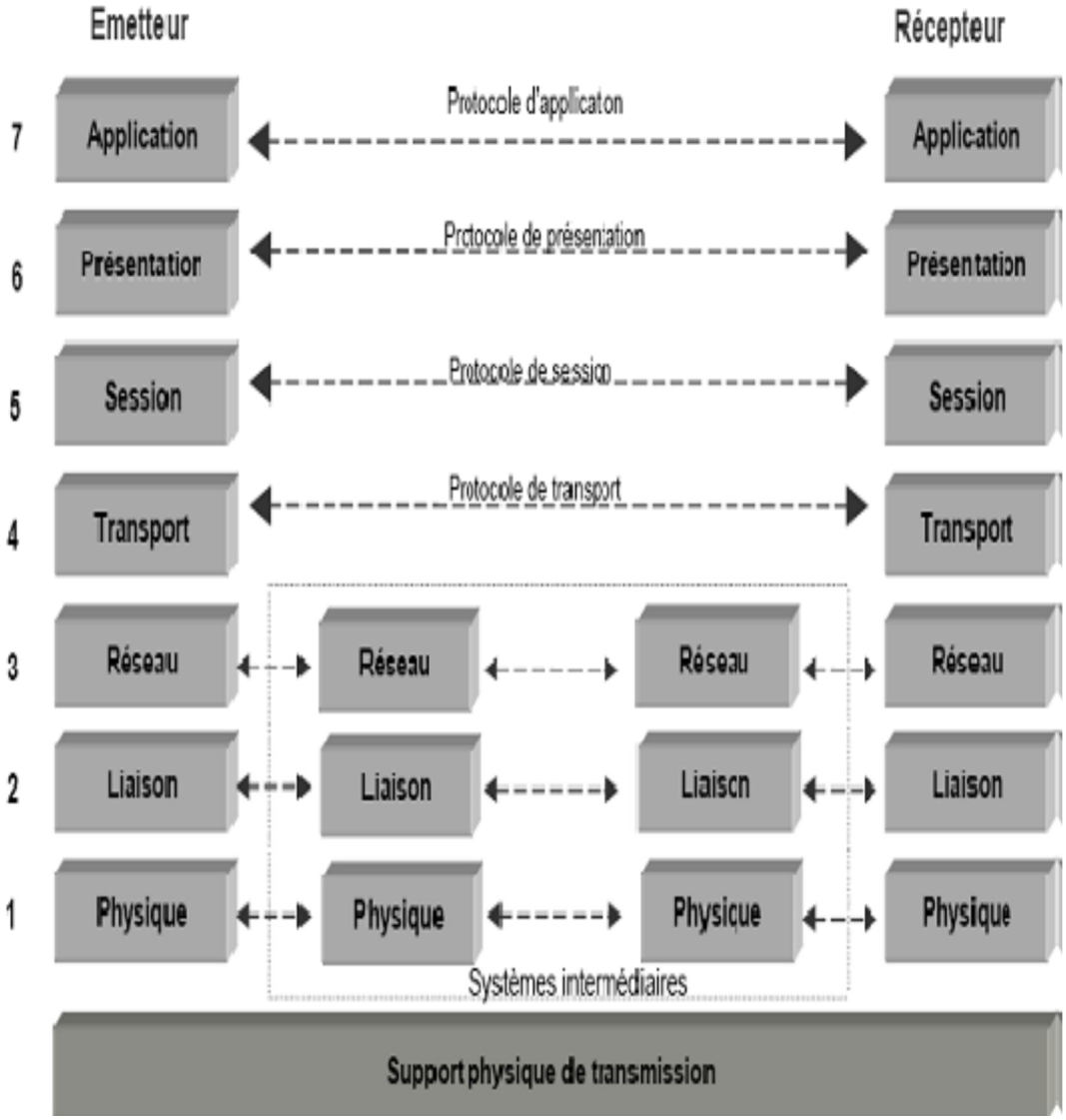


Figure 2.4. *Les couches du module OSI et leurs protocoles*

2.2.4.2 le modèle de référence TCP/IP

Contrairement au modèle OSI, le modèle TCP/IP est né d'une implémentation mais il est inspiré du modèle OSI. Il reprend l'approche modulaire (utilisation de modules ou des couches) mais en contient uniquement quatre. Les trois couches supérieures du modèle OSI sont souvent utilisées par une même application [6] [7].

Le schéma ci-dessous (Figure 2.5) nous montre la différence entre ces deux modèles :

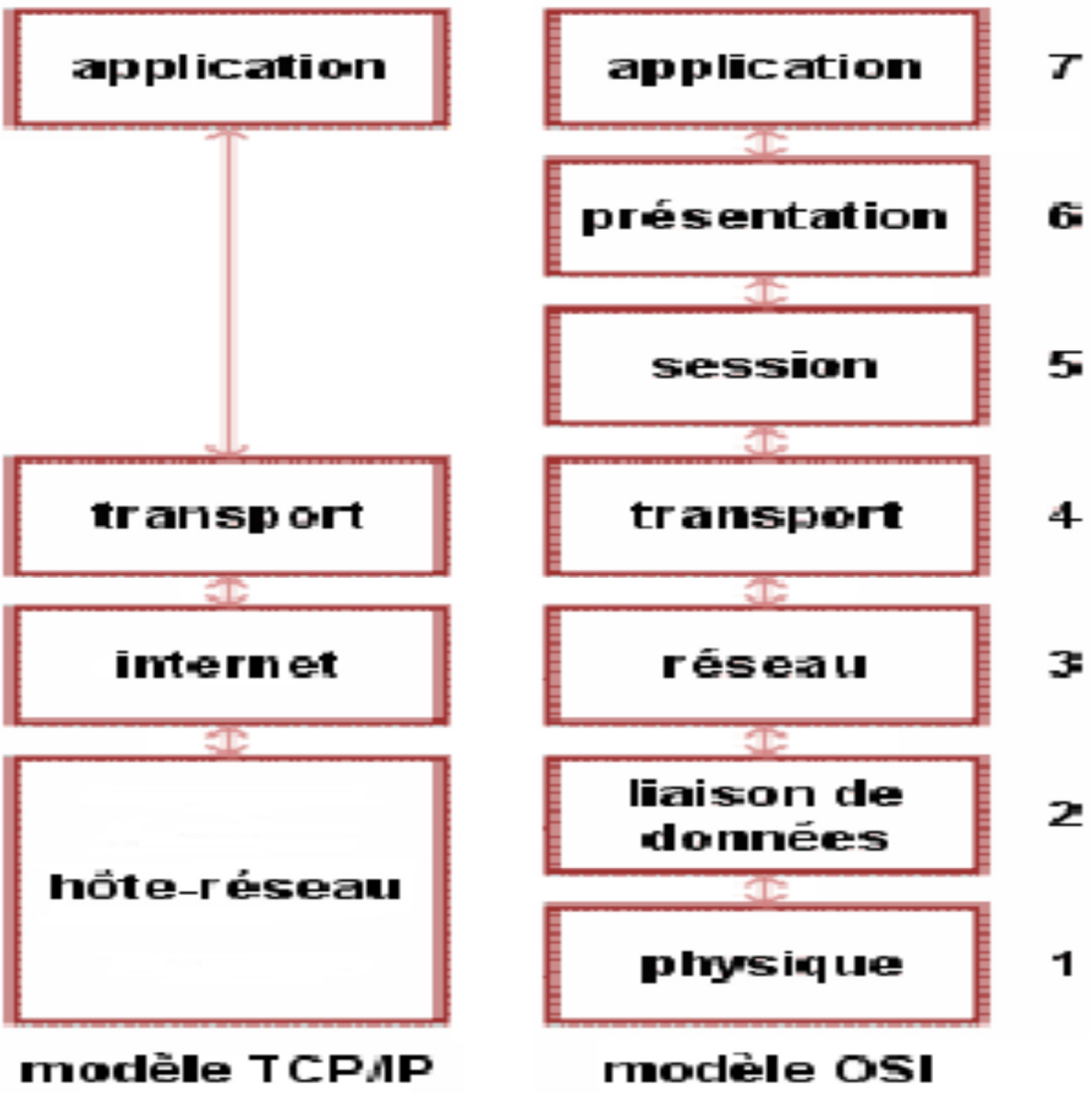


Figure 2.5. *Comparaison entre le modèle TCP/IP et le modèle OSI*

2.3 Généralités sur la sécurité informatique

C'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système informatique contre les menaces accidentelles ou intentionnelles auxquelles il peut être confronté. En d'autres mots, c'est l'ensemble des techniques qui assure que les ressources du système d'information (matérielles ou logicielles) d'une organisation soient utilisées uniquement dans le cadre où il est prévu d'être. [8]

2.3.1 Objectifs de la sécurité informatique

La sécurité informatique vise généralement cinq objectifs : [9]

- L'intégrité : c'est-à-dire garantir que les données sont bien celles que l'on croit être ;
- La confidentialité : consiste à assurer que seules les personnes concernées aient accès aux ressources échangées ;
- La disponibilité : permettant de maintenir le bon fonctionnement du système d'information ;
- La non-répudiation : permettant de garantir qu'une transaction ne peut être niée ;
- L'authentification : consiste à assurer que seules les personnes autorisées aient accès aux ressources.

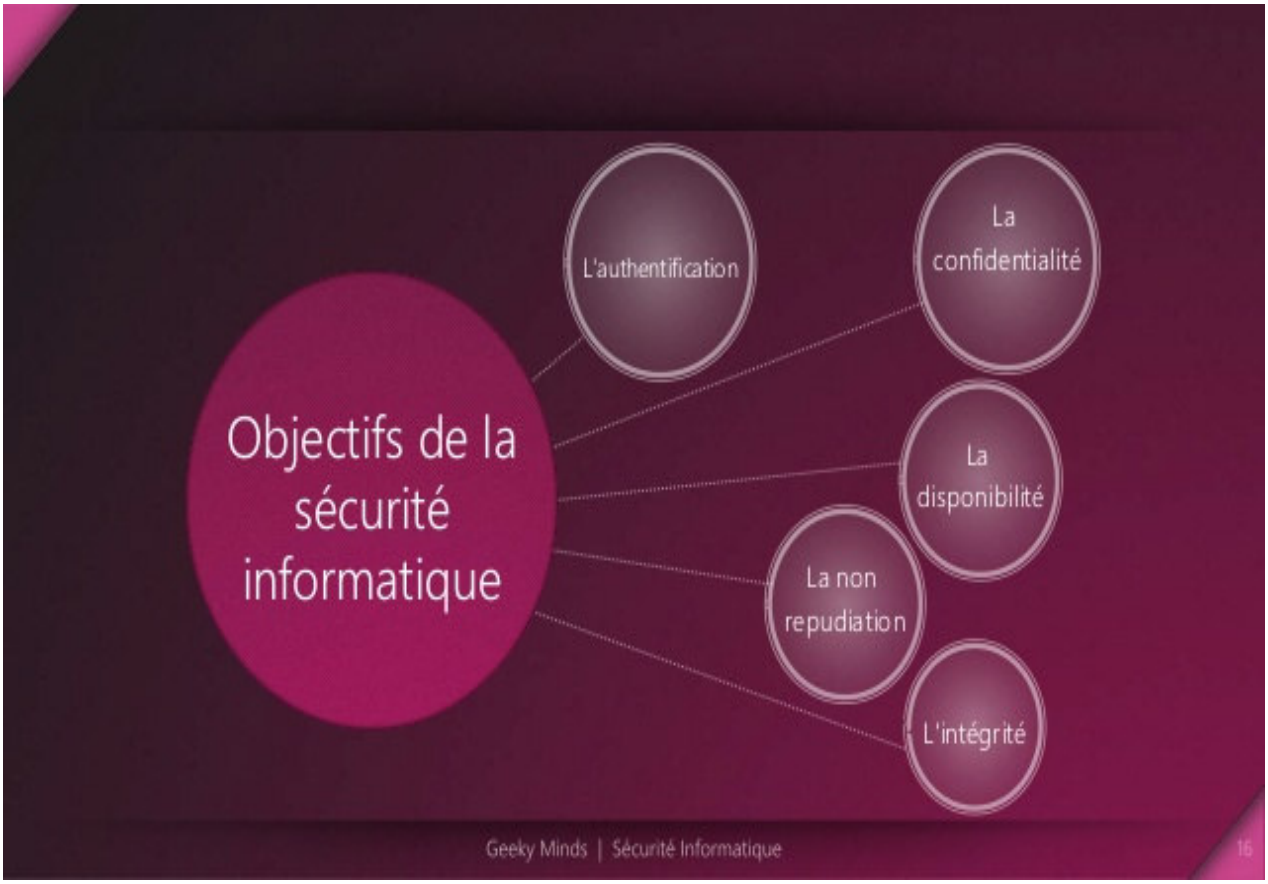


Figure 2.6. *Objectifs de la sécurité informatique*

2.3.2 Les attaques

Une attaque représente les moyens d'exploiter une vulnérabilité en s'appuyant sur divers types de faiblesses telles que les faiblesses des protocoles, faiblesses d'authentification, faiblesses d'implémentation et les mauvaises configurations.

2.3.2.1 Classification des attaques

Les attaques peuvent être classées en deux grandes catégories : Attaques passives et Attaques actives.

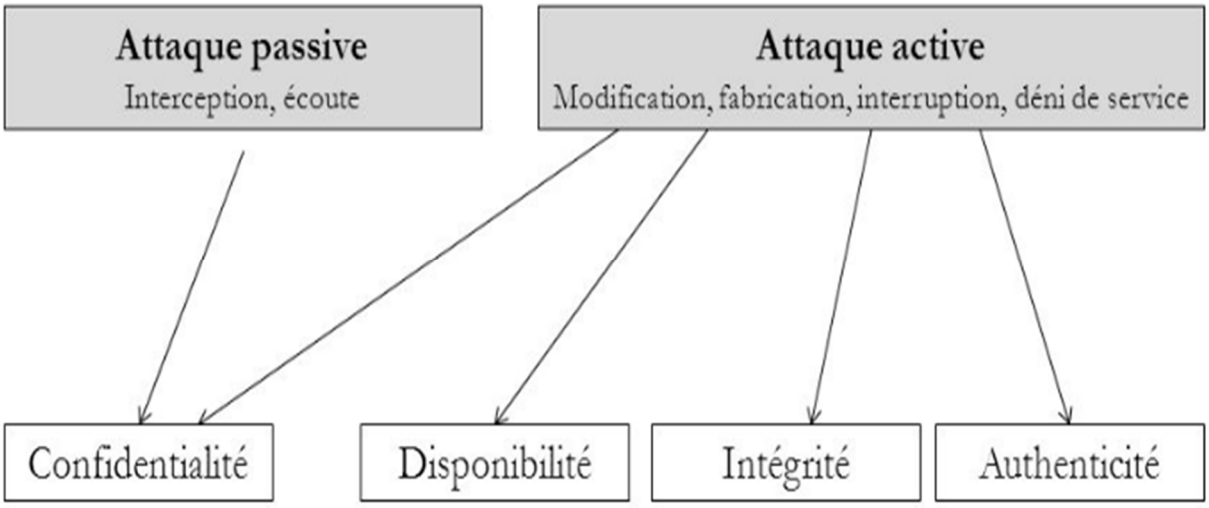


Figure 2.7. *Classification des attaques*

- **Attaques passives** : Consistent à écouter et à analyser le trafic échangé sans modifier les données ou le fonctionnement du réseau. Elles sont généralement indétectables mais une prévention est possible [10].

- **Attaques actives** : Les attaques actives concernent celles qui entrainent une modification des données ou création de données incorrectes. Autrement dit, celles qui portent atteinte à l'intégrité, l'authenticité et la disponibilité.

2.3.2.2 Description de quelques attaques

Les attaques réseau sont aujourd'hui si nombreuses qu'il serait imaginaire de prétendre les décrire toutes. Elles touchent généralement les trois composantes suivantes d'un système : La couche réseau, le système d'exploitation et la couche application. De plus, beaucoup d'attaques peuvent impacter le réseau de manière directe ou indirecte, en voici quelques unes [11][12] :

a. Attaques par déni de service (DoS) : Le déni de service est une attaque qui vise à rendre un service, un système ou un réseau indisponible. Ces attaques se basent généralement soit sur une faiblesse d'implémentation ou bogue, soit sur une faiblesse d'un protocole. Il existe plusieurs types de déni de service, on peut citer par exemple le *flooding*, le *smurf* ou les *DDOS* .

b. L'attaque IP spoofing : Elle consiste à se faire passer pour un autre système en falsifiant son adresse IP. Le pirate commence par choisir le système qu'il veut attaquer. Après avoir obtenu le maximum de détails sur le système cible, il détermine les adresses IP autorisés à se connecter au système cible.

c. Attaques permettant d'écouter le trafic réseau (sniffing) : L'attaque par *sniffing* est généralement utilisée par les pirates pour capturer les mots de passe.
Lorsqu'on se connecte à un réseau qui utilise le mode *broadcast*, toutes les données en transit arrivent à toutes les cartes réseau connectées à ce réseau. En temps normal, seules les trames destinées à la machine sont lues, les autres étant ignorées. Grace à un sniffer, il est possible d'intercepter les trames reçues par la carte réseau d'un système pirate qui ne lui sont pas destinées.

2.3.3 Stratégies de la sécurité

Les stratégies de la sécurité consistent à déployer des moyens et des dispositifs visant à sécuriser le système d'information ainsi que de faire appliquer les règles définies dans une politique de sécurité. Parmi ces mécanismes, on peut citer :

2.3.3.1 Pare-feu (Firewall)

Le pare-feu est un ensemble de différents composants matériels (physique) et logiciels (logique) qui contrôlent le trafic intérieur/extérieur selon une politique de sécurité.
Un système pare-feu fonctionne la plupart du temps grâce à des règles de filtrage indiquant les adresses IP autorisées à communiquer avec les machines aux réseaux, il s'agit ainsi d'une passerelle filtrante.

Il permet d'une part de bloquer des attaques ou connexions suspectes d'accéder au réseau interne, d'autre part, un firewall sert dans de nombreux cas également à éviter la fuite non contrôlée d'informations vers l'extérieur. Il propose un véritable contrôle sur le trafic réseau de l'entreprise, Il permet donc d'analyser, de sécuriser et de gérer le trafic réseau [13].

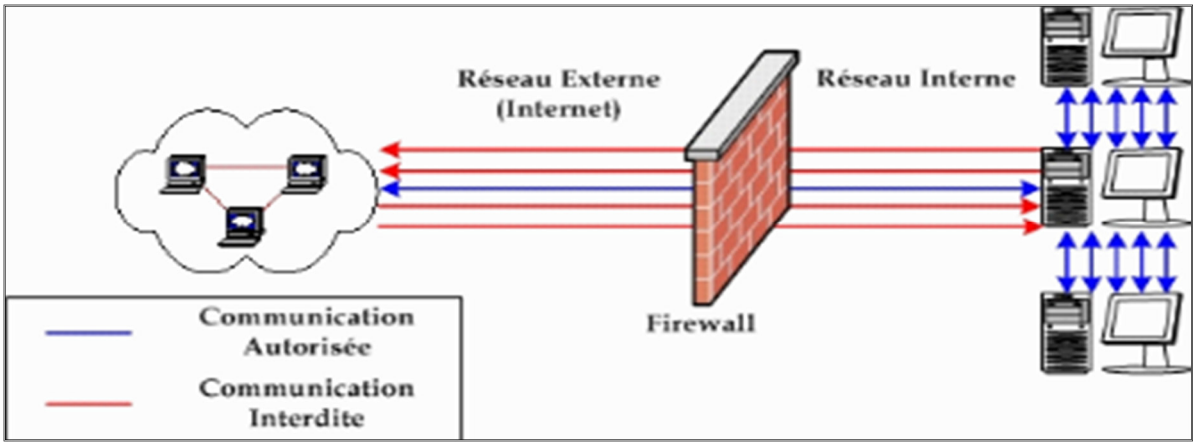


Figure 2.8. *Schéma d'une architecture réseau utilisant un Firewall*

2.3.3.2 Zone démilitarisée

Une DMZ est une interface située entre un réseau connu (réseau interne) et un réseau externe (internet). Une série de règles de connexion configurées sur le pare-feu font de cette interface une zone physiquement isolée entre les deux réseaux. Cette séparation physique permet d'autoriser les accès internet à destination des serveurs placés dans la DMZ et non à ceux destinés au réseau privé (interne) [14].

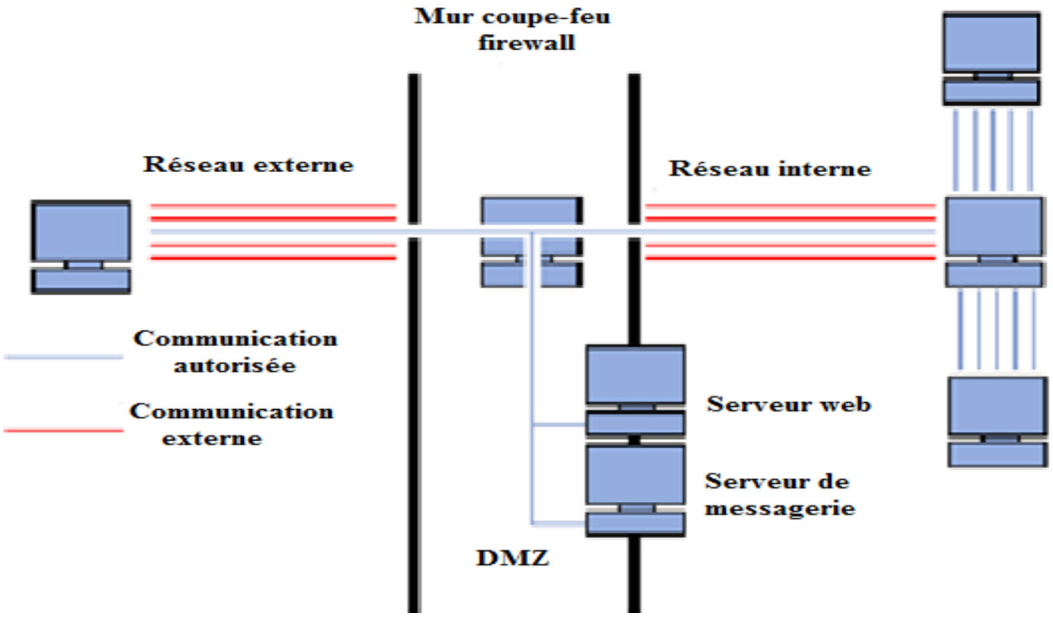


Figure 2.9. *DMZ (zone démilitarisée)*

2.3.3.3 Systèmes de détection d'intrusion (IDS)

Un système de détection d'intrusion (ou IDS : Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies. [15]
Il faut distinguer deux aspects dans le fonctionnement d'un IDS : le mode de détection utilisé et la réponse apportée par l'IDS lors de la détection d'une intrusion.

2.3.3.4 Les VLANs

Un VLAN est assimilable à un domaine de diffusion (*Broadcast Domain*). Ceci signifie que les messages de diffusion émis par une station d'un VLAN ne sont reçus que par les stations de ce VLAN. Ces derniers n'ont été réalisables qu'avec l'apparition des commutateurs (*switches*) [16]

2.3.3.5 La cryptographie

Le chiffrement est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de déchiffrement. Ce principe est généralement lié au principe d'accès conditionnel.

Bien que le chiffrement puisse rendre secret le sens d'un document, d'autres techniques cryptographiques sont nécessaires pour communiquer de façon sûre. [15]

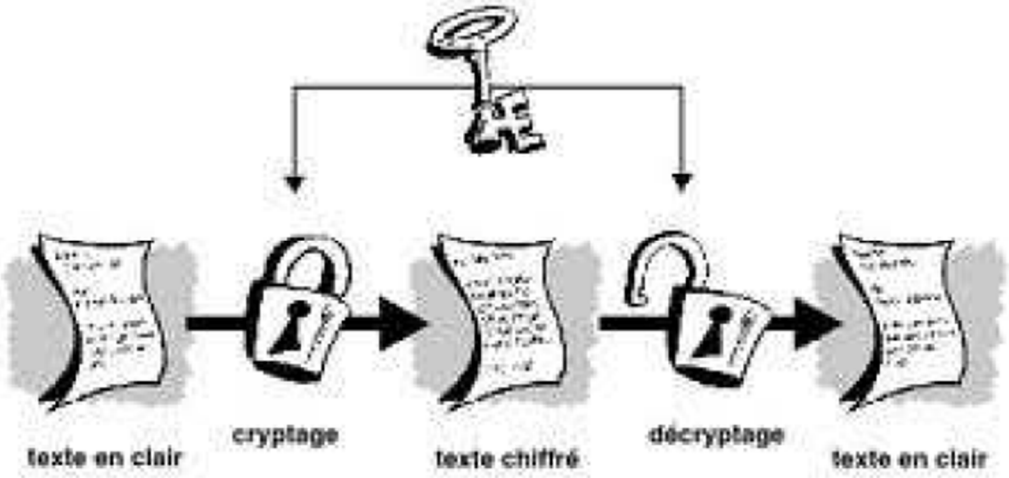


Figure 2.10. *La cryptographie*

2.3.3.6 Les VPNs

Dans les réseaux informatiques, le réseau privé virtuel (de l'anglais *Virtual Private Network*, abrégé en VPN) est une technique permettant aux postes distants de communiquer de manière sûre, tout en empruntant des infrastructures publiques (internet). [18]

Un VPN repose sur un protocole, appelé protocole de tunnelisation, c'est-à-dire un protocole permettant aux données passant d'une extrémité à une autre du VPN d'être sécurisées par des algorithmes de cryptographie. [18]

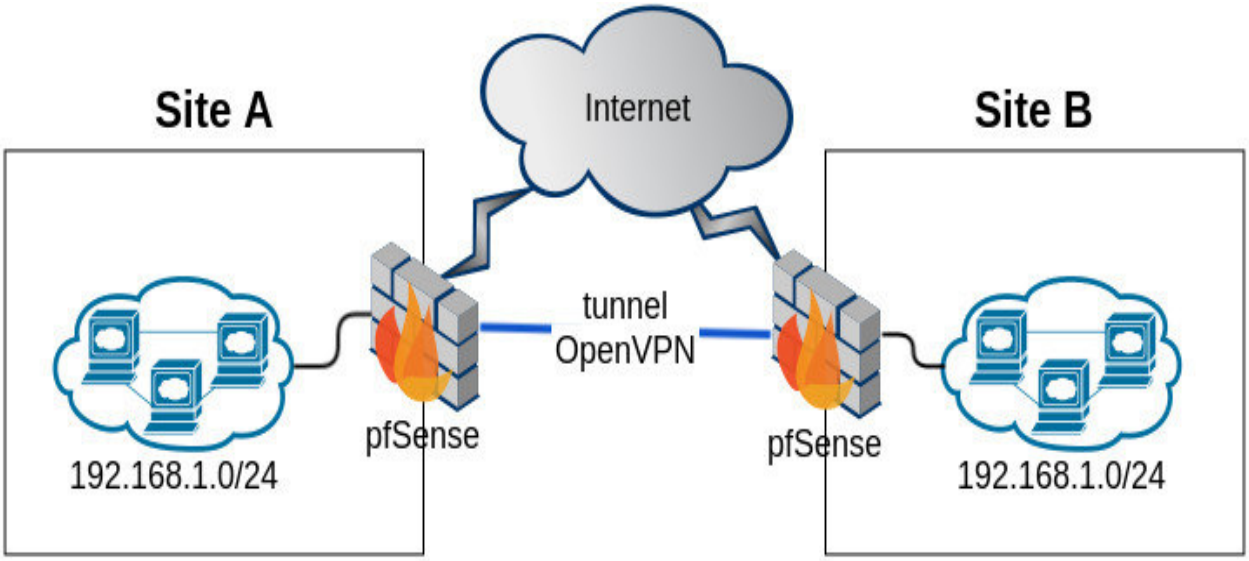


Figure 2.11 *Principe de fonctionnement d'un VPN*

2.4 Conclusion

Ce chapitre nous a permis d'avoir une idée bien claire sur les réseaux locaux et de mieux comprendre les raisons pour lesquelles les spécialistes en réseau ont élaboré le modèle de référence OSI et surtout l'apport de ce modèle pour le développement des réseaux locaux. Nous avons aussi abordé la sécurité des réseaux informatiques qui est devenue un sérieux problème et que la majorité des entreprises ne peuvent plus ignorer. Nous avons résumé quelques stratégies de sécurités telles que l'utilisation d'un pare-feu, ce dernier permet de vérifier la confidentialité et l'intégrité des ressources sur les réseaux. Nous avons vu aussi les VLANs qui sont la stratégie que nous détaillerons dans le chapitre suivant afin de l'implémenter au réseau intranet de l'EPB

CHAPITRE 3 : LES RESEAUX LOCAUX VIRTUELS (VLANs)

3.1 Introduction

Aujourd'hui, une majorité d'entreprises possède leur propre parc de réseau informatique interne sous la forme d'un LAN (*Local Area Network*) permettant la communication de données ou tout simplement d'informations d'un pôle d'une entreprise à un autre, et se présentant sous la forme d'un ensemble de matériels réseaux (commutateurs, routeurs, etc.) reliés entre eux. Cependant, il est parfois nécessaire de couper quelques uns de ces liens pour des raisons sécuritaires, c'est à dire, interdire la communication d'un poste à l'autre.

Dans ce chapitre, nous donnons dans un premier temps une définition des réseaux locaux virtuels et les raisons de leur utilisation, ensuite nous concentrons notre attention sur les types des réseaux locaux virtuels. Nous présenterons quelques avantages des VLANs, puis nous conclurons ce chapitre par la présentation de quelques protocoles utilisés afin de répondre aux besoins de cette technologie.

3.2 Définition

Un réseau local virtuel est un regroupement virtuel d'au moins deux périphériques. Ce regroupement virtuel peut s'étendre au-delà de plusieurs commutateurs. Les périphériques sont regroupés sur la base d'un certain nombre de facteurs suivant la configuration du réseau. [19]

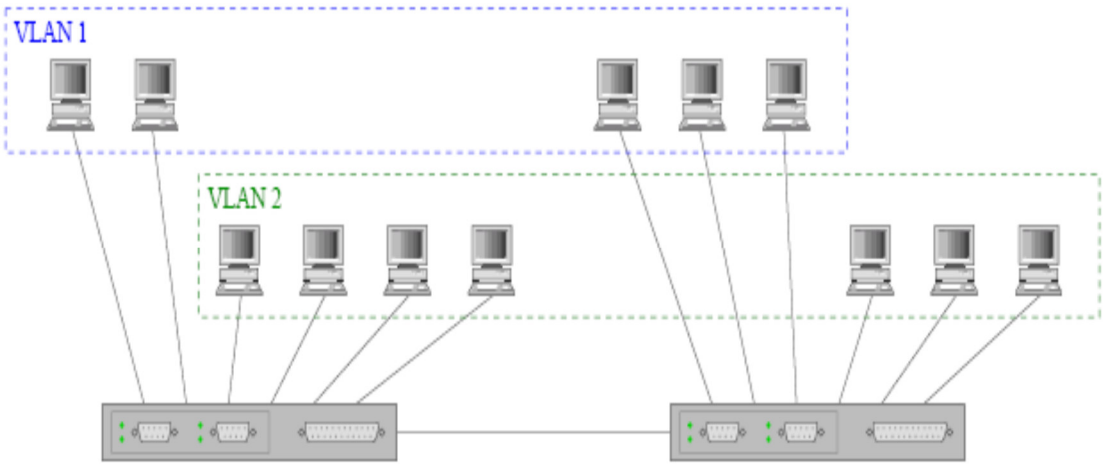


Figure 3.1. *Plusieurs VLANs dans un réseau Ethernet*

3.3 Les raisons d'utilisation des VLANs

Quatre raisons principales sous-tendent le développement des VLANs et leurs inter-Connexions : la nécessité de gérer des organisations virtuelles, la possibilité de simplifier l'administration des réseaux, une meilleure utilisation de la bande passante du réseau et l'amélioration de la sécurité du réseau. Etudions successivement chacune d'elles [20] [21].

a. L'optimisation de l'utilisation de la bande passante : Dans un réseau local, les paquets transmis par un utilisateur sont envoyés à toutes les stations du réseau alors qu'avec les réseaux virtuels, les paquets transmis par un membre d'un groupe ne sont reçus que par les autres membres de ce groupe et non par toutes les stations du réseau. Ainsi, il n'y a pas de trafic vers des destinations inutiles ou non déclarées.

b. Augmentation de la sécurité : Dans un réseau local, des informations sensibles sont diffusées sur le réseau. Avec les VLANs, il est possible de créer un groupe composé uniquement d'utilisateurs qui peuvent avoir accès à ces informations. Comme les émissions de paquets sont limitées à des domaines, tous les systèmes qui n'appartiennent pas à ces domaines ne seront pas en mesure de recevoir ces informations. Les VLANs créent une frontière virtuelle qui n'est franchissable qu'avec un routeur (ou un commutateur de niveau 3).

c. L'administration des réseaux : l'administration des réseaux est simplifiée. Ainsi, on limitera la reconstruction du réseau (refaire le câblage, reconfigurer les équipements, etc.) et les frais (le déplacement physique d'une station d'un réseau local à un autre implique des coûts élevés).

d. Le support d'organisations virtuelles : Il est possible avec les réseaux virtuels de définir un groupe temporaire, par exemple, un groupe constitué d'employés de telle entreprise qui travaillent sur un même projet dans différents LAN ou non. Les VLANs leur permettent de partager des données et de travailler ensemble sur ce projet et cela indépendamment de la localisation de ces employés.

3.4 Méthodes d'attribution des VLANs

Trois méthodes sont généralement utilisées pour attribuer un équipement à un réseau VLAN :

a) Les réseaux VLAN basés sur les ports
b) Les réseaux VLAN basés sur les adresses MAC
c) Les réseaux VLAN basés sur les protocoles ou les sous-réseaux

Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue. [19]

3.4.1 VLAN niveau 1

Un VLAN de niveau 1 (aussi appelés **VLAN par port**, en anglais *Port-Based VLAN*) définit un réseau virtuel en fonction des ports de raccordement sur le *switch*. Dans le cadre des réseaux VLAN basés sur les ports, l'appartenance de chaque port du commutateur à tel ou tel réseau VLAN est configurée manuellement.

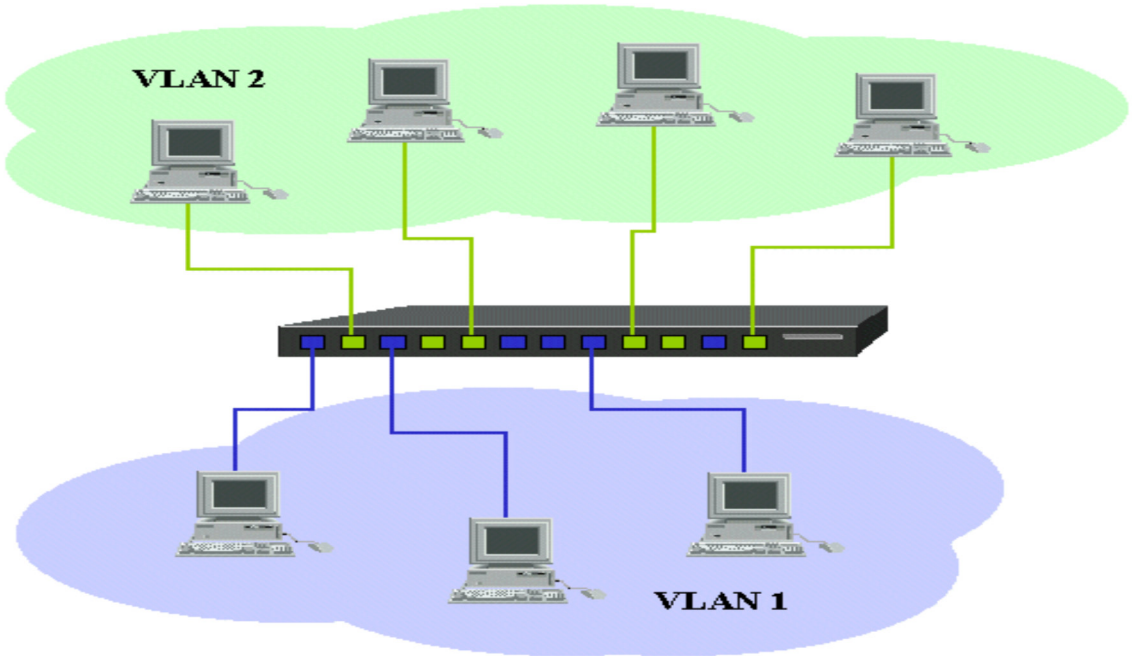


Figure 3.2. *Construction des VLANs par port*

3.4.2 VLAN niveau 2

Un VLAN de niveau 2 (également appelé **VLAN MAC**, VLAN par adresse IEEE ou en anglais *MAC Address-Based VLAN*) consiste à définir un réseau virtuel en fonction des adresses MAC des stations. Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station. L'un des problèmes que posent les réseaux VLAN basés sur les ports est que si le périphérique d'origine est retiré du port pour être remplacé par un autre périphérique, le nouveau périphérique appartiendra au même réseau VLAN que son prédécesseur. Dans l'exemple du réseau VLAN composé d'imprimantes, imaginons qu'une imprimante soit retirée d'un port du commutateur pour être remplacée par un périphérique du service de comptabilité. Ce dernier dépendra désormais du réseau VLAN des imprimantes. Ceci risque de limiter l'accès du périphérique de comptabilité aux ressources du réseau. Les réseaux VLAN basés sur les adresses MAC permettent de résoudre ce problème. En effet, dans ce cas, l'appartenance au réseau VLAN dépend de l'adresse MAC du périphérique et non du port de commutation physique. Lorsque le périphérique est retiré pour être connecté à un autre port, son appartenance au réseau VLAN le suit. Malheureusement, la corrélation entre les adresses MAC et le numéro VLAN prend pas mal de temps et donc ce type de réseau VLAN est rarement utilisé.

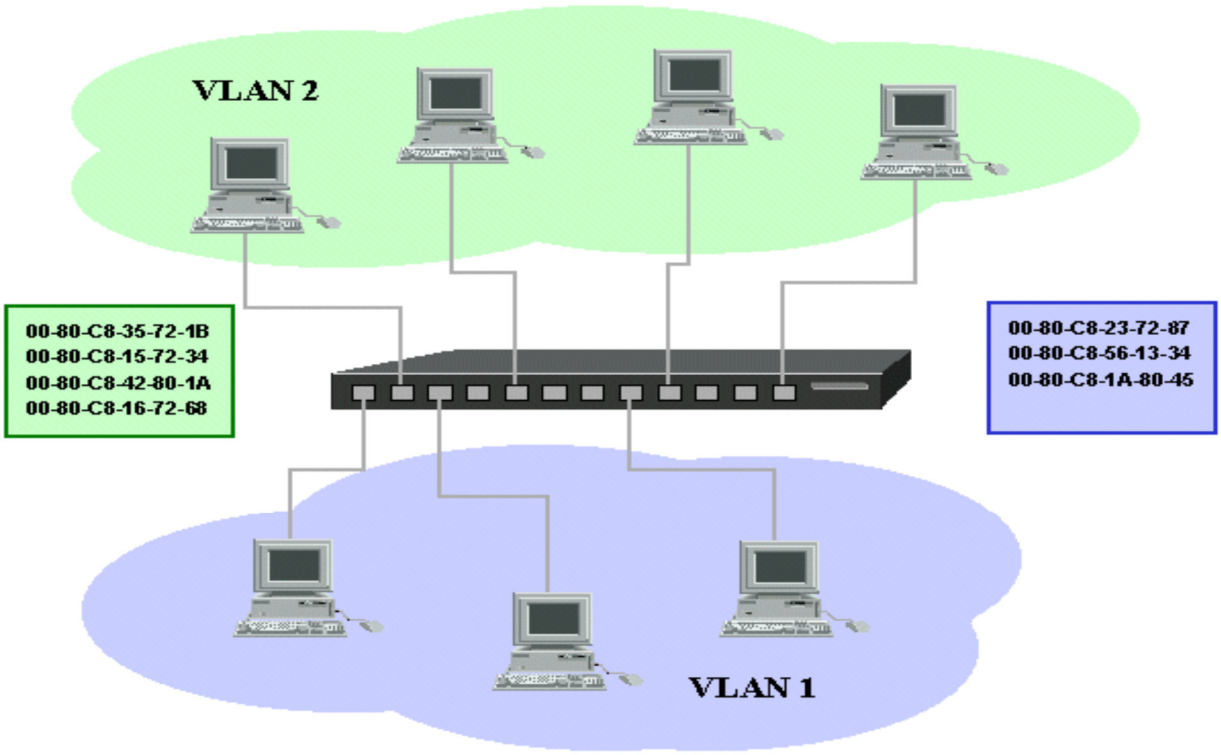


Figure 3.3. *Construction des VLANs par adresse MAC*

3.4.3 VLAN niveau 3

On distingue deux types de VLAN de niveau 3 :

- **Le VLAN par sous-réseau** (en anglais *Network Address-Based VLAN*) associe des sous réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de déplacement d'une station. En contrepartie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.

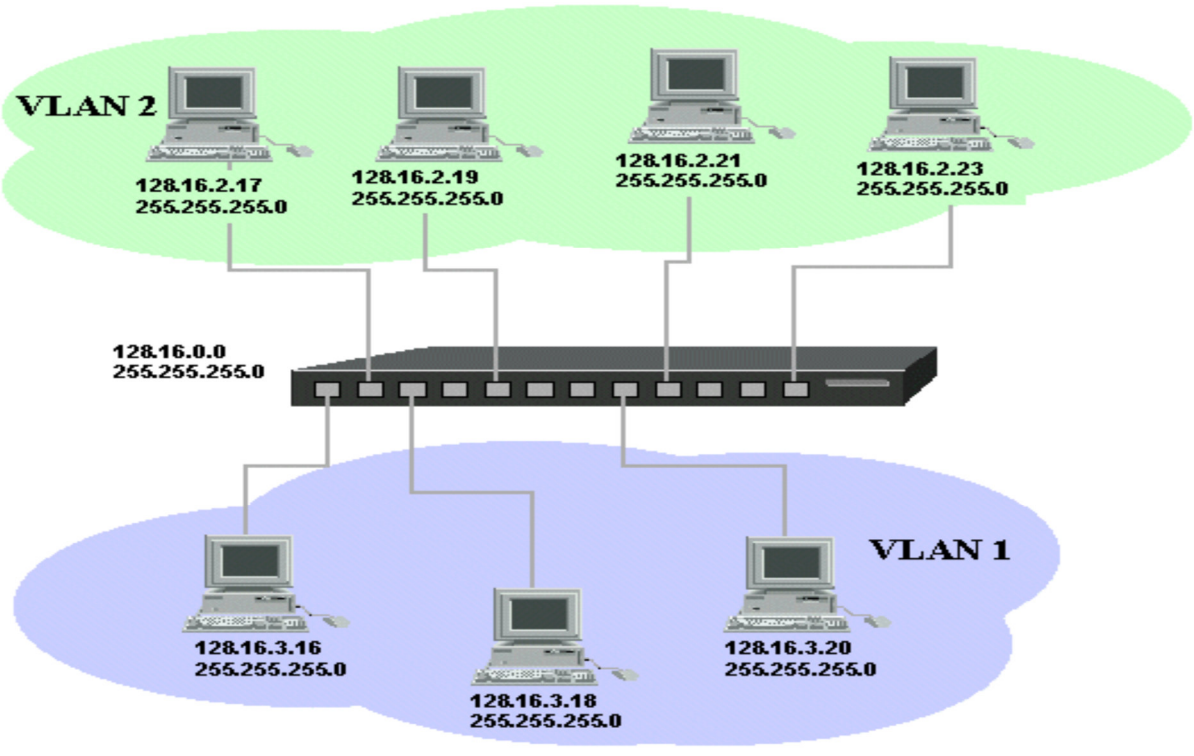


Figure 3.4. *Construction des VLANs par sous- réseau*

- **VLAN par protocole** (en anglais *Protocol-Based VLAN*) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau. Avec les réseaux VLAN basés sur les protocoles, c'est le protocole de couche 3 transporté par la trame qui permet de déterminer l'appartenance aux réseaux VLAN. Cette méthode peut fonctionner dans un environnement où figurent plusieurs protocoles, mais n'est pas très pratique sur un réseau à prédominance IP.

3.5 Communication inter VLAN

Le principe des réseaux locaux virtuels est de limiter la diffusion des informations entre eux. Ce qui rend imperméable la communication entre deux machines situées sur des VLAN différents. Les ports d'interconnexion entre commutateurs supportant les VLANs sont dénommés ***trunk***. Cette dénomination permet de prendre en compte de façon particulière la communication inter commutateurs. Cette communication maintien l'isolement entre les VLANs. La seule solution technique permettant de partager des ressources ou d'échanger des données est soit de passer par un routeur qui assurera la communication à l'aide de ses tables de routage, soit de rendre disponibles les ressources aux deux VLANs [22].

3.6 Les avantages des VLANs

Le réseau local virtuel permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants :

- Plus de souplesse pour l'administration et les modifications du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs.
- Gain en sécurité, car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées.
- Réduction de la diffusion du trafic sur le réseau.

3.7 Les protocoles de transport des VLANs

3.7.1 La notion du TRUNK

Pour communiquer entre plusieurs réseaux locaux virtuels et assurer la répartition de ces derniers sur plusieurs équipements, il est nécessaire d'élaborer une technique de partage des réseaux locaux entre équipements. Cette technique consiste à étiqueter les trames pour identifier le trafic des différents réseaux locaux sur un même canal physique. Ainsi, les réseaux locaux sont distribués sur les différents équipements via des liaisons logiques dédiées appelées ***trunks***. Le ***trunk*** est une connexion physique unique sur laquelle on transmet le trafic de plusieurs réseaux virtuels. Les trames qui traversent le *trunk* sont complétées avec un identificateur de réseau local virtuel (VLAN id). Grâce à cette identification, les trames sont conservées dans un même VLAN (ou domaine de diffusion) [26].

Les ***trunks*** peuvent être utilisés :

- **Entre deux commutateurs**

C'est le mode de distribution des réseaux locaux le plus courant. C'est la solution du second problème énoncé ci-dessus.

- **Entre un commutateur et un hôte**

C'est le mode de fonctionnement à surveiller étroitement. Un hôte qui supporte le *trunking* a la possibilité d'analyser le trafic de tous les réseaux locaux virtuels.

- **Entre un commutateur et un routeur**

C'est le mode de fonctionnement qui permet d'accéder aux fonctions de routage ; donc à l'interconnexion des réseaux virtuels par routage inter-VLAN. C'est la solution du premier problème énoncé ci-dessus.

3.7.2 La norme 802.1Q

Le protocole IEEE 802.1Q est un protocole normalisé par L'IEEE (il fonctionne sur tous les équipements.). Il est de nos jours le protocole le plus utilisé pour faire du *trunking*.

Le principe consiste à ajouter dans l'entête de la trame Ethernet un marqueur qui va identifier le VLAN. Il existe quelques solutions propriétaires pour réaliser ceci, mais le système s'est avéré tellement intéressant qu'une norme a été définie, il s'agit de la norme 802.1q [24].

La norme 802.1Q rajoute deux champs à l'entête de protocole de niveau 2 appelés tag. Voici l'exemple d'une trame Ethernet pour laquelle les champs TPID et TCI ont été ajoutés [23] :

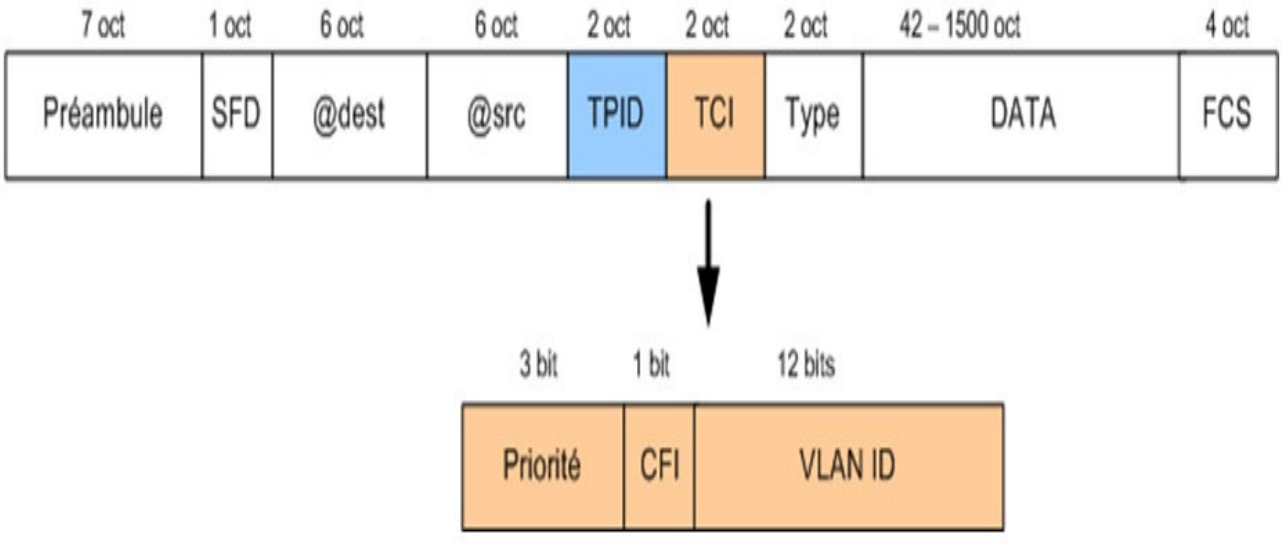


Figure 3.5. *Extension de la trame Ethernet modifiée par la norme 802.1Q.*

✓ **Le champ TPID (*Tag Protocol Identifier*)**

C'est la partie qui détermine le type du tag (0x8100 pour 802.1Q) ce champ est utilisé pour prévoir des évolutions futures afin de pouvoir utiliser le principe du *tagging* pour différentes fonctionnalités.

✓ **Le champ TCI (*Tag Control Information*)**

Cette partie se décline en plusieurs éléments :

- Priorité: niveaux de priorité définis par l'IEEE 802.1P. Ce champ permet de réaliser une priorisation des flux. Le champ étant sur trois bits il est possible de déterminer 7 niveaux de priorité.
- CFI: Ce bit permet de déterminer si le tag s'applique à une trame de type Ethernet ou Token-Ring.
- VID: VLAN identifier. C'est l'identifiant du VLAN. L'appartenance d'une trame à un VLAN se fait grâce à cet identifiant. Le champ étant sur 12 bits, il est donc possible de déclarer jusqu'à 4096 VLANs. (les valeurs 0 et FFF sont réservés)

3.7.3 Le protocole ISL (*Inter Switch Link Protocol*)

Le protocole ISL est un protocole propriétaire Cisco (il ne peut être utilisé qu'entre équipements Cisco) qui date d'avant la création du protocole IEE 802.1Q. ISL encapsule complètement la trame Ethernet en ajoutant un en-tête et un en-queue, en laissant la trame initiale intacte. L'en-tête ISL contient un champ identifient du VLAN et l'adresse MAC de la trame, permettant d'acheminer le paquet vers le routeur et les commutateurs appropriés. Lorsqu'elle atteint le réseau destination, l'en-tête est supprimé et la trame est acheminée vers l'équipement récepteur [25] [20].

3.8 Les protocoles de gestion des VLANs

3.8.1 Le protocole VTP

Pour éviter de redéfinir tous les VLANs existant sur chaque commutateur, Cisco a développé un protocole permettant un héritage de VLANs entre commutateur. C'est le protocole VTP. Ce protocole est basé sur la norme 802.1Q et exploite une architecture client-serveur avec la possibilité d'instancier plusieurs serveurs. [27]

❖ **Comprendre le VTP**

Un commutateur doit alors être déclaré en serveur, on lui attribut également un nom de domaine VTP. C'est sur ce commutateur que chaque nouveau VLAN devra être défini, modifié ou supprimé. Ainsi chaque commutateur client présent dans le domaine héritera automatiquement des nouveaux VLANs créés, modifiés ou supprimés sur le commutateur serveur. [27]

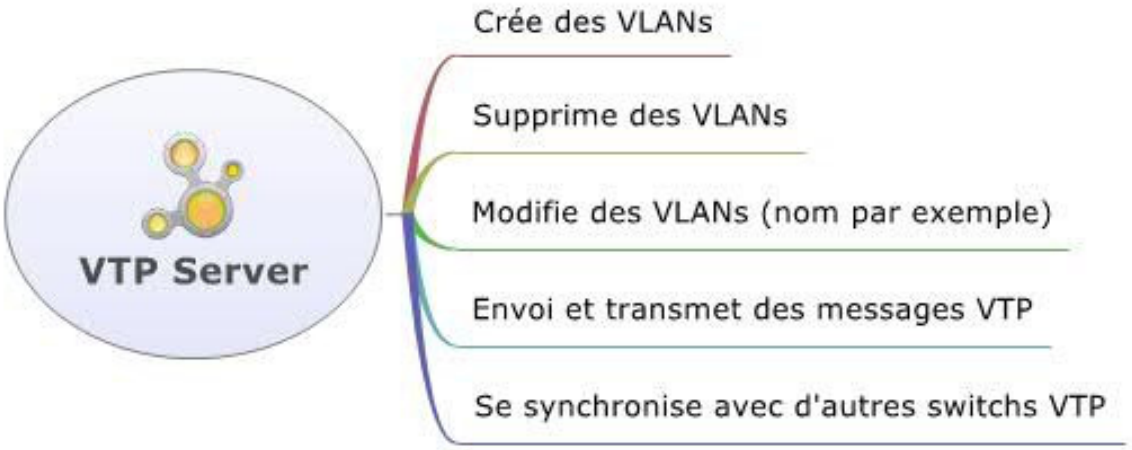
Le VLAN *Trunking Protocol* (VTP) minimise donc l'administration dans le réseau commuté. Ceci réduit avantageusement le besoin de configurer les mêmes VLANs sur chaque commutateur individuellement.

❖ **Architecture du VTP**

Les dispositifs de VTP peuvent être configurés pour fonctionner selon les trois modes suivants [28] :

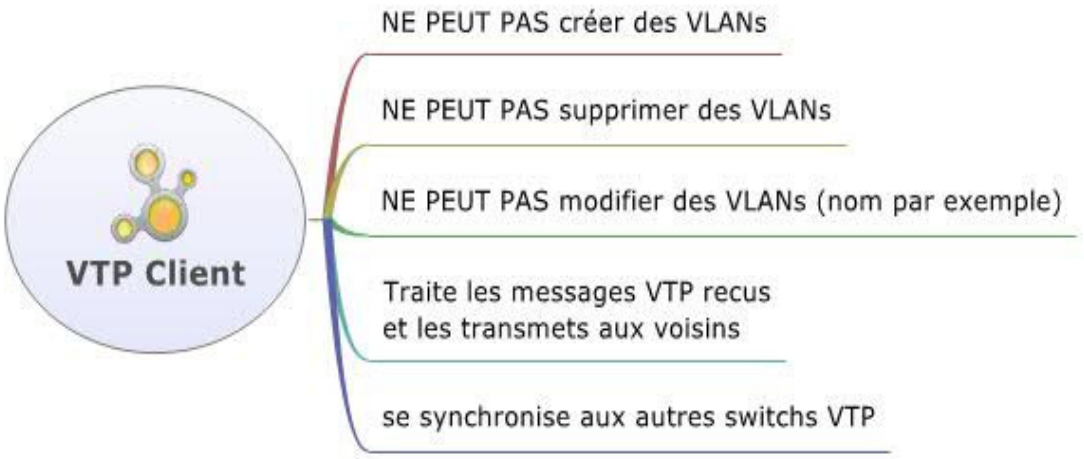
➢ Le mode serveur :

Un commutateur en mode Serveur permet à l'administrateur de faire toute modification sur les VLANs et de propager automatiquement ses modifications vers tous les *switches* du réseau.



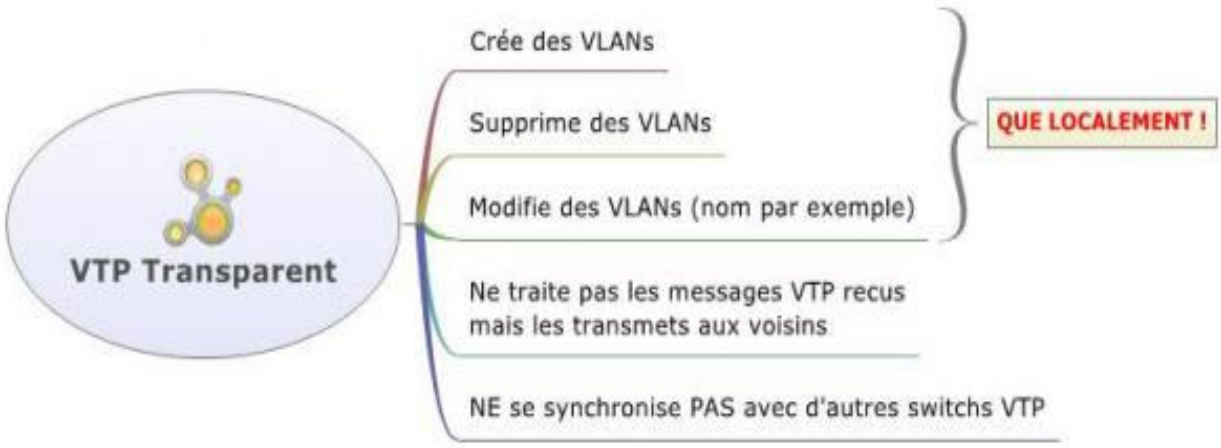
➢ Le mode client :

Un commutateur en mode *Client* ne permet pas à l'administrateur de faire des modifications sur les VLANs. Vous recevez un message d'erreur quand vous essayez de créer un VLAN.



➢ Le mode transparent :

Un commutateur en mode *Transparent* permet à l'administrateur de faire toute modification sur les VLANs en local uniquement et donc ne propage pas ses modifications vers tous les commutateurs du réseau.



3.8.2 Le protocole VMPS

VMPS est un service créé par Cisco. Il est chargé de faire correspondre un VLAN à une ou plusieurs adresses MAC. Pour pouvoir fonctionner et assurer la gestion dynamique des VLANs, le VMPS nécessite l'utilisation du protocole VTP (*VLAN Trunking Protocol*) et du protocole VQP (*VLAN Query Protocol*). [29]

❖ **Comprendre le VMPS**

Le VMPS utilisera le nom du domaine VTP lors de la connexion d'une machine sur le commutateur, puis l'étude du protocole VQP (*VLAN Query Protocol*) permet au *switch* client d'interroger un serveur VMPS qui utilise une base de données contenant les adresses MAC des stations enregistrées et leurs VLANs correspondants. Ainsi le *switch* client pourra associer le port avec le bon VLAN.

Le VMPS est donc basé sur une architecture client/serveur et permet de gérer dynamiquement les assignations de VLAN en fonction d'adresse MAC.

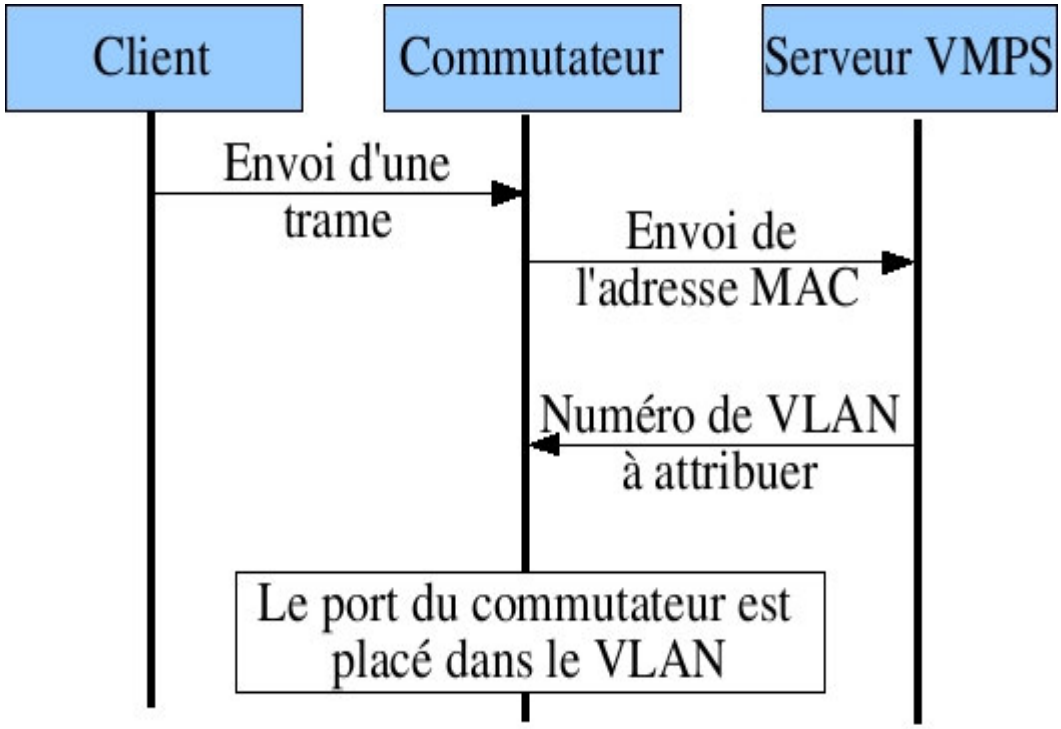


Figure 3.6. *Affectation dynamique d'un client à un VLAN*

3.9 Conclusion

Nous avons vu tout au long de ce chapitre que la technologie des VLANs repose sur des concepts principaux et essentiels tels que la limitation des domaines de diffusion, la mobilité des utilisateurs et la sécurité des réseaux locaux. En effet, cette technologie est une nouvelle manière de mettre à profit la technique de la commutation pour donner plus de flexibilité aux réseaux locaux tout en gardant une sécurité assez fiable et moins couteuse au sein de l'entreprise.

Après avoir étudié l'architecture actuelle du réseau local de l'EPB, et après avoir vu en théorie les VLANs dans les chapitres précédents, nous allons implémenter notre solution

proposée qui consiste à créer de différents VLANs au sein de l'entreprise en exposant les différentes configurations nécessaires, tout cela sera abordé dans le chapitre suivant.

CHAPITRE 4 : REALISATION

4.1 Introduction

Ce présent chapitre consistera à mettre en œuvre la solution proposée pour la réalisation de notre projet, en exposant les différentes configurations nécessaires à implémenter sur le LAN. Ces configurations entourent entre la configuration des VLANs, VTP, STP et En se basant sur le simulateur Cisco packet tracer.

Pour présenter les configurations que nous avons réalisées, nous nous sommes servis des captures d'écran qui illustrent les étapes de la configuration afin d'éclaircir chaque composant de cette dernière et son fonctionnement. Enfin, des tests de validation pour confirmer le bon fonctionnement du réseau, seront réalisés.

4.2 Présentation du simulateur Cisco « Packet Tracer »

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

4.3 Segmentation des VLANs

L'organisation réseau se fera de manière à optimiser le trafic en la segmentant à l'aide des VLANs. Chacune de ces 4 directions à savoir, la direction générale, direction domaine et développement, direction des systèmes d'information et la direction remorquage représente un VLAN. Un VLAN pour la téléphonie et un autre pour les Caméras de surveillance. Par conséquent, il y'aura naissance de 6 VLANs à savoir :

- Direction Générale **D.G**
- Direction Domaine et Développement **D.D.D**
- Direction des Systèmes d'information **D.S.I**
- Direction Remorquage **D.R**
- La téléphonie **Telephonie**
- Les vidéos de surveillances **Videos.S**

4.4 Plan d'adressage

Un réseau ne peut fonctionner sans une attribution et une configuration correcte de différentes adresses. Le plan d'adressage est la stratégie qui s'applique afin de permettre l'accessibilité des différentes entités d'un réseau de la manière la plus optimale.

Le premier objectif du plan d'adressage est d'éviter la duplication accidentelle des adresses, c'est-à-dire, il permet de désigner un équipement sans ambigüité, car une adresse IP affectée ne doit être réutilisée.

L'élaboration d'un plan d'adressage nécessite la prise en considération de certaines règles, telle que la classe d'adressage, la définition de sous-réseau, l'attribution statique et/ou dynamique des adresses.

- **Adressage des VLANs**

L'adresse du réseau est 192.168.0.0/24 avec une possibilité de création de 255 sous-réseaux, avec un masque 255.255.255.0

L'adressage du réseau local et de toutes les stations, se basera sur une adresse privée et à partir de cette dernière que l'affectation des adresses IP pour l'ensemble des équipements et des VLANs va être accomplie. Les machines affiliées à un VLAN, vont prendre toute les adresses IP d'une même adresses sous-réseau. Le tableau suivant montre le plan d'adressage des VLANs.

Nom VLAN	Vlan-id	Adresse sous réseau
D.G	10	192.168.10.0/24
D.D.D	20	192.168.20.0/24
D.S.I	30	192.168.30.0/24
D.R	40	192.168.40.0/24
Telephonie	50	192.168.50.0/24

Video.S	60	192.168.60.0/24

Tableau 4.1. *Plan d'adressage des VLANs*

4.5 présentation de l'architecture réseau avant la configuration

La figure 4.1 illustre notre architecture réseau que nous allons réaliser sous le simulateur packet tracer

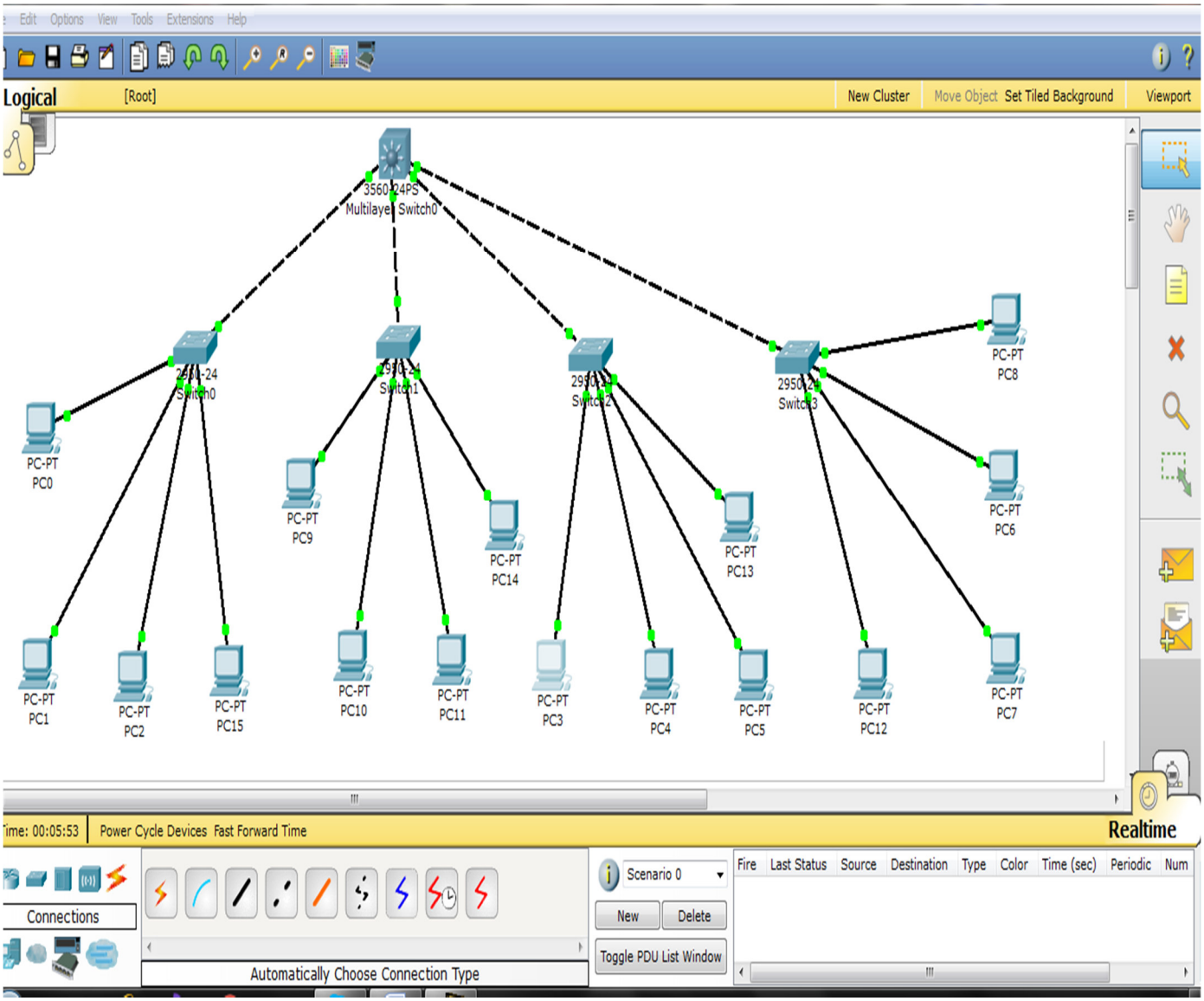


Figure 4.1. *Présentation de l'architecture*

4.6 Interface commande de Packet Tracer

Toutes les configurations des équipements du réseau seront réalisées au niveau de CLI (Commande Langage Interface). CLI est une interface de simulateur 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.

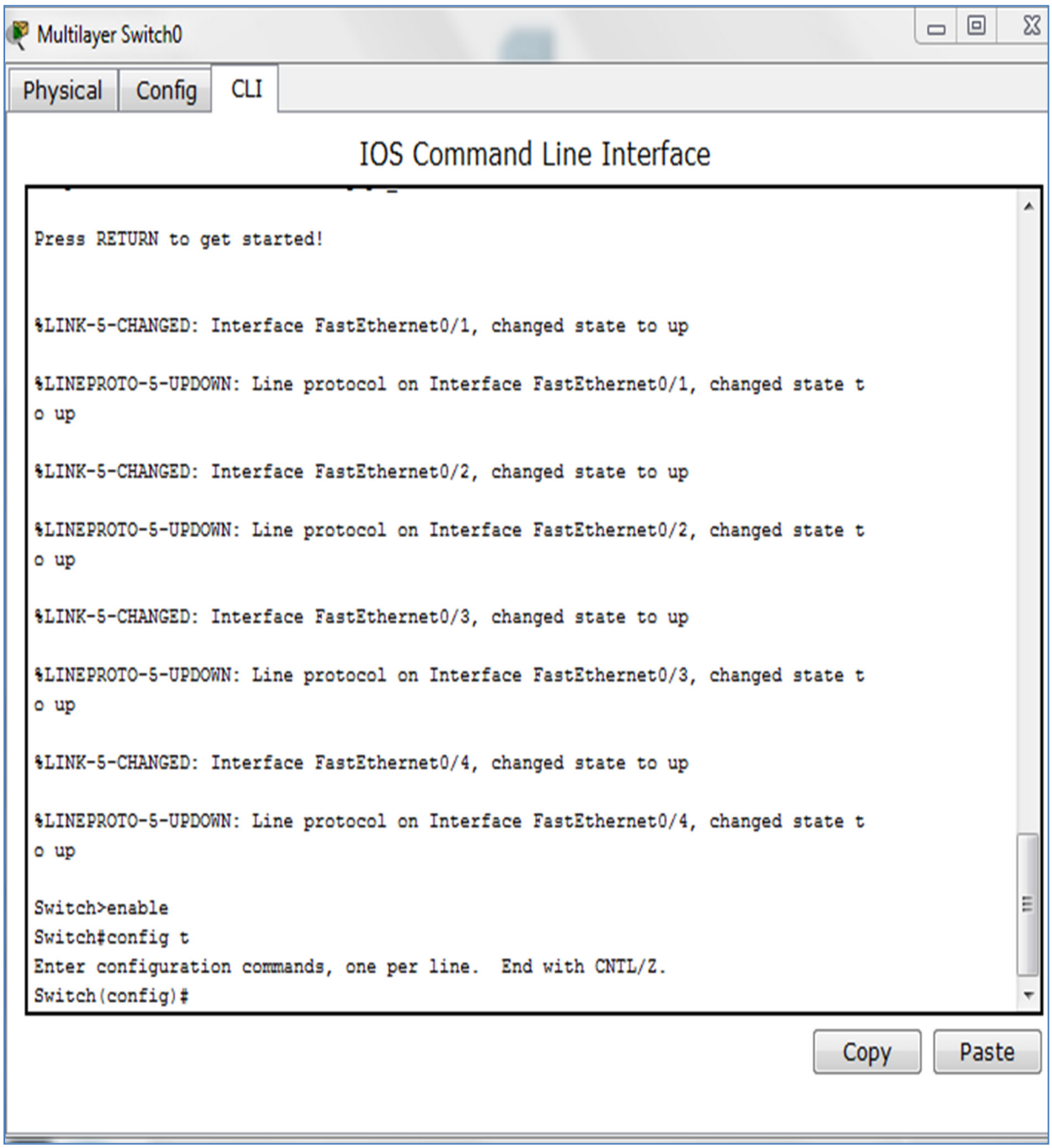


***Figure 4.2**. Interface CLI*

4.7 Configuration des équipements

La configuration des équipements du réseau sera au niveau des commutateurs de niveau 2 et niveau 3 constituants le réseau local des stations En effet, une série de configuration a été réalisée à travers ces équipements, en montrant un exemple de chaque configuration.

4.7.1 Sécuriser l'accès aux périphériques

Il faut savoir qu'IOS (International Standardization Organization) utilise des modes organisés hiérarchiquement pour faciliter la protection des périphériques. Dans le cadre de ce dispositif de sécurité, IOS peut accepter plusieurs mots de passe, ce qui nous permet d'établir différents privilèges d'accès au périphérique.

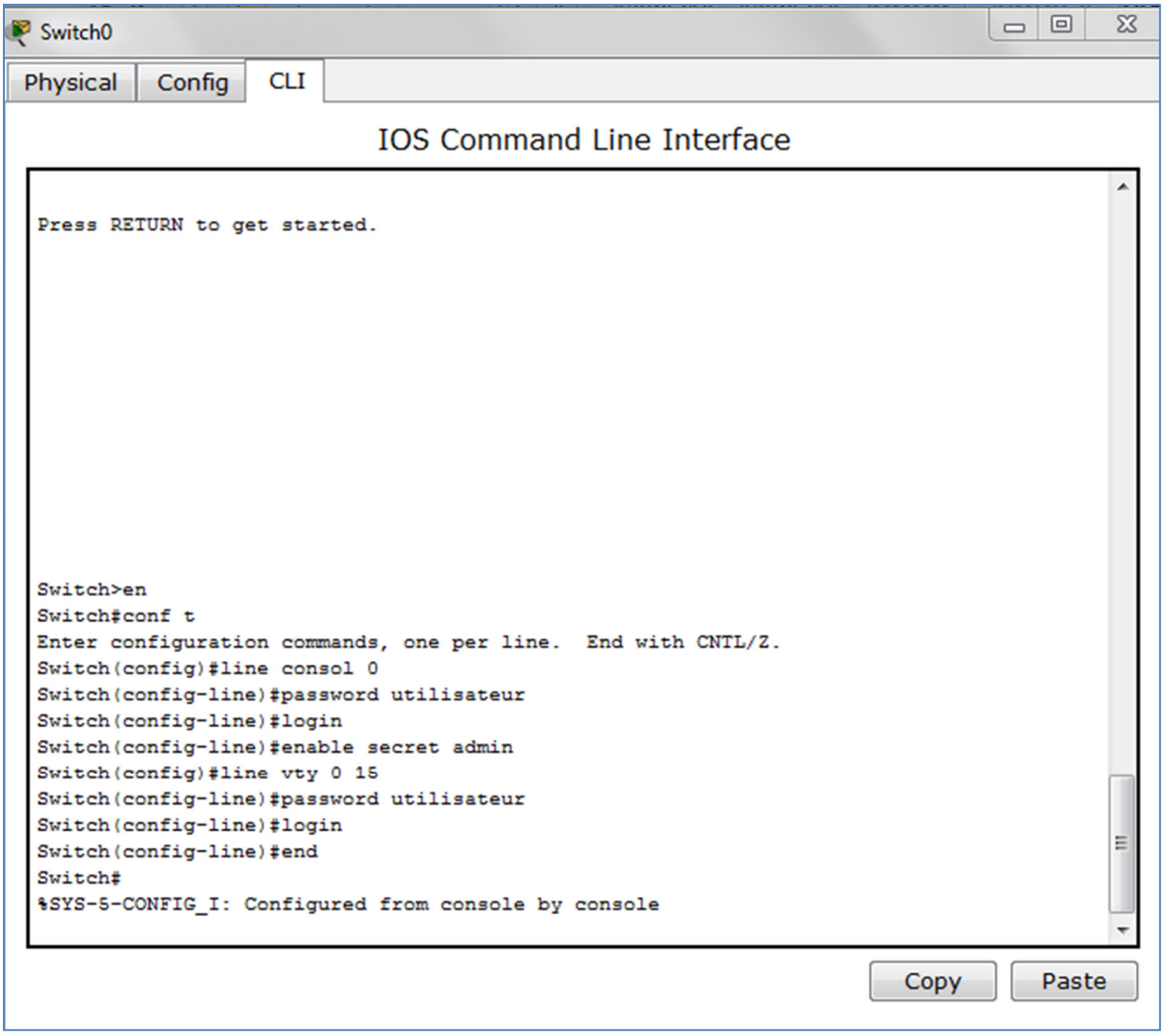


Figure 4.3. *Configuration du mot de passe*

4.7.2 Configuration du protocole VTP

- Le commutateur cœur de LAN sera configuré comme un serveur –VTP. Donc, c'est lui qui gère l'administration de l'ensemble des VLANs. Un nom de domaine est attribué. La (figure 4.4) représente la configuration du serveur VTP au niveau de Switch multifonctions.

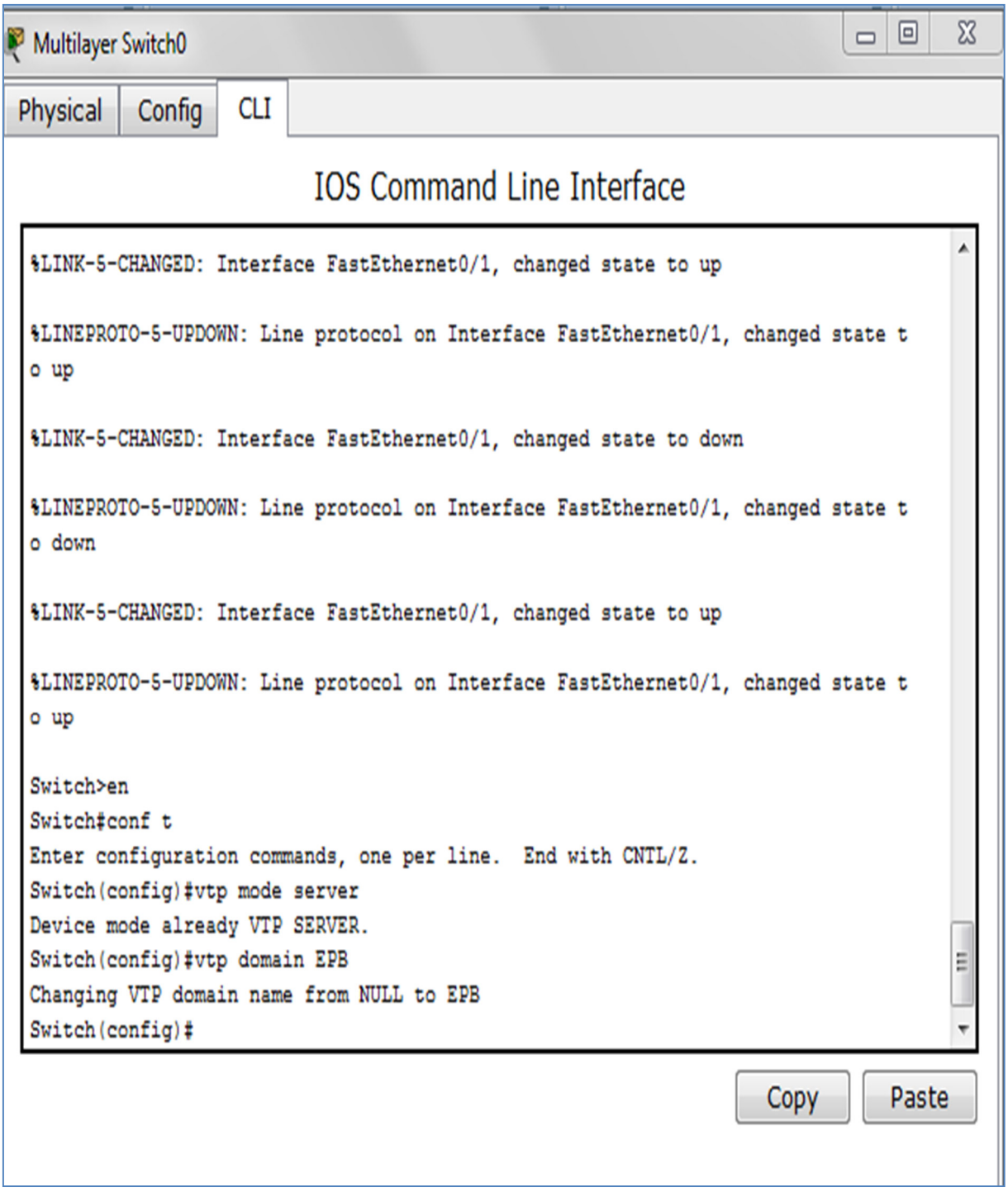


Figure 4.4. *Configuration VTP-server*

- La configuration des clients-VTP sera au niveau de tous les commutateurs Accès.

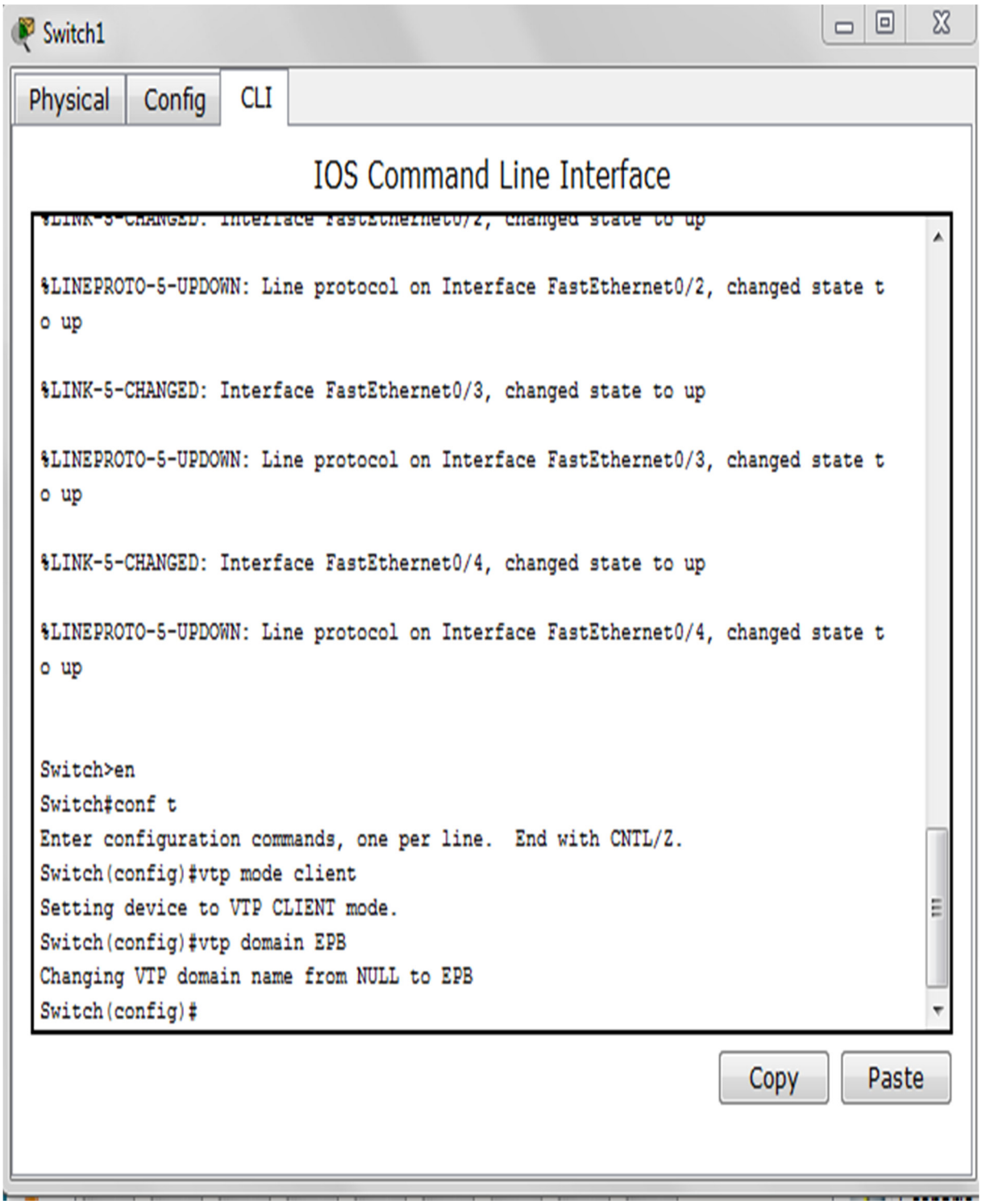


Figure 4.5. *Configuration VTP-client*

4.7.3 Création des VLANs

La création des VLANs est faite au niveau des commutateurs multifonction (server VTP) comme le montre la figure 4.6

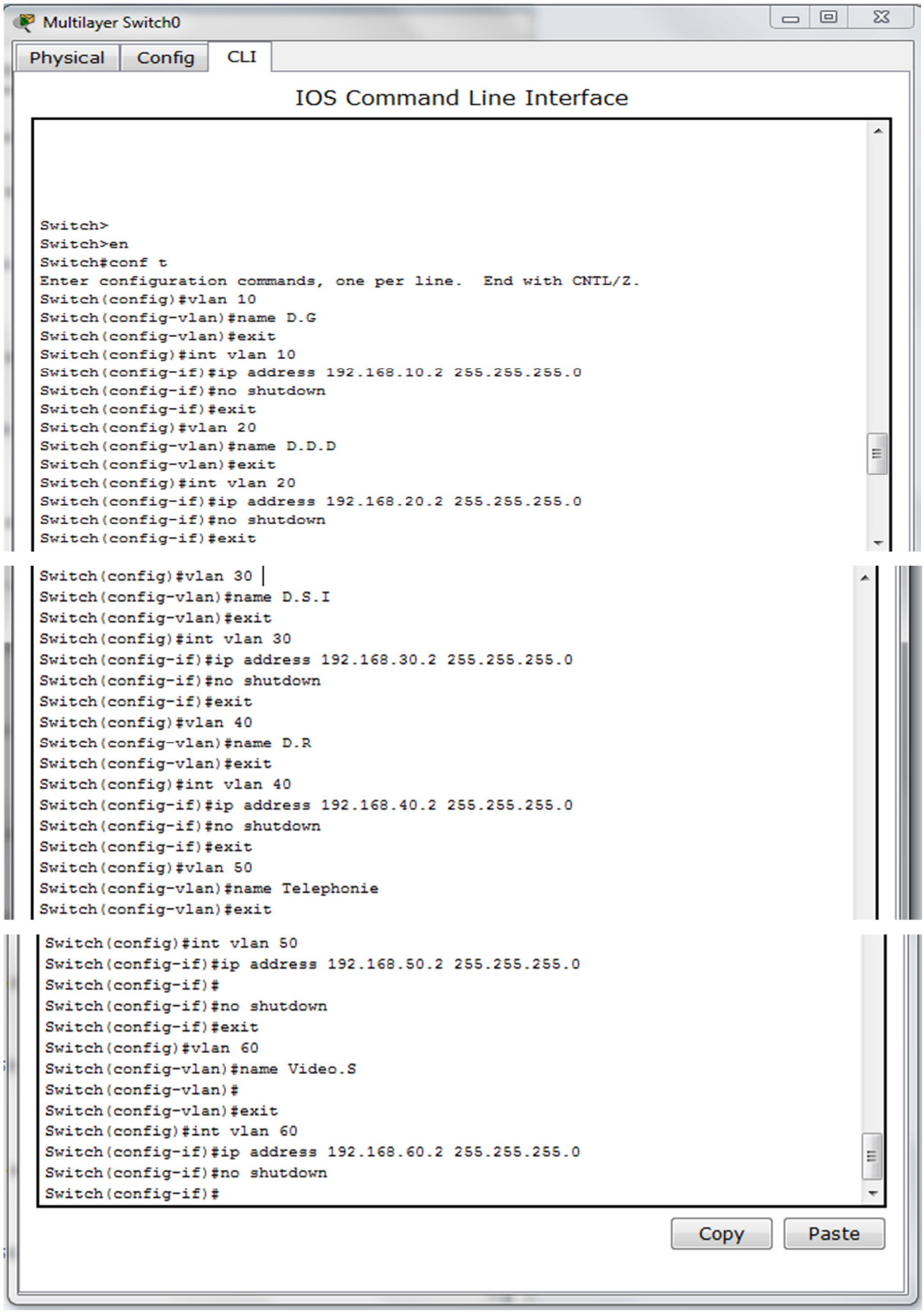


Figure 4.6. *Configuration des VLANs sur le serveur VTP*

4.7.4 Configuration des liens trunk

Les interfaces des équipements d'interconnexion à configurer en mode trunk, existent toutes entre l'ensemble des commutateurs Accès et le commutateur cœur. Les commandes suivantes nous permettent d'associer un port à un vlan en mode trunk en s'aidant de la commande range qui pourra réunir toutes les interfaces en une seule fois.

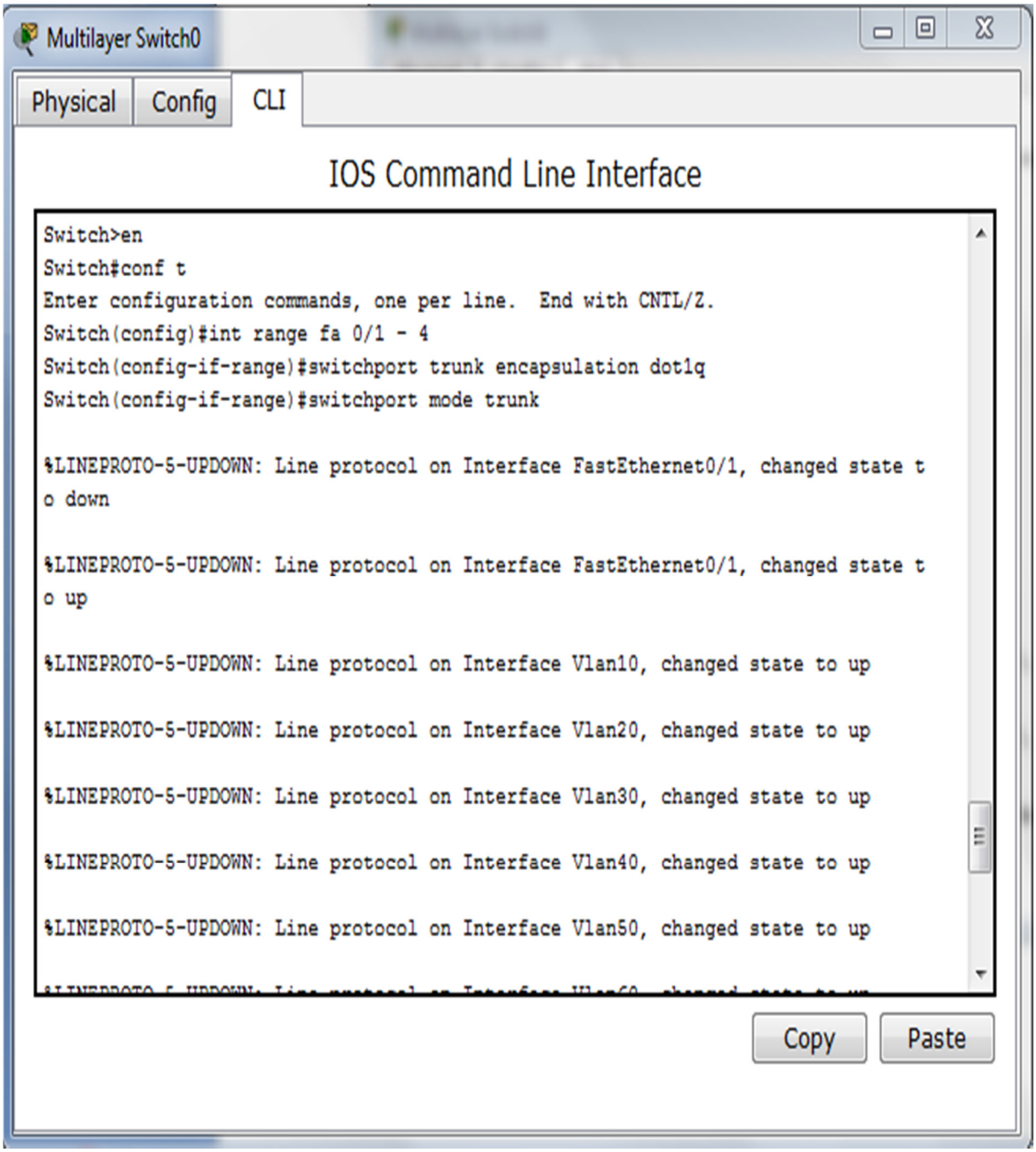


Figure 4.7. *Configuration des liens trunk.*

4.7.5 Attribution des ports des commutateurs au VLANs

C'est au niveau de chaque commutateur Accès que les ports vont être assignés aux différents VLANs existant. En effet, chaque port d'un commutateur appartiendra à un VLAN donné. Les commandes suivantes nous permettent d'associer un port à un VLAN en mode Accès. Figure 4.8

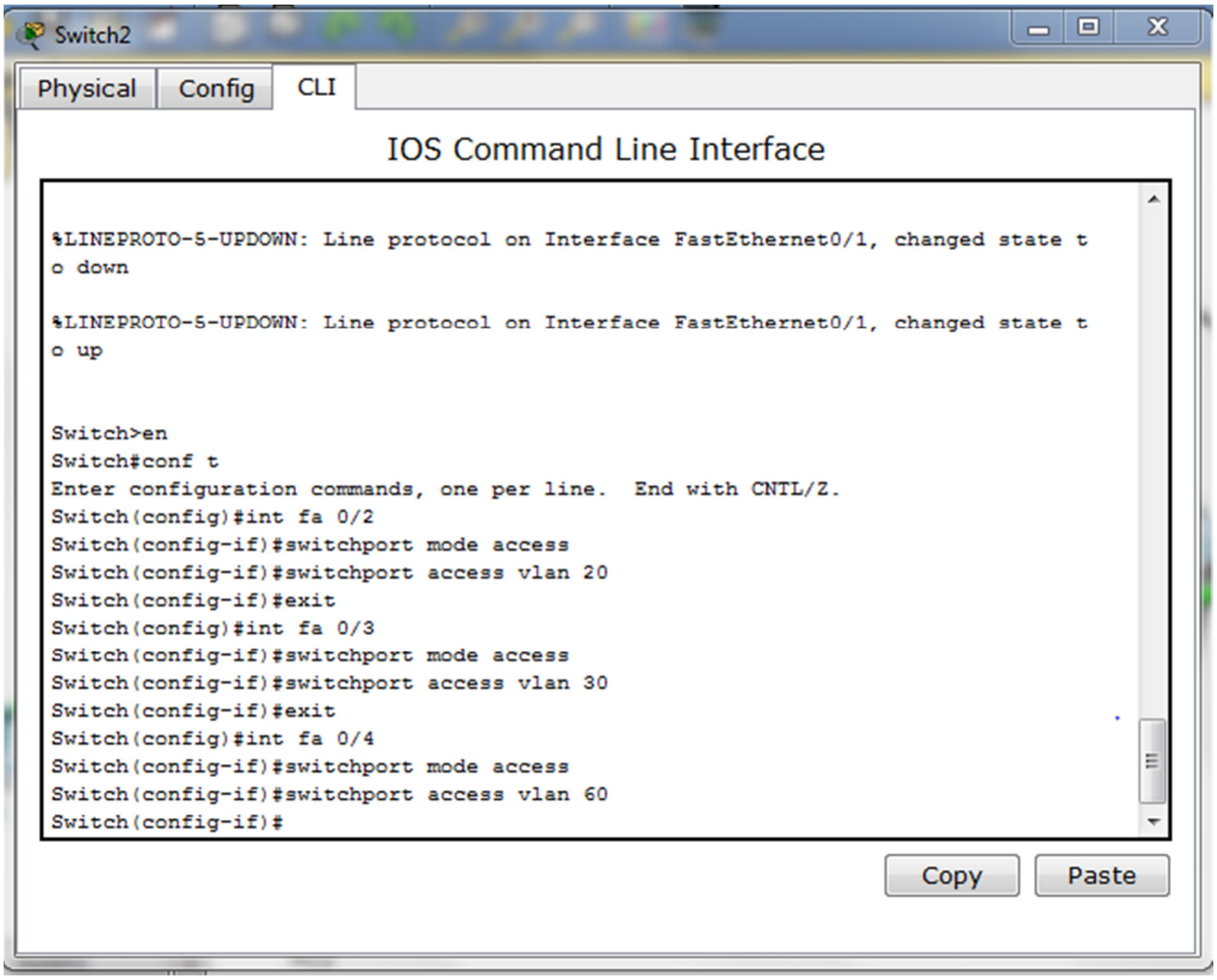


Figure 4.8. *Attribution des ports aux VLANs*

4.7.6 Configuration de DHCP

Afin de simplifier à l'administrateur la gestion et l'attribution des adresses IP, on utilise le protocole DHCP qui permet de configurer les paramètres réseaux client, au lieu de les configurer sur chaque ordinateur client. La figure 4.9 illustre les commandes qui nous permettent de configurer ce protocole au niveau du serveur

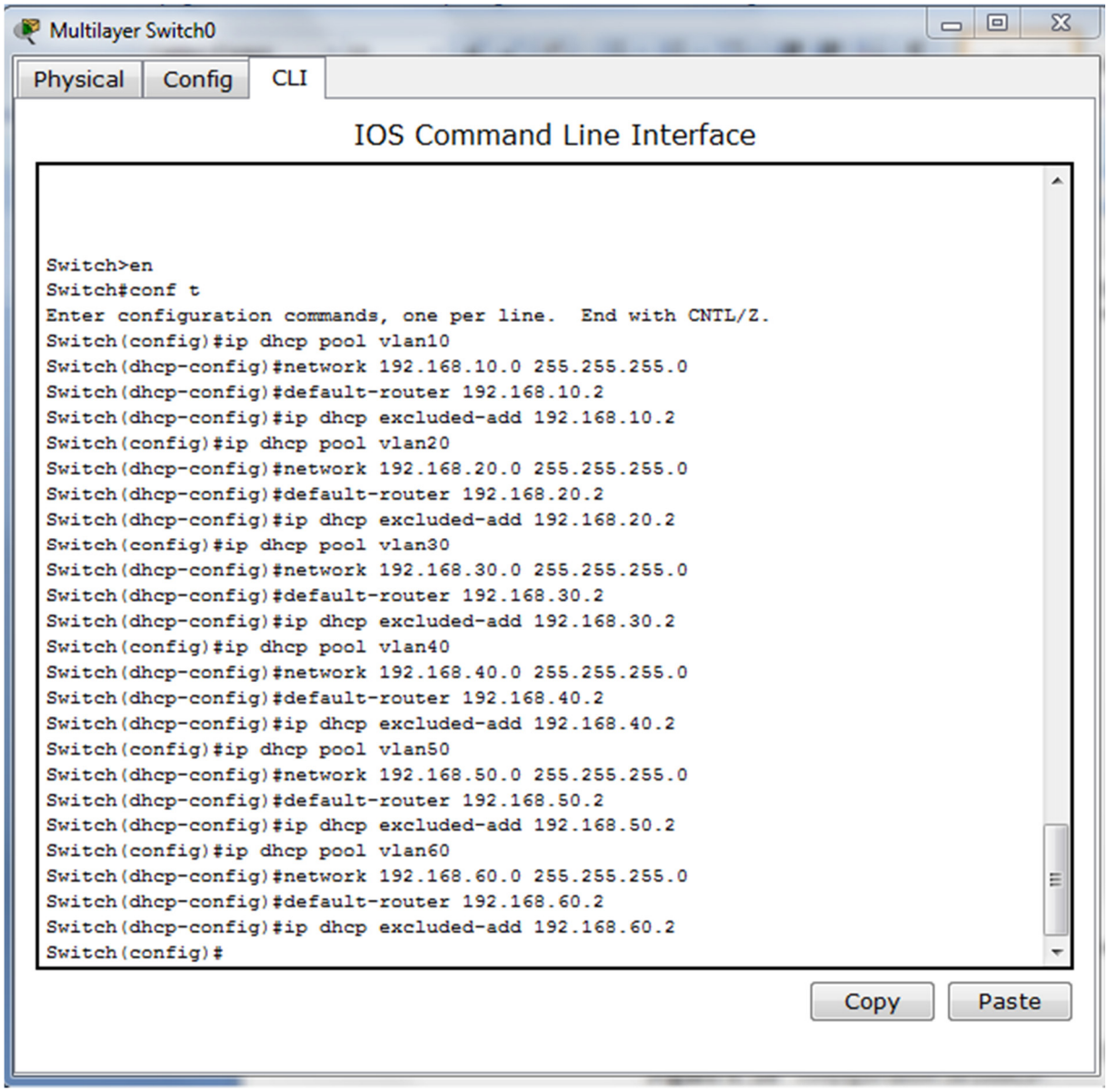


***Figure 4.9**. Configuration de DHCP.*

Apres la configuration DHCP du serveur place au PC la figure 4.10 montre notre configuration :

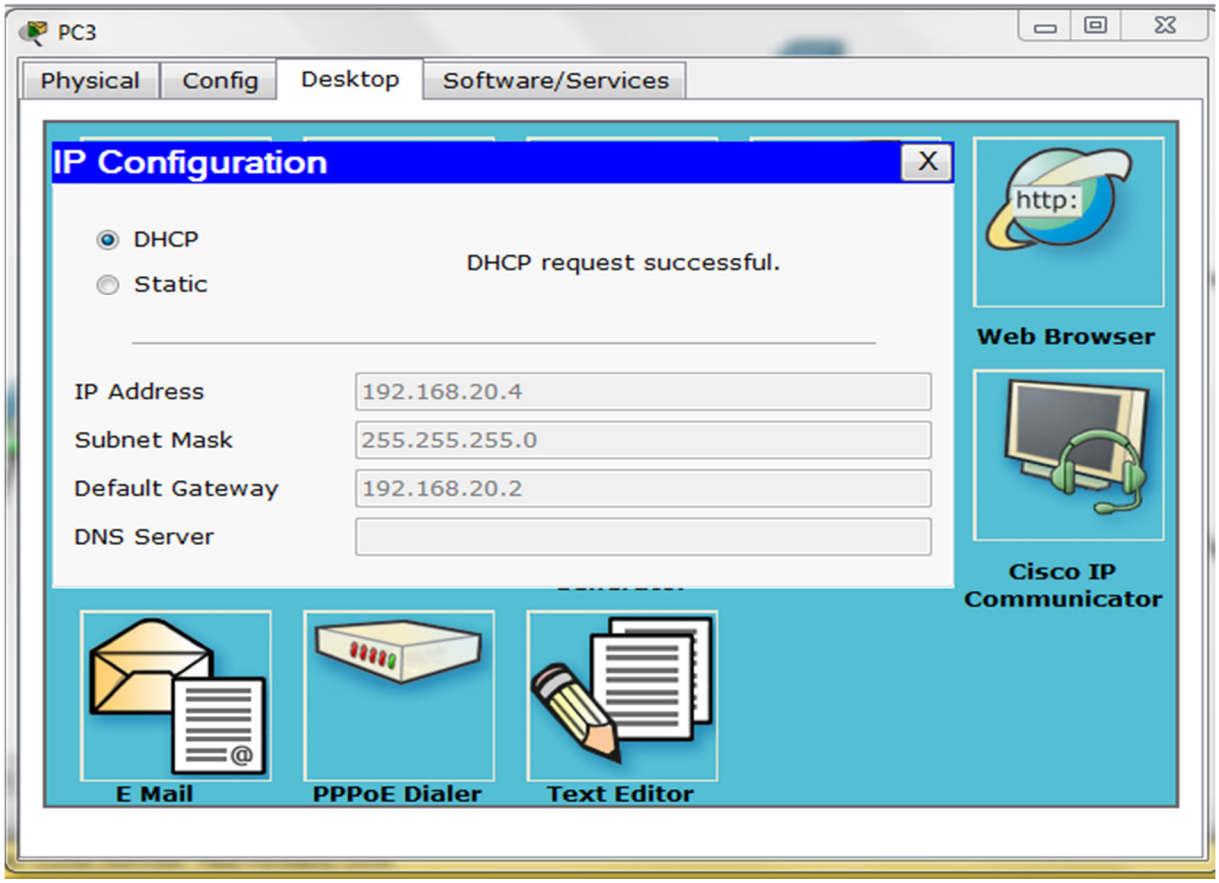


Figure 4.10. *DHCP sur PC*

4.7.7 Configuration de STP

La figure 4.11 illustre les commandes qui nous permettent de configurer le protocole STP, ainsi affecter un root primaire ou secondaire à un VLAN.

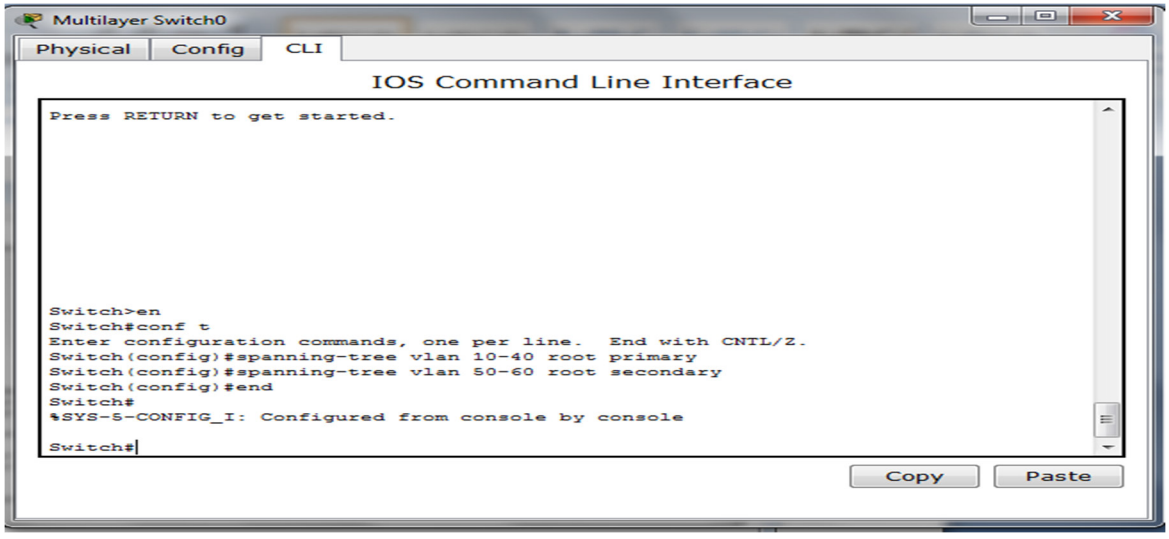


Figure 4. 11. *Configuration du STP.*

4.8 Vérification et test de validation

4.8.1 Vérification

Dans cette partie nous avons vérifié la configuration de tous les équipements à l'aide des commandes de vérification.

4.8.1.1 Contrôle de la bonne configuration du VTP

- VTP serveur en utilisant la commande *#show vtp statu* sur le switch multilayer figure 4.12

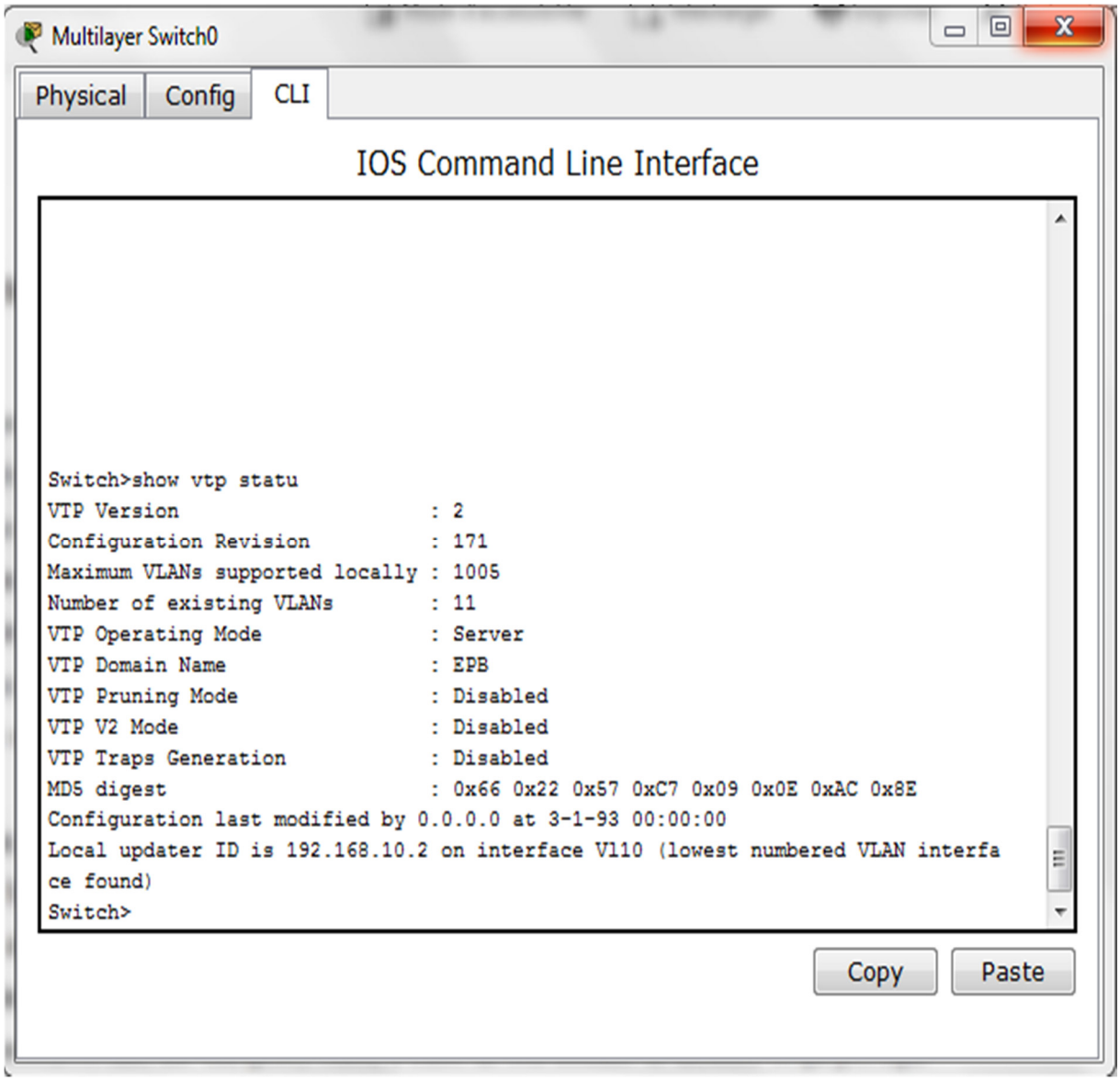


Figure 4.12. *Contrôle de la configuration vtp server.*

- VTP client en utilisant la commande *#show vtp statu* sur le switch1 (suitch accès) figure 4.13

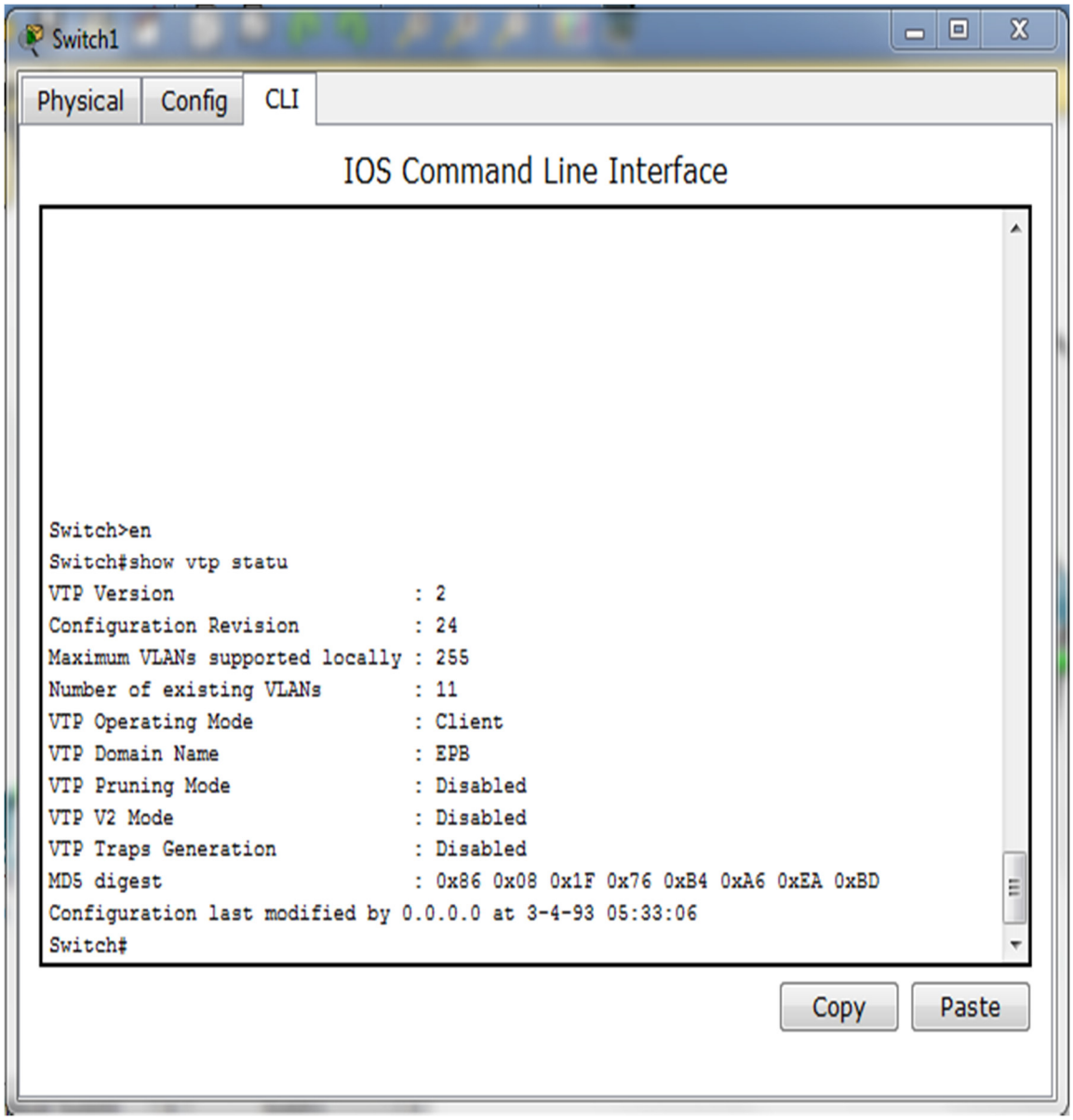


Figure 4.13. *Configuration vtp client.*

4.8.1.2 Contrôle des réseaux locaux virtuels créent sur le Switch server si ont été distribués sur les Switch clients

Apres avoir vérifié les VTP, nous allons passer à la vérification de la distribution des VLANs dans les switches client, nous nous sommes servis de la commande *#show vlan brief* figure 4.14

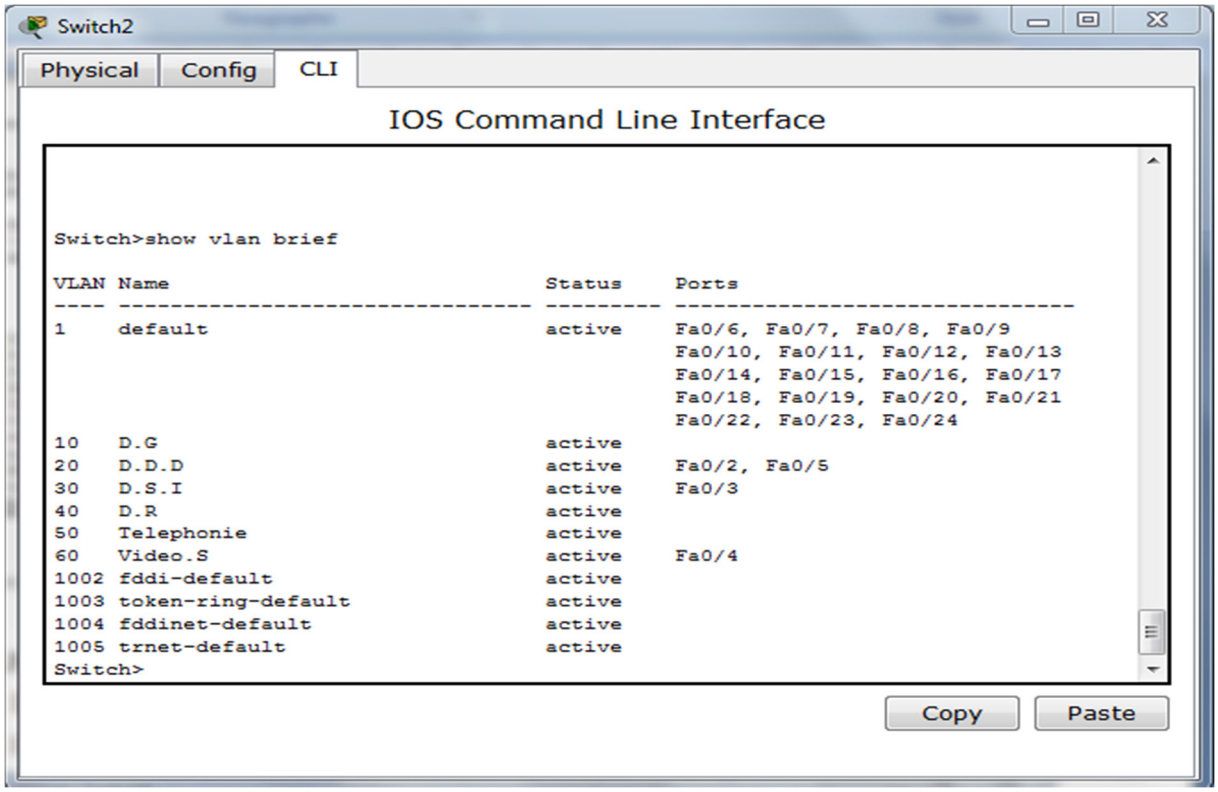


Figure 4.14. *VLANs distribué dans le Switch2 client*

4.8.1.3 Vérification de la distribution des adresses IP avec le DHCP

- Il est possible de vérifier que chaque poste a bien récupéré une adresse DHCP à l'aide de la commande # *show ip dhcp binding* :

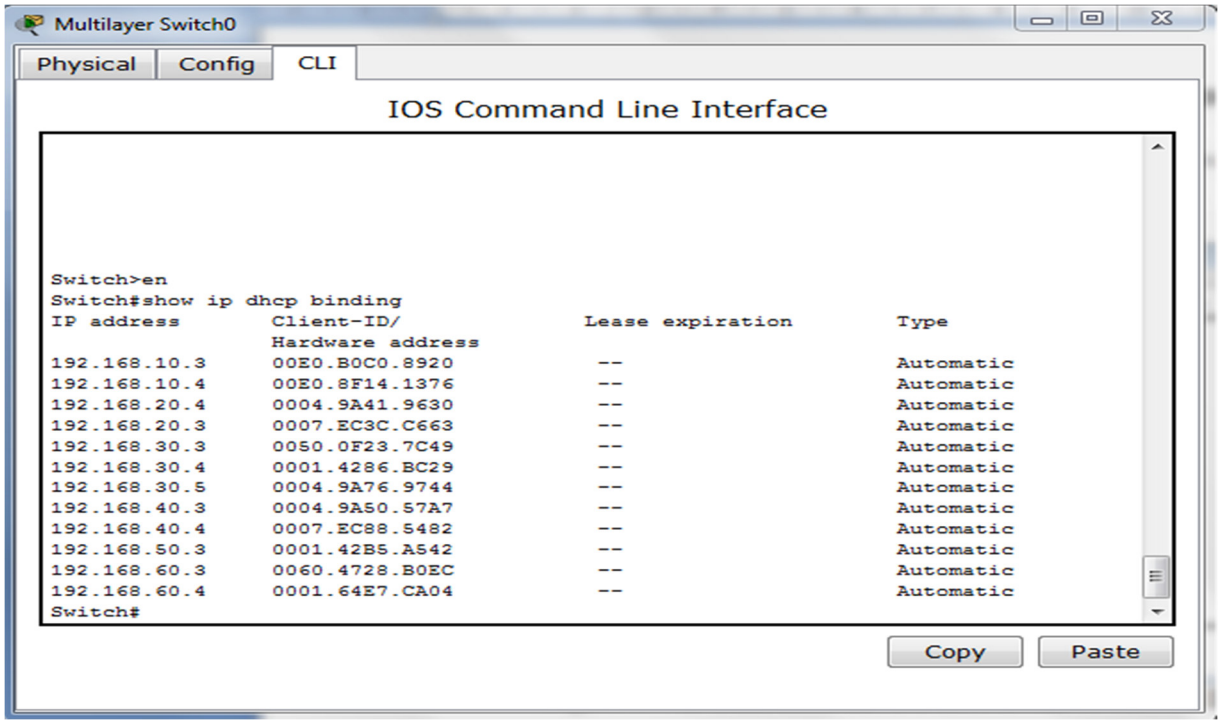


Figure 4.15*. L'attribution des adresses IP sur le serveur DHCP*

- Comme on peut faire la vérification des adresses IP des PC attribue par le DHCP en accédant à « ip configuration » des postes**.** La figure 4.16 montre l'attribution des adresses IP par le DHCP

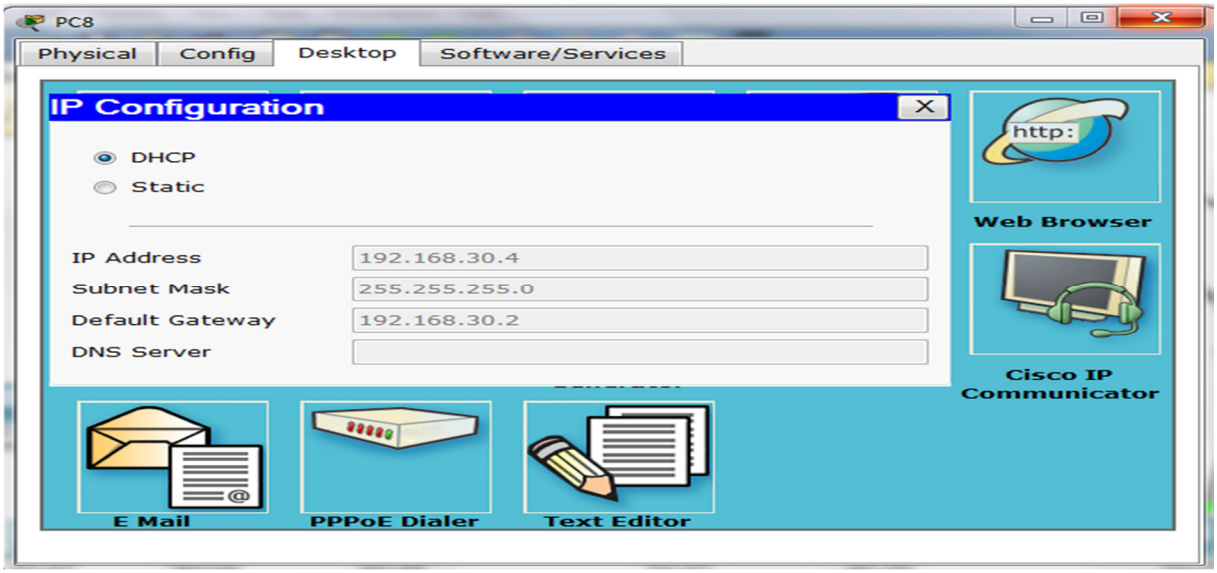


Figure 4.16. *Attribution des adresses IP par le DHCP*

4.8.2 Teste de validation

- **Teste 1** : ce teste sera le ping sur le VLAN 10 (D.G) à partir du PC9 (192.168.10.1) en essayant d'accéder au PC12 (192.168.10.3) qui correspond toujours au VALN 10 (D.G) et qui est sur le même switch que le PC9.

  Nous remarquons que les deux postes se communiquent entre eux. Le résultat du Ping est illustré dans la figure suivante(Fig4.17)

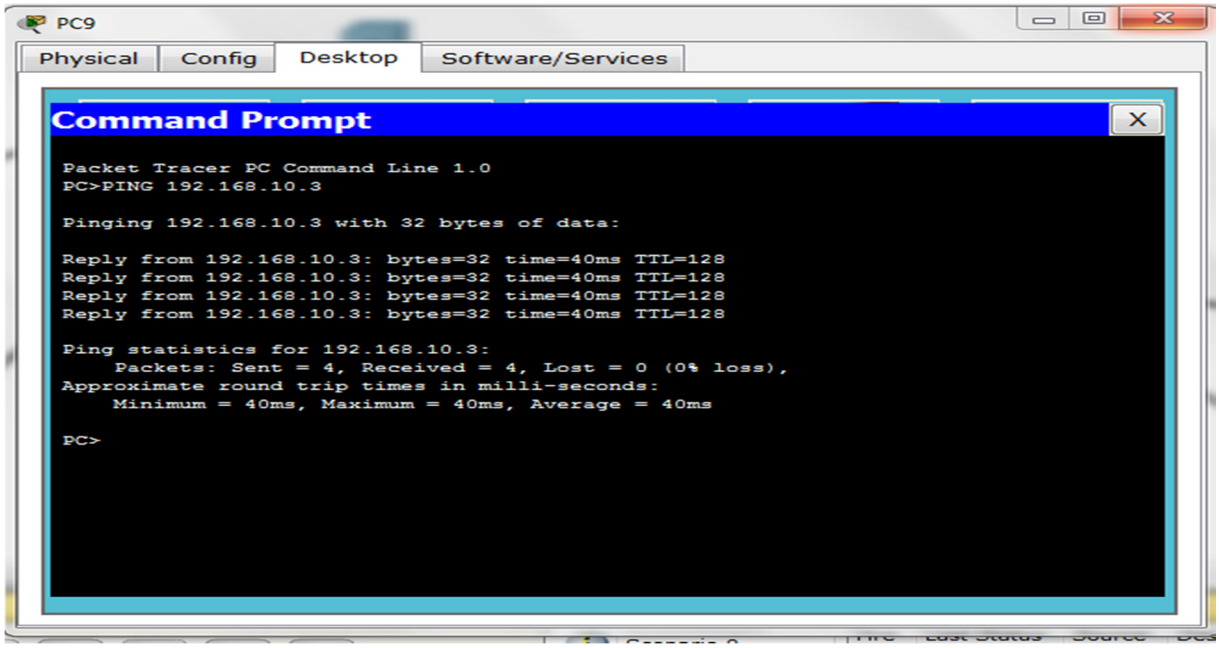


Figure 4.17*. Ping entre deux postes de même VLAN dans le même switch.*

- **Teste 2** : Les deux postes sont connectés à un même VLAN mais qui sont dans de différents switches, ce teste sera le ping sur le VLAN 30 (D.S.I.), à partir du PC2 (192.168.30.3) en essayant d'accéder au PC4 (192.168.30.5) qui correspond toujours au VALN (D.S.I) et qui est sur un switch différent que celui du PC2

  Nous constatant que les deux postes se communiquent entre eux. Le résultat du Ping est illustré dans la figure suivante(Fig4.18)

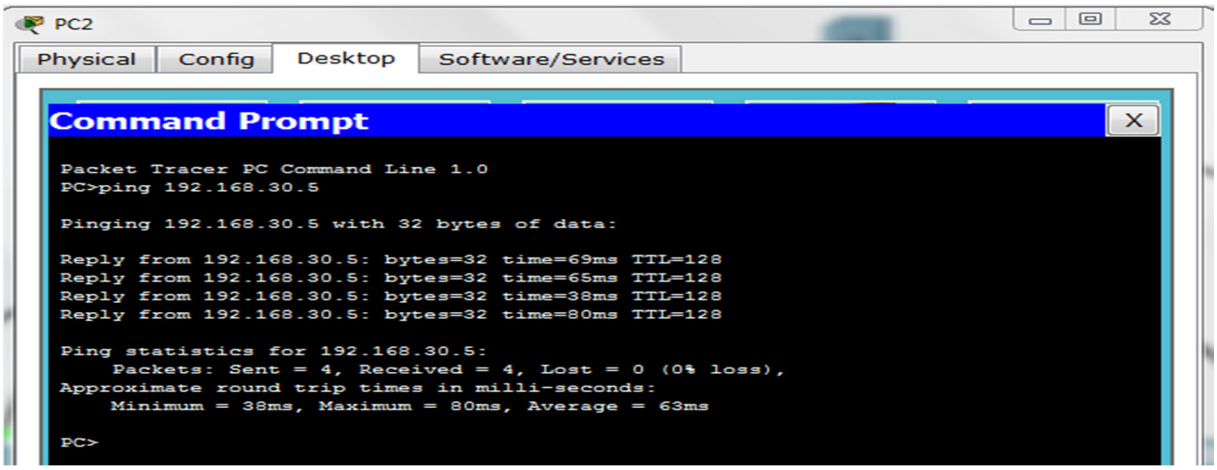


***Figure 4.18**. Ping entre deux postes de même VLAN dans différents switches.*

- **Teste 3** : les deux postes sont connectés à deux VLAN et deux switches différents

Ce troisième test sera le ping sur le VLAN 50(Telephonie) à partir du VLAN 40(D.R), le PC7 (192.168.40.1) qui appartient au VLAN 40, et le PC11(192.168.50.3) qui appartient au VLAN 50.

Nous remarquons qu'il n'y a pas de communication entre les deux postes. Les résultats sont présents dans la figure ci-dessous (Figure 4.19) :

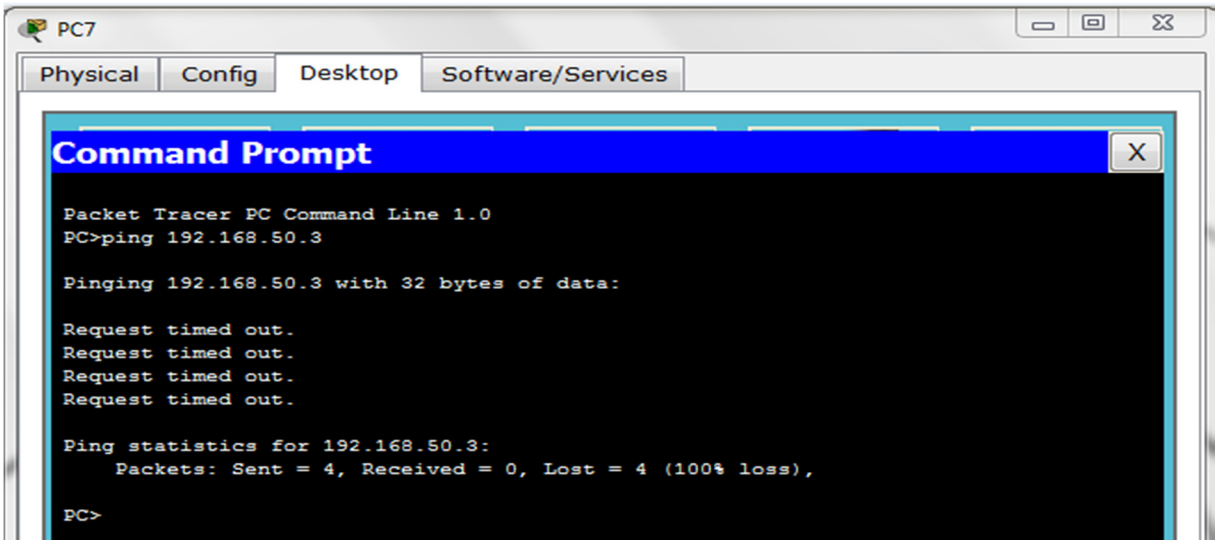


***Figure 4.19**. Ping entre deux postes de différent VLAN dans différents switches*

Teste 4 : tester la communication entre les machines des différents VLANs et d'un même switch. On fait le ping à partir du PC4 (192.168.30.5) qui appartient au VLAN 30(D.S.I) sur le PC5 (192.168.60.3) qui appartient au VLAN 60(Video.S) et qui est relié au même Switch où se trouve le PC4.

Nous remarquons communication entre les deux postes n'est pas établie. Les résultats sont présents dans la figure ci-dessous (Figure 4.20)

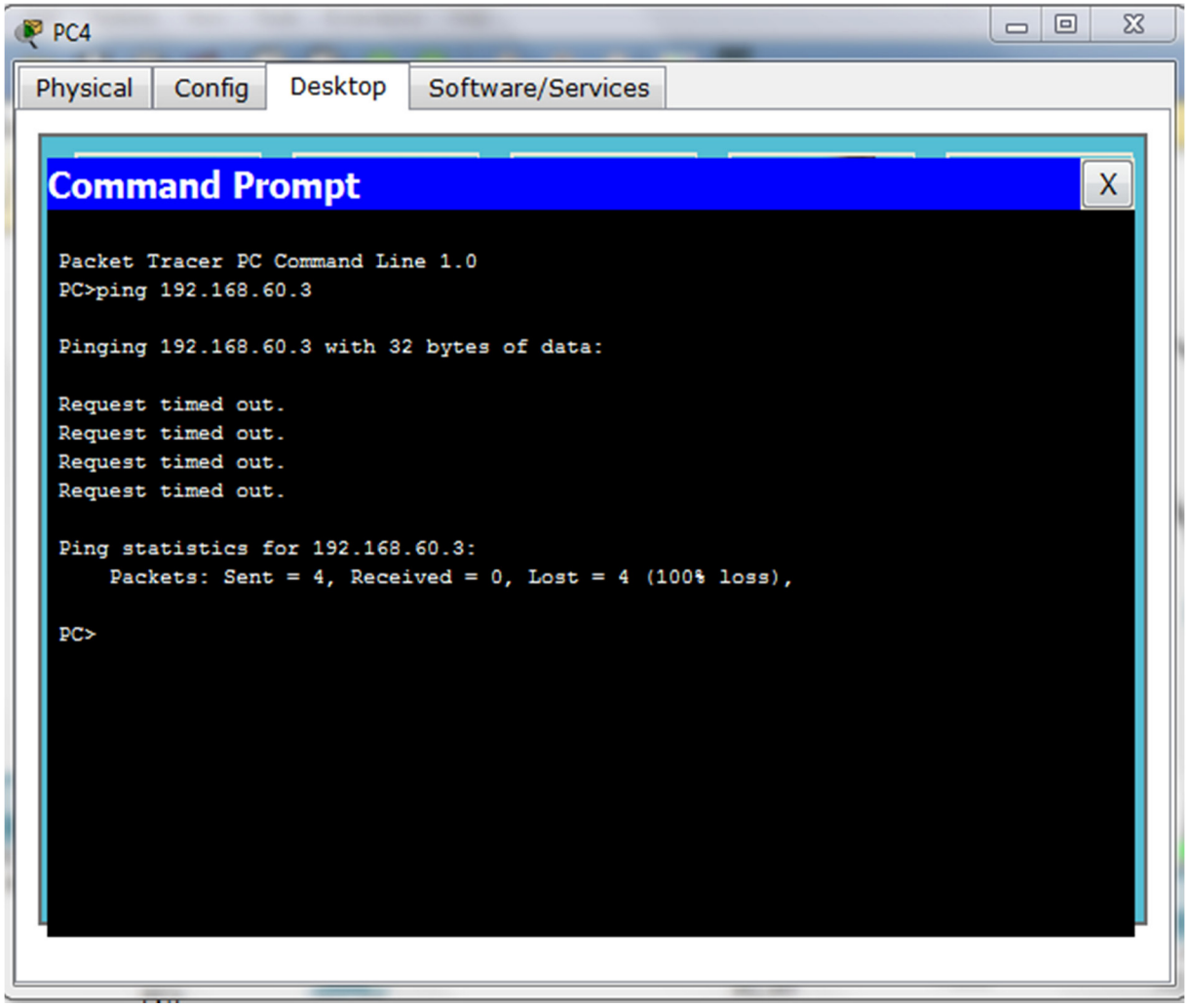


***Figure 4.20**. Ping entre deux postes de différent VLAN dans le même switch.*

Dans ces tests, nous avons montré que les barrières entre les différents VLANs sont infranchissables. En effet, nous avons constaté d'après les tests qu'il n'y a pas de communication entre les stations qui n'appartiennent pas au même réseau virtuel, donc l'objectif qui est la sécurité d'un réseau est atteint.

Pour permettre la communication inter-VLANs, nous devons configurer le switch fédérateur (qui doit être de niveau 3).

4.8.3 Le routage Inter-Vlan

- Pour autoriser la communication entre des stations de différents VLANs, il faut activer la fonction du routage inter-vlan et cela en utilisant la commande # *ip routing* sur le switch server.

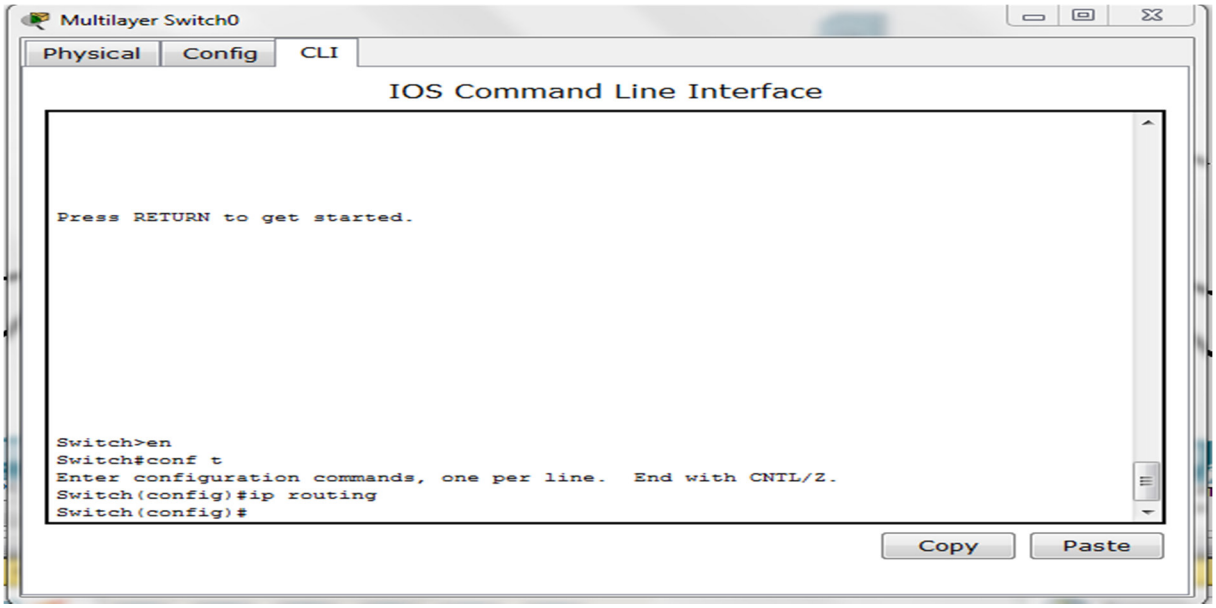


Figure 4.21. *Le routage inter-vlan*

- **Teste de communication inter-vlan**

  A ce stade, vérifiant l'accessibilité des différents équipements qui sont dans deux VLANs distincts. A partir du PC0 (192.168.20.3) qui appartient au VLAN 20 (D.D.D) en asseyons d'accéder au PC14 (192.168.50.4) qui est sur le VLAN 50 (Telephonie). La figure 4.22 illustre le succès du teste effectué sur la communication entre les différents VLANs

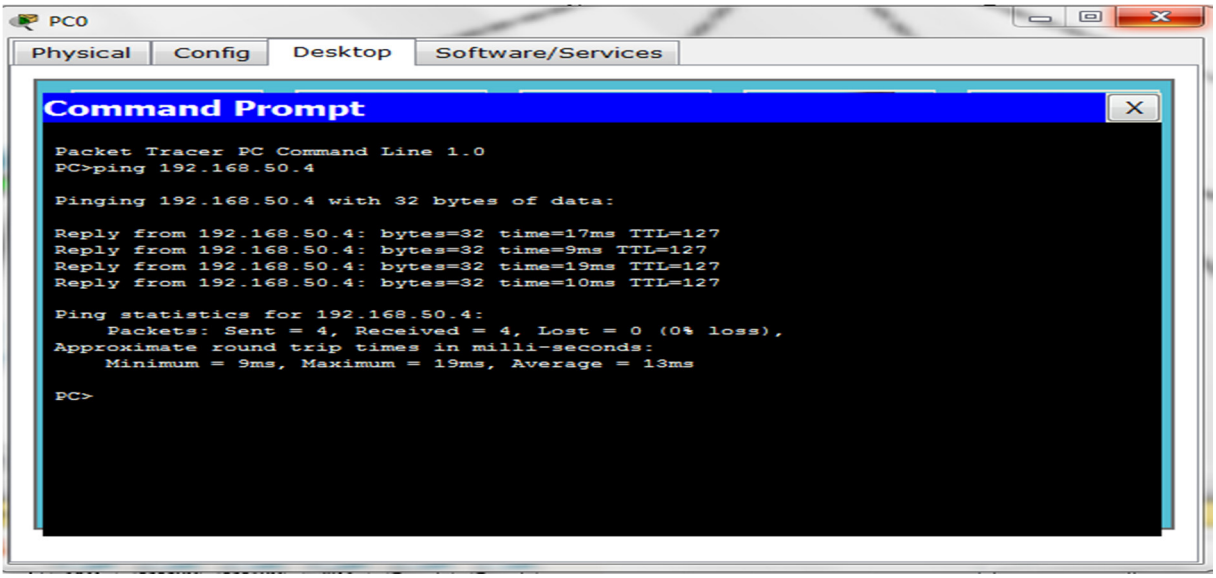


Figure 4.22. *ping entre deux postes de différents VLANs après le routage inter-valn*

4.9 Conclusion

Après avoir présenté une brève description de l'environnement de développement de réseau local, nous avons mis l'accent sur la présentation de quelques interfaces, qui porte sur l'ensemble des configurations, la mise en place du réseau LAN que nous avons réalisé, puis nous avons effectué un ensemble de tests de validation afin de prouver la fiabilité du réseau.

Conclusion générale

Nous avons tenté à travers ce mémoire d'apporter une nouvelle solution pour l'amélioration de la sécurité et les performances du réseau contre les surcharges rencontrées par les utilisateurs de l'EPB. Comme nous l'avons constaté, le personnel de l'EPB est constitué de plusieurs services, à savoir la direction des systèmes d'information, la direction domaine et développement, la direction remorquage, etc. Pour cela, il y a eu lieu de sécuriser le réseau intranet de l'EPB en organisant ces derniers dans des sous réseaux distinctes. Notre démarche a donc consisté à implémenter une solution basée sur les réseaux virtuels en procédant à la segmentation logique du réseau de l'EPB afin d'améliorer ses performances.

Dans un premier temps, nous avons présenté l'architecture physique existante du réseau intranet de l'EPB. Sa critique est l'un des points importants de notre travail, car elle nous a dévoilé ces points faibles afin d'implémenter notre solution. En effet, nous avons constaté l'absence de serveurs en redondances pour assurer la tolérance aux pannes (assurer la disponibilité et la continuité des données et des ressources dans une entreprise). En outre, il existe un seul domaine de diffusion, ce qui provoque une surcharge du réseau de l'entreprise, les machines communiquent sans cesse entre elles, en conséquent, le trafic réseau devient lourd, ce qui cause un ralentissement de la communication sur le réseau et qui peut engendrer une lourdeur sur les applications et machines clients.

Sur le plan applicatif, nous avons proposé d'organiser l'ensemble du personnel de l'entreprise dans des réseaux virtuels en fonction de leurs tâches et besoins, en séparant les groupes contenant des données sensibles du reste du réseau, ce qui diminue les risques de violation de la confidentialité. Par exemple, les ordinateurs du personnel de la direction générale qui se trouvent sur le VLAN 10, sont complètement séparés du trafic des données du personnel de la direction domaine et développement (Vlan 20). Ainsi, nous avons définit des VLANs pour différentes directions et services.

Vers la fin, et afin de tester le niveau de sécurité de notre solution, nous avons procédé à une série de tests en envoyant les requêtes "ping". Les résultats de ces tests ont permis de mesurer le niveau de sécurité élevé de notre solution.

Notre solution est efficace pour sécuriser le réseau intranet de l'EPB. Toutefois, il est préférable de définir des listes d'accès (ACL) afin de filtrer le trafic réseau passant par le commutateur.
Dans la continuité de notre travail présenté, nous pourrions approfondir notre étude afin de compléter notre solution. En effet, avec l'apparition des nouveaux switches Cisco Catalysts, on peut filtrer le trafic dans le même VLAN grâce aux listes d'accès pour VLAN (VACL).

Les switches Cisco Catalyst ont également la possibilité de diviser logiquement un même VLAN en plusieurs partitions. Chacune de ces partitions peut être isolée l'une de l'autre, bien qu'elles partagent le même sous-réseau IP et l'adresse du commutateur.

Bibliographie

[1] Rziza Mohammed, Cours des réseaux Informatiques (2010-2011)

[2] Jean-Francois Pillou, Tout sur les réseaux et Internet, DUNOD 2006.

[3] Académie de Lyon GENERALITES, SUR LES RESEAUX
http ://www.ac-lyon.fr

[4] Frederic Jacquenod, Cours Réseaux Nº5 : les matériels d'interconnexion.

http ://www.netalya.com/fr/reseaux5.asp

[5] http://lycee-desfontaines.eu/si/sequences-ts/reseau1/res/reseaux_cr

[6] Pierre Erny,LES RESEAUX INFORMATIQUES D'ENTREPRISE, 1998

[7] Sylvain le modµele TCP/IP, http ://www.frameip.com/tcpip/, 2003.

[8] concevoir-la-sc3a9curitc3a9-informatique-en-entreprise_aman-vladimir1

[9]http://xenod.free.fr/0_La_securite_informatique.htm#Objectifsdelasécuritéinformatique

[10] S.Bouam et J.Ben-Othman, protocole de sécurisation des données à base de routage dans les réseaux AD HOC, 2004.

[11] Cédric Llorens, Informatique et Réseaux Mesure de la sécurité "logique" d'un réseau d'un operateur de télécommunications ,2005.

[12] GILBERT Held, les réseaux locaux virtuels, Conception, mise en œuvre et administration. Aout 1998.

[13] http://dspace.univ-tlemcen.dz/bitstream/112/4798/1/PFE
Master_Zineb_BENDELLA.pdf

[14] Jabou Chaouki, Schillings Michaël et Hantach Anis, « TER Détection d'anomalies sur le réseau », Rapport de projet, Université Paris Descartes, 2009.

[15] Elies Jebri, « Introduction à la sécurité», support de cours, 2008

[16] http://www.codeproject.com/Articles/439890/Text-Documents-Clusteringusing-K-Means-Algorithm.

[17] Rabehi Sidi Mohamed El Amine, « Mise en place d'un serveur radius sous linux pour la sécurisation d'un réseau 802.11 », Projet de fin d'étude, Université Abou Bakr Belkaid,Tlemcen, Algérie, 2011

[18] Rachid NAIT BEKOU et Younès MOUSSAHHIL, « Etude de fiabilité et conception d'une solution VPN », Mémoire de Projet de fin d'étude, Université mohammed V SOUSSI, Maroc, 2004.

Bibliographie

[19] http://mariepascal.delamare.free.fr/IMG/pdf/VLAN_CM.pdf

[20] John W. Lockwood. Implementation of Campus-wide Wireless Network Services using ATM, Virtual LANs, and Wireless Basestations. In IEEE Wireless Communications and Networking Conference (WCNC), September 1999.

[21] Les VLANs : les protocoles de transport et de contr^ole, http ://www-igm.univ-mlv.fr/ dr/XPOSE2006/SURZUR-DEFRANCE/vlanport.html

[22] http://perso.modulonet.fr/placurie/Ressources/BTS2-AMSI/Chap-10-%20Les%20VLAN.pdf

[23] http://igm.univ-mlv.fr/~dr/XPOSE2007/vlanparlegrandquinapascomprislesconsignes/8021QTrame.html

[24] http://irp.nain-t.net/doku.php/310lansecure:10_vlans:10_theorie

[25] http://joryck-leyes.fr/tuto/VLAN.pdf

[26] https://www.inetdoc.net/articles/inter-vlan-routing/inter-vlan-routing.vlan.html#inter-vlan-routing.vlan.definitions

[27] http://www.antipedophil.fr/download/guides/LeGrandLivre.pdf

[28] http://reussirsonccna.fr/vtp-vlan-trunking-protocol/

[29] http://roche-maxime.weebly.com/uploads/2/5/8/6/25864829/tuto_vtp_vmps.pdf

Résumé

Les réseaux locaux virtuels ou VLANs ont révolutionné le concept de segmentation des réseaux, ils permettent de constituer autant de réseaux logiques que l'on désire sur une seule infrastructure.

Ce document s'inscrit dans le cadre de projet de fin d'études pour l'obtention du diplôme de master 2 en Informatique, option administration et sécurité des réseaux à l'université de Béjaia.

Il décrit un travail fournit au sein du service informatique de la direction des systèmes d'information de l'entreprise portuaire de Béjaia.

Dans ce document, un design d'une solution sera présenté pour l'amélioration de la sécurité et l'optimisation de la bande passante du réseau, cette solution consiste à mettre en place des réseaux locaux virtuels.

Mots clés :

Réseau informatique d'entreprise, Réseaux locaux virtuel, Sécurité des réseaux, norme 802.1Q, Protocole ISL.

Abstract

The virtual local area networks or VLANs made a huge revolution of network segmentation concept, making possibl to form as many logical networks as desired in one infrastructure.

This document is part of studies project to obtain Master 2 in computer science option ASR at the university of Bejaia.

It describes the work done at data service, EPB information system direction.

This document presents a design of a solution for security improvement and band widthand optimization. This solution involves setting up a virtual local area network.

Keywords:

Corporate computer network, Virtual Local Area Network, Network security, Norm 8002.Q, Protocol ISL.