République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A. MIRA-BEJAIA

Faculté des Sciences Exactes

Département d'Informatique

MÈMOIRE

EN VUE DE L'OBTENTION DU DIPLÔME DE MASTER PROFESSIONNEL

Domaine : Mathématiques et Informatique **Filière :** Informatique

Spécialité : Administration et sécurité des réseaux

Thème

Etude et proposition d'une solution VLAN au sein de l'entreprise Naftal CBR

Présenté par

M BENMOUHOUB Mounir et M GHANEM Massinissa

déposé le 14 /10/2020

Devant le jury composé de :

Mme.	BACHIRI Lina	Docteur	Univ. de Béjaia	Encadreur
Mme.	ZIDANI Faroudja	Docteur	Univ. de Béjaia	Co-encadreur
M.	MOKTEFI Mohand	MAA	Univ. de Béjaia	Examinateur
Mme.	BELKHIRI Louiza	MCB	Univ. de Béjaia	Examinatrice

Année Universitaire : 2019/2020

Remerciements

Avant tout,on remercie Allah le tout puissant, qui nous a donné la force et la patience pour l'accomplissement de ce travail.

Nous tenons aussi à remercier nos promotrices qui nous ont aidé tout au long de la réalisation de notre travail,ainsi que toutes les personnes qui nous ont apporté leus aide et qui ont contribué à l'élaboration de ce mémoire ainsi qu'à la réussite de cette année universitaire.

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

Nos sincères reconnaissances pour tous nos enseignants, qui nous ont transmis fidèlement leur savoir et qui nous ont appris le vrai sens des études.

Enfin, nous adressons nos plus sincères remerciements à nos parents et ami(e)s, pour leurs encouragements au cours de la réalisation de ce mémoire. Merci à tous et à toutes.

Dédicaces

Ce modeste travail est dédié :

A mon Père

Qui m'a encouragé à aller de l'avant et qui m'a donné tout son soutien moral et matériel afin de réaliser mes projets

À la mémoire de ma Mère

qui m'a toujours poussé et motivé dans mes études

À mes frères et soeurs :

pour tous leurs encouragements

À mes amis

Et toute personne que je connais et qui m'est chere et tous ceux qui m'aiment. . .

BEN.Mounir.

Dédicaces

Je dédie ce modeste travail

À mes très chers parents,

pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études,

À mes chères sœurs Dihia,Tinhinan et Tiziri,

pour leurs encouragements permanents, et leur soutien moral,

À toute ma famille

pour son soutien tout au long de mon parcours universitaire,

À mon binôme Mounir,

Avec qui j'ai partagé de belles années d'études .

Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fruit de votre soutien infaillible,

Merci d'être toujours là pour moi.

GH.Massinissa

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

ACL : Access Control List

CFI :Canonical Format Indentifier

CISCO :Computer Information System Company

CLI :Command Language Interface

CRC :Cyclic Redundancy Codes

DHCP :Dynamic Host Configuration Protocol

ETTD :Équipement terminal de traitement des données

ETCD :Équipement terminal de circuit des données

FDDI :Fiber Distributed Data Interface

FTP :File Transfer Protocol

GPL :Gaz de pétrole liquéfié

GVRP :Multiple Registration Protocol

HTTP : Hyper Text Transfer Protocol

IOS :International Organization for Standardization

IP :Internet Protocol

IPV4 :Internet Protocol version 4

ISL :Inter-Switch Link Protocol

LAN :Local Area Network

MAC :Media Access Control

MAN :Metropolitain Area Network

OSI :Open System Interconnexion

PAN :Personnal Area Network

STP :Spannig-Tree Protocol

TCP :Transmission Control Protocol

TCI :Tag Control Information

TPID :Tag Protocol Identifier

UDP :User Datagram Protocol

VLAN :Virtual Local Area Network

VTP :Vlan Trunk Protocol

WAN :Wide Area Network

INTRODUCTION GÉNÉRALE

Introduction Générale

Le rôle des réseaux a sensiblement évolué ces dernières années,il ne se limite pas au transfert de l'information en toute sécurité mais aujourd'hui il contribue largement à la rationalisation des utilisateurs et à l'optimisation des performances applicatives. De ce fait on a besoin d'un ensemble de moyens et de techniques permettant la diffusion d'un message auprès d'un groupe plus ou moins vaste et hétérogène.

A l'heure actuelle, il est plus fréquent de voir l'utilisation des VLANs au sein des entreprises car ils offrent de nouvelles solutions et opportunités en matière de gestion des réseaux .

Ce nouveau mode de segmentation modifie radicalement la manière dont les réseaux sont conçus, maintenus et administrés .

L'objectif principal de notre projet est de proposer une nouvelle architecture pour le réseau local de NAFTAL . Pour cela notre mémoire de fin de cycle contiendra les quatre chapitres suivants :

- Dans le premier chapitre, nous présentons un aperçu sur les généralités des réseaux informatiques ,qui aidera à la compréhension de la problématique posée.
- Puis dans le deuxième chapitre , nous allons faire le point sur le concept des vlans.Nous donnons le principe de leur fonctionnement,leurs différent types,leurs avantages et leurs normes existantes.
- Le troisième chapitre est consacré pour la présentation de l'organisme d'accueil avec ses différents services pour chaque département,en étudiant son architecture.
- Enfin, dans le quatrième chapitre, nous allons passer à la réalisation en implémentant notre solution VLAN.

CHAPITRE 1 : GÉNÉRALITÉS SUR LES RÉSEAUX INFORMATIQUES

Chapitre 1

Généralités Sur Les Réseaux Informatiques

1.1 Introduction

Dans ce chapitre, nous allons passer en revue quelques notions, bien que connues de base, mais que nous jugeons opportun de les faire rappeler très brièvement pour une meilleure compréhension de l'avancement de l'objectif posé. Il résume en général les réseaux informatiques à savoir de ses types allant à la sécurité,

1.2 Définition d'un réseau informatique :

Un réseau informatique est un ensemble d'équipements matériels et logiciels interconnectés les uns avec les autres dans le but de partager des ressources (physiques ou logicielles).[1]

1.3 Différents types de réseaux informatiques :

On distingue différents types de réseaux selon leurs tailles (en termes de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue. Les réseaux informatiques sont généralement classifiés en trois catégories de réseaux selon leur échelle géographique[1].

1.3.1 PAN (Personnal Area Network) :

Le PAN , est le plus petit étendue des réseaux, il désigne une interconnexion d'équipements informatiques dans un espace de dizaine de mètres. Il peut être appelé réseau individuel ou réseau domestique.

1.3.2 LAN(Local Area network) :

Un réseau local est un réseau informatique à une échelle géographique relativement restreinte, il est utilisé pour relier les ordinateurs d'une habitation particulière, d'une entreprise ou d'une salle informatique. L'infrastructure est privée et est gérée localement.

1.3.3 MAN(Métropolitan area netwok) :

Les MANs interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de kilomètres) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local. Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

1.3.4 WAN(Wide area network) :

Un WAN (réseau étendu) interconnecte plusieurs LANs à travers de grandes distances géographiques. Les débits disponibles sur un WAN résultent d'un arbitrage avec le cout des liaisons (qui augmente avec la distance) et peuvent être faibles. Les WANs fonctionnent grâce a des routeurs qui permettent de ''choisir" le trajet le plus approprié pour atteindre un nœud du réseau. Le plus connu des WAN est Internet.

1.4 Topologies des réseaux informatiques :

Il existe deux types de topologies :

1.4.1 Topologie physique :

la topologie physique est la façon dont les équipements sont connectés physiquement les uns aux autres grâce à des lignes de communication (câbles réseaux) et des éléments matériels (cartes réseaux, etc.) .
On distingue généralement les topologies suivantes : [2]

En bus : Une topologie en bus est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câbles, généralement coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau.

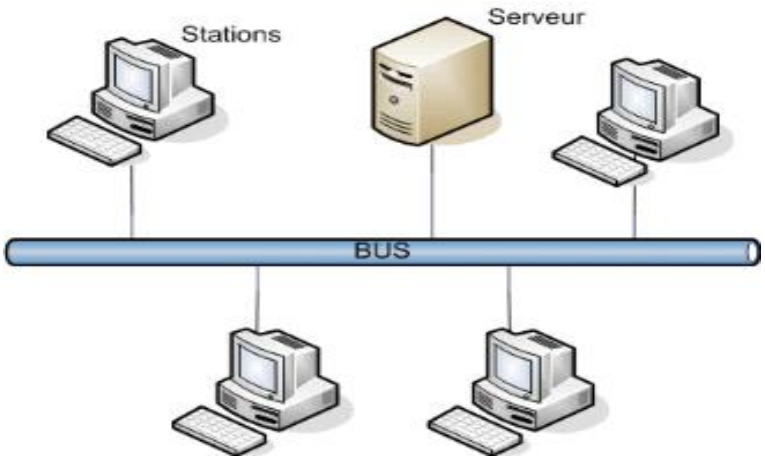

FIGURE 1.1 – Topologie en bus.

En étoile : La topologie en étoile est la plus utilisée. Dans la topologie en étoile, tous les ordinateurs sont reliés à un seul équipement central, qui peut être un concentrateur (Hub), un commutateur (Switch), ou un Routeur.

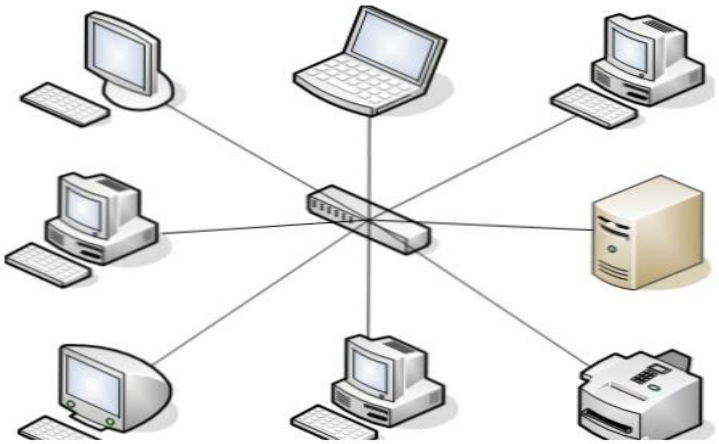

FIGURE 1.2 – Topologie en étoile.

En anneau : Dans un réseau possédant une topologie en anneau, les stations sont reliées en boucle et communiquent entre elles. Elle est utilisée pour le réseau Token ring ou FDDI (Fiber Distributed Data Interface).

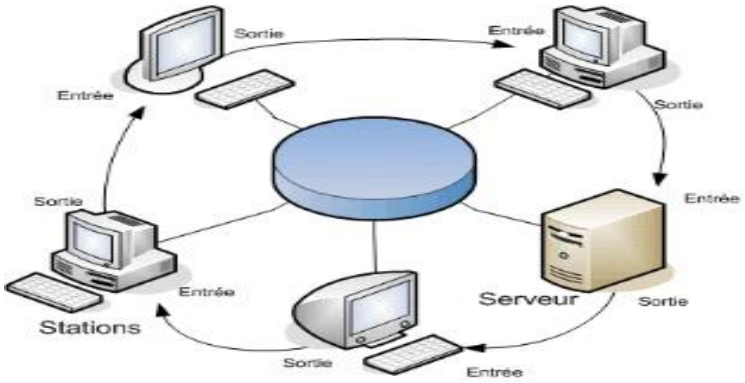

FIGURE 1.3 – Topologie en anneau.

Maillée : Une topologie maillée correspond à plusieurs liaisons point à point : chaque terminal peut être relié à tous les autres.

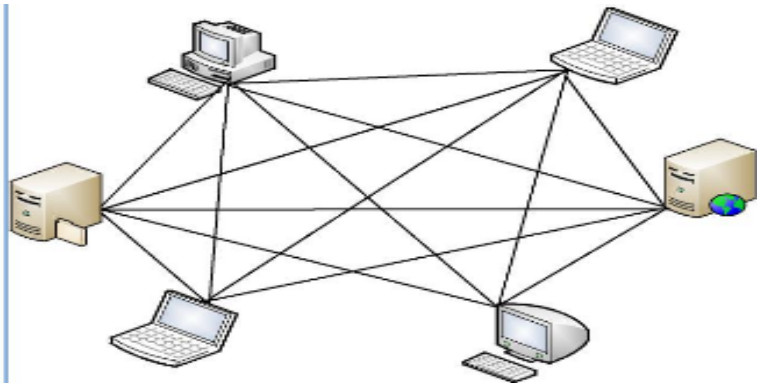

FIGURE 1.4 – Topologie maillée.

1.4.2 Topologie logique :

Par opposition à la topologie physique,elle représente la façon dont les données transitent sur les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token Ring et FDDI [3].

Aujourd'hui, un réseau local repose presque systématiquement sur la technologie Ethernet, car le prix de revient d'un tel réseau n'est pas très élevé.

1.5 Les liaisons entre les stations :

On peut distinguer deux types de liaisons de données :[2]

1.5.1 Liaison point à point :

Elles sont utilisées principalement par les réseaux publics. Chaque station est commutée avec une autre d'une façon individuelle.

FIGURE 1.5 – liaison point a point[2].

1.5.2 Liaison multipoint :

Elles sont principalement utilisées par les réseaux locaux. Une station primaire a accès aux stations secondaires, et elles peuvent communiquer entre elles.

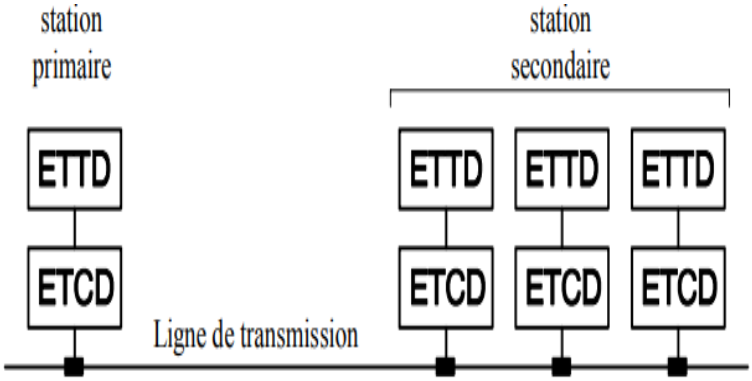

FIGURE 1.6 – liaison multipoint[2].

ETTD : est un élément qui ne se connecte pas directement à la ligne de transmission. Par exemple : un ordinateur, un terminal, une imprimante,...

ETCD :assure la transmission des données. Par exemple : un modem, un multiplexeur.

1.6 Modèles d'architecture de réseaux :

Il existe deux types de modèle de réseau de base : le modèle de référence (OSI) et le modèle d'applications (TCP/IP)[4] :

1.6.1 Modèle OSI (Open System Interconnection) :

Le modèle OSI est un modèle conceptuel. Il a pour but d'analyser la communication en découpant les différentes étapes en 7 couches, chacune de ces couches remplissant une tâche bien spécifique (voir la figure ci-dessous).

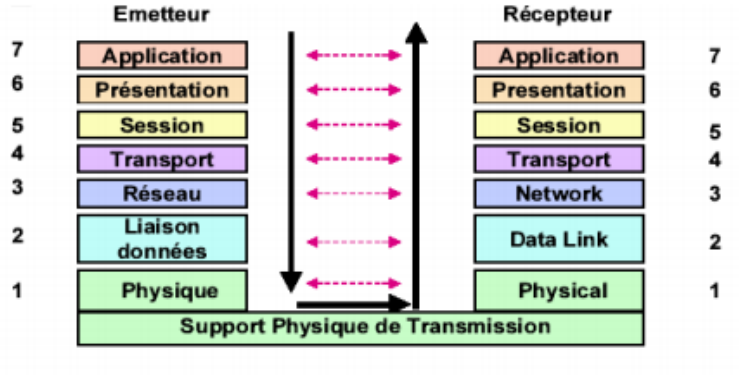

FIGURE 1.7 – Le modèle OSI [4].

Afin de connaitre les services de chaque couche on va les présenter ci-dessous l'une après l'autre :

- **Couche physique :** fournit les moyens mécaniques, optiques, électroniques, fonctionnels et procéduraux nécessaires à l'activation, au maintien et à la désactivation des connexions physiques nécessaires à la transmission des bits. Les systèmes sont interconnectés réellement au moyen de supports physiques de communication.
- **Couche liaison de données :** assure la transmission d'informations entre deux ou plusieurs systèmes immédiatement adjacents. Détecte et corrige, dans la mesure du possible, les erreurs issues de la couche inférieure. Les objets échangés sont souvent appelés trames.
- **Couche réseau :** achemine les informations à travers un réseau pouvant être constitué de systèmes intermédiaires (routeurs). Les objets échangés sont souvent appelés paquets.
- **Couche transport :** assure une transmission de bout en bout des données. Maintient une certaine qualité de la transmission, notamment vis-à-vis de la fiabilité et de l'optimisation de l'utilisation des ressources. Les objets échangés sont souvent appelés segments.

- **Couche session :** fournit aux entités coopérantes les moyens nécessaires pour synchroniser leurs dialogues, les interrompre ou les reprendre tout en assurant la cohérence des données échangées.
- **Couche présentation :** spécifie les formats des données des applications(compression, cryptage,etc).
- **Couche application :** donne aux processus d'application les moyens d'accéder à l'environnement de communication de l'OSI. Comporte de nombreux protocoles adaptés aux différentes classes d'application.

1.6.2 Modèle TCP/IP :

Contrairement au modèle OSI, le modèle TCP/IP est né d'une implémentation . Il reprend l'approche modulaire (utilisation de modules ou couches) mais en contient uniquement quatre. Les trois couches supérieures du modèle OSI sont souvent utilisées par une même application (voir la figure 1.8).

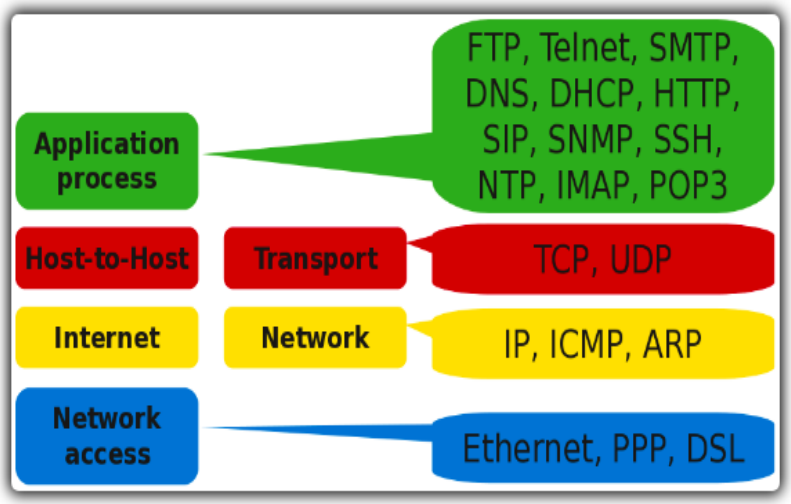

FIGURE 1.8 – Modèle TCP/IP [5].

Afin de connaitre les services de chaque couche on va les présenter brièvement ci-dessous l'une après l'autre

- **Couche application :** les applications interagissent d'une manière adéquate avec les protocoles de la couche "Transport" pour envoyer ou recevoir des données.
- **Couche transport :** chargée de fournir un moyen de communication de bout en bout entre 2 programmes d'application. Agi en mode connecté et en mode non connecté. Elle divise le flux de données venant des applications en paquets, transmis avec l'adresse

destination IP au niveau IP.

- **Internet :** encapsule les paquets reçus de la couche "Transport" dans des datagrammes IP.
- **Accès réseau :** assure la transmission d'un datagramme venant de la couche IP en l'encapsulant dans une trame physique et en transmettant cette dernière sur un réseau physique.

1.6.3 Comparaison entre le modèle OSI et TCP/IP :

Ces deux modèles sont très similaires, dans la mesure où les deux sont des modèles de communication à couches et utilisent l'encapsulation de données. On remarque cependant deux différences majeures :

- TCP/IP regroupe certaines couches du modèle OSI dans des couches plus générales.
- TCP/IP est plus qu'un modèle de conception théorique, c'est sur lui que repose le réseau.

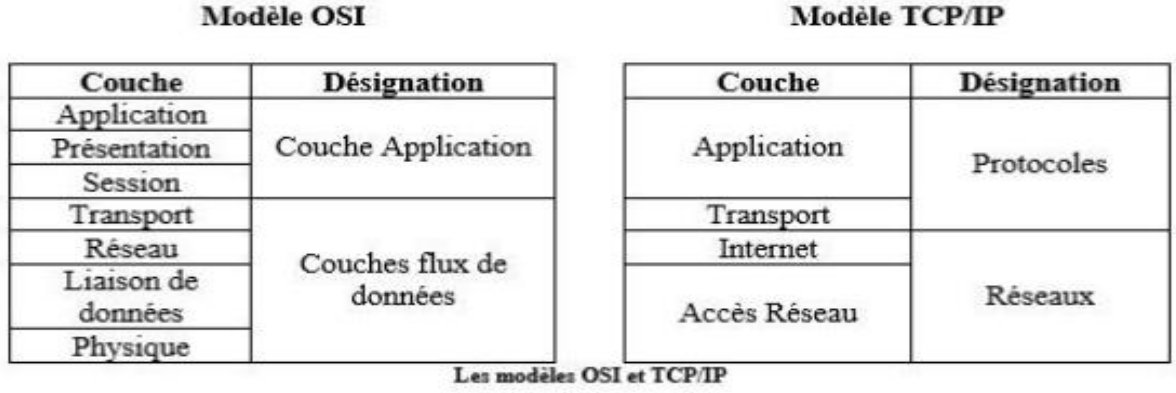

FIGURE 1.9 – Comparaison entre OSI et TCP/IP.

1.7 Equipements de base d'un réseau informatique :

Pour la mise en place d'un réseau,on a besoin de certains périphériques physiques necessaires à la communication et l'interaction entre les appareils de ce réseau.y compris[6] :

- **Répéteur :** est un dispositif électronique combinant un récepteur et un émetteur, qui compense les pertes de transmission d'un média (ligne, fibre, radio) en amplifiant et traitant éventuellement le signal, sans modifier son contenu.
- **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 architectures de réseaux différentes. 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 les connecter à un système de câblage.
- **Carte réseau :** est un périphérique informatique qui fait le lien entre l'ordinateur dans lequel elle est installée et le réseau auquel elle le connecte. Elle est constituée d'un ensemble de composants électroniques soudés entre eux sur un même circuit imprimé.
- **Modem :** c'est un appareil qui sert à convertir les données numériques de l'ordinateur en signal modulé, dit « analogique », transmissible par un réseau analogique et réciproquement.

1.8 Adressage IP :

L'addresse IP est attribuée à chaque interface avec le réseau de tout matériel informatique[7].

1.8.1 structure des adresses IP :

Comme l'Internet est un réseau, l'adressage est particulièrement important. Les adresses IP ont été définies pour être traitées rapidement. Les routeurs qui effectuent le routage en se basant sur le numéro de réseau sont dépendants de cette structure. Les adresses IP v4 sont représentées sur 32 bits, Regroupées en quatre octets de 8 bits séparés par des points décimaux.
Ces 32 bits sont séparés en deux zones de bits contiguës :

- **Network ID :** cette partie décrit le numéro du réseau local auquel est rattachée la station.
- **Host ID :** cette partie correspond au numéro de la station dans le réseau lui-même, appelée numéro d'hôte.

classes d'adresses :

Selon l'adresse IP on définit différentes classes d'adresses. Il existe cinq classes d'adresses IPv4 (version courante) des protocoles TCP/IP, car les parties réseau et hôte n'ont pas toujours la même taille.

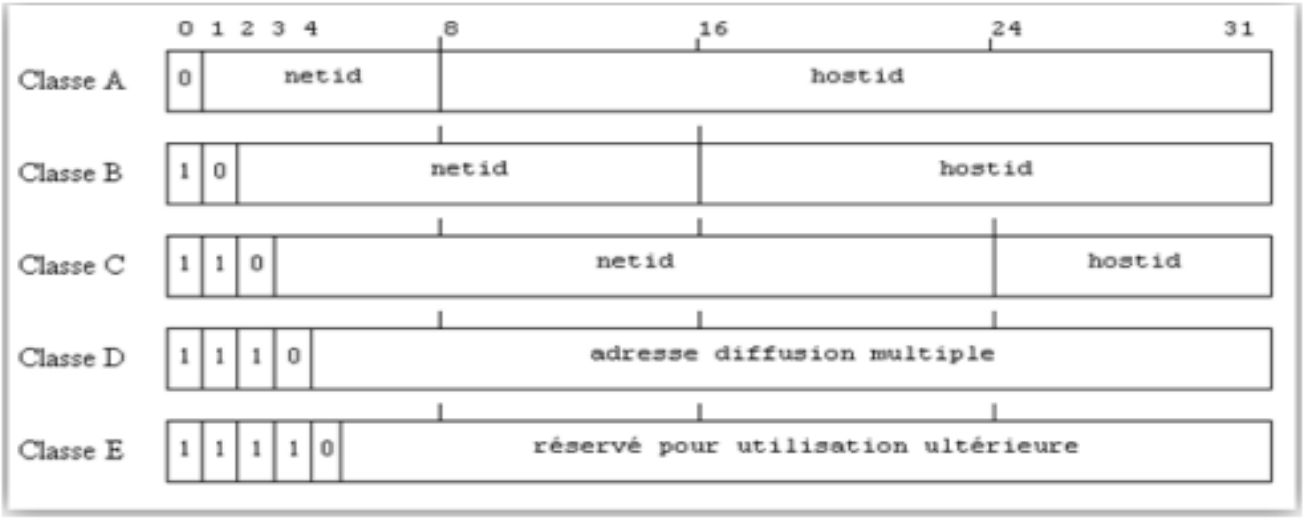

FIGURE 1.10 – Caractéristiques des classes des adresses IP[7].

Le but de la division des adresses IP en classes, est de faciliter la recherche d'un ordinateur sur le réseau. En effet, avec cette notation il est possible de rechercher dans un premier temps le réseau à atteindre puis de chercher un ordinateur sur celui-ci. Ainsi, l'attribution des adresses IP se fait selon la taille du réseau :

Il faut connaître une chose importante dans l'adressage IP c'est qu'il y a des adresses réservées qui sont :

- Classe A : 10.0.0.1 à 10.255.255.254
- Classe B : 172.16.0.1 à 172.31.255.254
- Classe C :192.168.0.1 à 192.168.255.254

1.8.2 Notions importantes :

- **sous-réseau :** un sous-réseau est une subdivision logique d'un réseau de taille plus importante.
- **masque sous-réseau :** le masque de sous-réseau indique quelle partie de l'adresse Internet est utilisée pour adresser le réseau, et laquelle est réservée à l'adressage d'un ordinateur particulier à l'intérieur du réseau logique. Le masque de sous-réseau n'a en principe aucune influence sur les paquets des données transmis par un ordinateur sur

le réseau. Il influence par contre le fonctionnement du logiciel local de réseau, en lui indiquant comment l'adresse Internet doit être interprétée.

- **Domaine de collision :**

  Une collision intervient lorsque deux hôtes d'un réseau émettent simultanément sur un média partagé. Le domaine de collision est un sous-ensemble du réseau à l'intérieur duquel les hôtes sont en compétition pour accéder à un même média ou canal de communication. Plus le nombre d'hôtes présents dans un même domaine de collision est important, plus la fréquence des collisions augmentent et plus les performances se dégradent. Pour garantir les meilleures conditions de communication, on cherche donc à réduire au maximum l'étendue du domaine de collision [8].

- **Domaine de diffusion :**

  La diffusion est un mécanisme d'annonce générale qui assure que tous les hôtes d'un réseau local reçoivent les trames de diffusion émises par n'importe quel autre hôte de ce même réseau. Le domaine de diffusion est un réseau à l'intérieur duquel tous les hôtes peuvent émettre et doivent recevoir des trames de diffusion. Comme dans le cas précédent, plus le nombre d'hôtes présents dans le domaine de diffusion est important, plus les performances se dégradent. la encore, pour garantir les meilleures conditions de communication, on cherche à réduire «raisonnablement» l'étendue du domaine de diffusion. [8]

1.9 Sécurité des réseaux informatique :

Le développement de la technologie méne les entreprise à utiliser les réseaux d'internet pour la communication entre elles ,mais elles sont exposées evéntuelement a des attaques ,de piratage ,de virus ...etc.A cause de ces probleme, il est necessaire de sécuriser le réseau et le systeme informatique.

1.9.1 La sécurité en informatique :

La sécurité informatique consiste à assurer que les ressources du système d'information (matérielles et/ou logicielles) d'une organisation sont uniquement utilisées dans le cadre où il est prévu qu'elles le soient[9].

- **La disponibilité :** c'est le faite de mener une ressource a la destination dans un temps correct .
- **L'intégrité :**elle permet de s'assurer que les données n'ont pas été altérées durant une communication.
- **La confidentialité :**consiste a s'assurer que seules les personnes autorisées peuvent acceder aux ressources échangées.
- **l'authentification :**s'assurer de l'identité d'un utilisateur
- **La non répudiation :**permettant de garantir qu'une transaction ne peut être niée .

1.9.2 Les dispositifs de sécurité :

Il existe plusieurs dispositifs pour mettre en place une politique de sécurité ,on va citer quelques uns :[10]

1. **Le pare-feu :** Un pare-feu (Firewall) est un logiciel ou un matériel qui se charge d'établir une barrière entre le monde intérieur et le monde extérieur pour faire barrage aux pirates comme le montre l'exemple suivant :

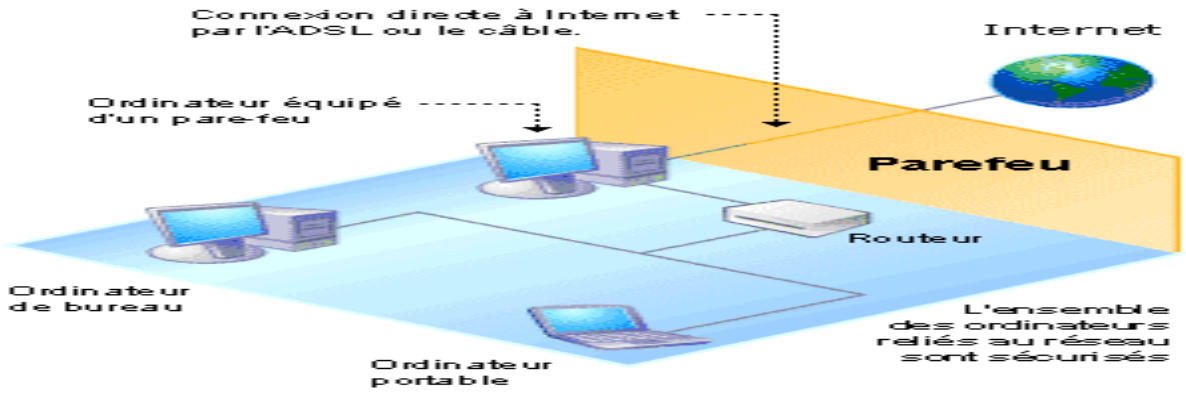

FIGURE 1.11 – exemple de pare-feu[10].

- **Types de pare-feu :**

  i. **Le pare-feu logiciel et personnel :**
  C'est un logiciel qui contrôle les données entrantes et sortantes.

  ii. **Le routeur :**
  il masque votre adresse IP et vos ports. C'est un périphérique matériel accompagné d'un logiciel qu'il faut mettre souvent à jour.

Il est déjà plus cher que le pare-feu personnel. Ce n'est pas un vrai pare-feu dans le sens que ce n'est pas sa fonction principale.

iii. **Le pare-feu matériel :**

Les firewalls hardware les plus simples sont sous forme de boîtier incluant deux connecteurs réseaux : le premier pour relier le réseau interne, le second pour relier l'extérieur.

2. **Demilitarized zone (DMZ) :**

On appelle DMZ (Demitarized Zone) un sous-réseau du réseau global à sécuriser comportant en général les serveurs http, ftp, smtp, ..., crées dont le but d'éviter toute connexion directe avec le réseau interne et de prévenir celui-ci de toute attaque extérieure depuis le Web.

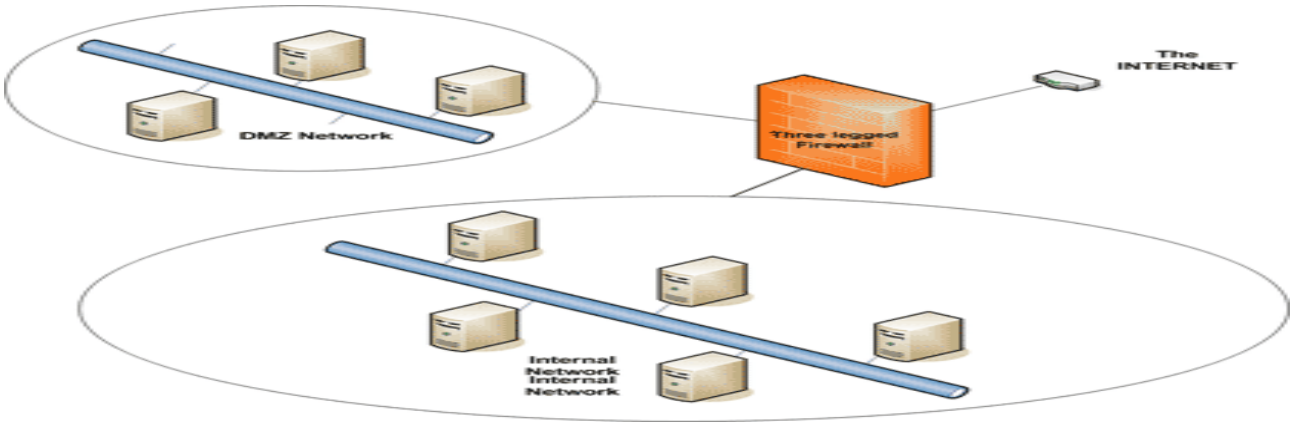

FIGURE 1.12 – schéma représentant le réseau de DMZ

3. **Les VPN :**

VPN (Virtuel Private Network) :est une technique permettant à un ou plusieurs postes distants de communiquer de maniére sure , tout en empruntant les infrastructures publiques[11].

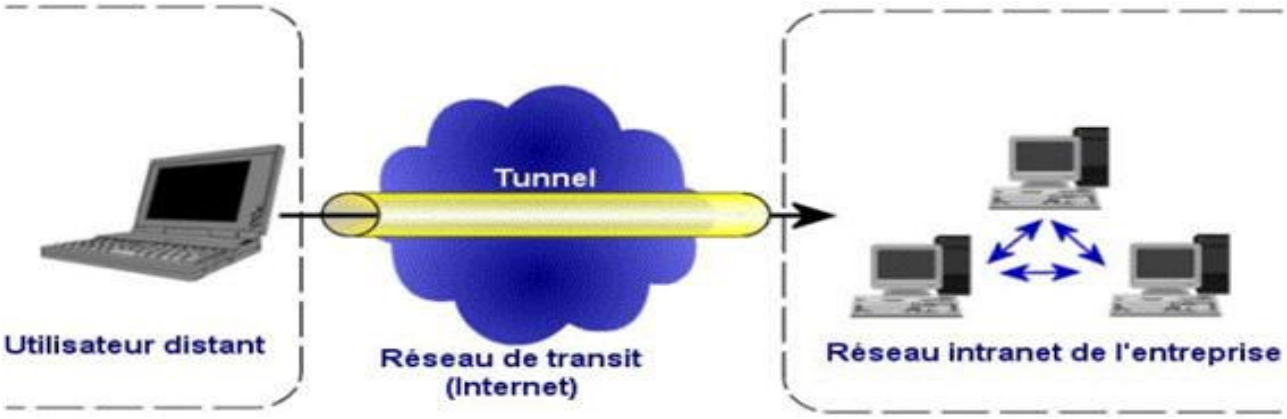

FIGURE 1.13 – schéma représentant un réseau VPN[11]

Il existe d'autres politiques de sécurité tel que le système de détection d'intrusions , le filtrage d'url, les VLAN sur lequel on s'est basé dans notre mémoire.

1.10 Conclusion

Ce chapitre a été une ligne droite sur la présentation de tout ce qui concerne les réseaux en général à savoir les types ,leurs classifications,le modèle de réference et d'application (OSI et TCP/IP),l'adressage IP , les équipements d'interconnexion et la séecurité dans un réseau local afin de bien aborder le chapitre suivant qui sera consacré aux réseaux virtuels VLANs.

CHAPITRE 2 :
INTRODUCTION AUX RESEAUX LOCAUX VIRTUELS

Chapitre 2

Introduction aux réseaux locaux virtuels

2.1 Introduction :

Le développement rapide d'internet a mené de nombreuses entreprises à étendre leur installation informatique. les réseaux virtuels (Virtual LAN) sont apparus comme une nouvelle fonctionnalité dans l'administration réseau avec le développement des commutateurs.
Il permettent la segmentation et la sécurisation des LAN tout en augmentant leur performance. Dans ce chapitre, nous allons présenter les principaux concepts d'un réseau local virtuel.

2.2 VLAN(Virtuel Local Area Network) :

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 [12].

2.3 Les avantages et les inconvénients des Vlans [13] :

Avantages :

- **Augmentation des performances :** la segmentation créée par les VLAN réduit la taille des domaines de diffusion et de ce fait le nombre de collisions sur ces domaines.
- **Réduction des coûts :** l'utilisation de VLAN permet de simplifier l'administration du réseau.De plus, l'utilisation des VLAN entraîne souvent la réduction du nombre de routeurs nécessaires, or les routeurs sont plus onéreux que les switches.
- **Formation de groupes virtuels :** il est courant de retrouver dans les entreprises, des groupes de développement de travail sur un projet spécifique composés de membres qui viennent de différents départements (production, vente, etc.).

- **La sécurité :** périodiquement, des données sensibles sont envoyées en broadcast sur le réseau par les machines (et plus particulièrement les serveurs). Les VLAN permettent d'isoler les serveurs dans un même domaine de broadcast et de les isoler par service. Les VLAN apportent donc une grande flexibilité dans la gestion des réseaux ; les utilisateurs pourront être regroupés selon leurs centres d'intérêts.
- **Une meilleure utilisation des serveurs réseaux :**lorsqu'un serveur possède une interface réseau compatible avec le VLAN, l'administrateur a l'opportunité de faire une etude et une mise en place d'un réseau informatique sécurisé et faire appartenir ce serveur à plusieurs VLAN en même temps. Cette appartenance à de multiples VLAN permet de réduire le trafic qui doit être routé (traité au niveau du protocole de niveau supérieur,par exemple IP) de, et vers ce serveur ; et donc d'optimiser ce trafic. Tout comme le découpage d'un disque dur en plusieurs partitions permet d'augmenter les performances (la fragmentation peut être diminuée) de son ordinateur, le VLAN améliore considérablement l'utilisation du réseau.
- **La simplification de la gestion :** l'ajout de nouveaux éléments ou le déplacement d'éléments existants peut être réalisé rapidement et simplement sans devoir manipuler les connexions physiques dans le local technique.
- **La régulation de la bande passante :** un des concepts fondamentaux des réseaux "Ethernet" est la notion d'émission d'un message réseau vers l'ensemble (broadcast ou multicast)des éléments connectés au même commutateurs (hub/Switch). Malheureusement, ce type d'émission augmente sérieusement le trafic réseau au sein du composant de connexion. Même si les vitesses de transmission ne cessent d'augmenter, il est important de pouvoir contrôler ce gaspillage de capacité de trafic (bande passante). Ici encore, le VLAN offre à l'administrateur les moyens de réguler l'utilisation de la capacité de trafic disponible au sein de l'infrastructure.

Inconvénients :

- Les normes de routage cohabitent toujours avec des solutions propriétaires, ce qui peut causer des problèmes d'interopérabilité si le matériel utilisé n'est pas homogène.

- Délais : lorsqu'une station est connectée à un commutateur, ce dernier peut mettre un peu de temps avant de trouver à quel VLAN elle appartient. De méme lorsqu'une station est déplacée d'un commutateur à un autre ,il peut y avoir des problèmes dans la reconfiguration.

2.4 Les techniques d'implémentation des VLAN :

Pour réaliser des VLANs, il faut tout d'abord des commutateurs spéciaux de niveau deux du model OSI qui supportent le VLAN [14]

1. **VLAN de niveau 1 ou VLAN par port :**

   On affecte chaque port des commutateurs à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminée par sa connexion à un port du commutateur. Les ports sont donc affectés statiquement à un VLAN [14]

   Le VLAN de niveau 1 correspond à une configuration physique du réseau, il s'agit d'associer chaque port du switch à un VLAN. Dans ce type de Vlan il n'y a pas de traitement lourd pour chaque trame dans le processus de routage.

   Ce type de VLAN comporte quelques inconvénients :

   - Un brassage est nécessaire en cas de déménagement géographique des stations.
   - Nécessite de modifier les VLAN en cas où le mécanisme de Vlan par port ne possède pas d'architecture centralisée qui pourrait permettre d'éviter la lourdeur de la configuration. Chaque switch possède sa table de correspondance indépendamment du contenu des autres switchs.d'ajouter ou de retrait d'utilisateurs (voir la figure ci-dessous).

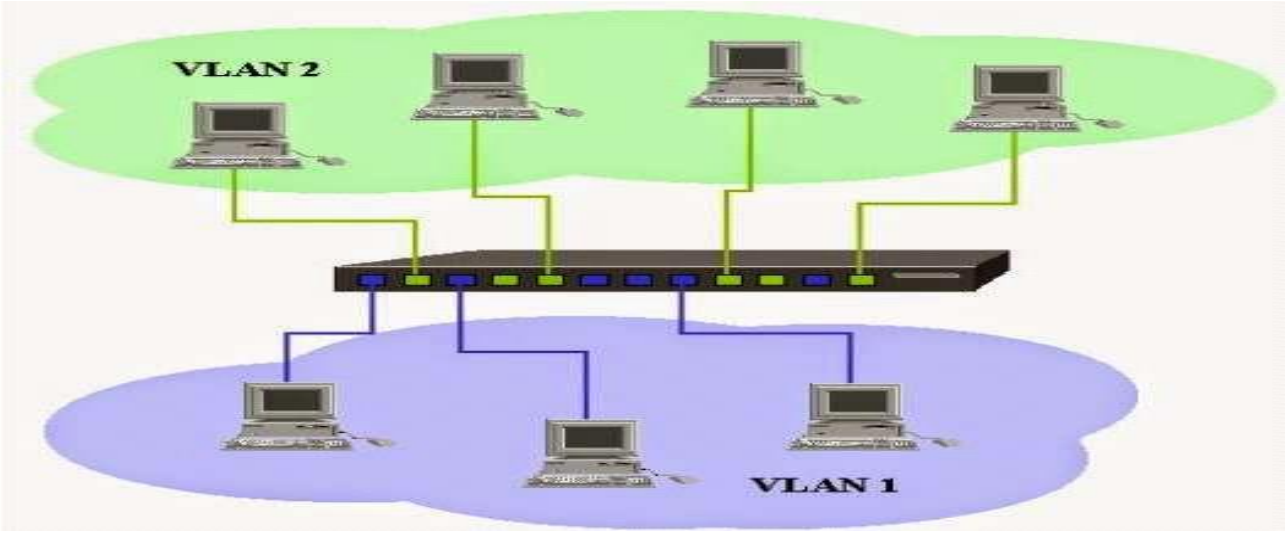

FIGURE 2.1 – VLAN par port[15].

2. **VLAN de niveau 2 ou VLAN MAC :**

   On affecte chaque adresse MAC à un VLAN. L'appartenance d'une trame à un VLAN est déterminée par son adresse MAC. En fait il s'agit, à partir de l'association Mac/VLAN, d'affecter dynamiquement les ports des commutateurs à chacun des VLAN en fonction de l'adresse MAC de l'hôte qui émet sur ce port .

   L'intérêt principal de ce type de VLAN est l'indépendance vis-à-vis de la localisation géographique. Si une station est déplacée sur le réseau physique, son adresse physique ne change pas, elle continue d'appartenir au même VLAN (ce fonctionnement est bien adapté à l'utilisation des machines portables). Si on veut changer de VLAN il faut modifier l'association Mac / VLAN (voir la figure ci-dessous).

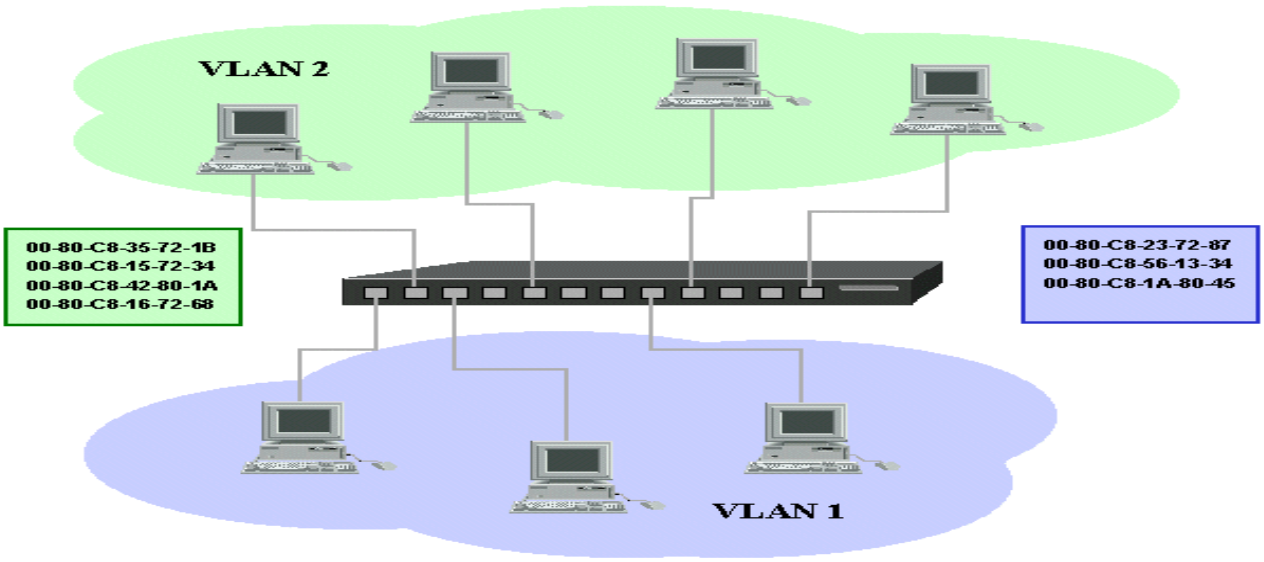

FIGURE 2.2 – VLAN par adresse MAC[15].

3. **VLAN de niveau 3 ou VLAN d'adresses réseaux :**

   On affecte une adresse de niveau 3 à un VLAN. L'appartenance d'une trame à un VLAN est alors déterminée par l'adresse de niveau 3 ou supérieur qu'elle contient (le commutateur doit donc accéder à ces informations). En fait, il s'agit d'affecter dynamiquement les ports des commutateurs à chacun des à partir de l'association adresse niveau 3/VLAN d'affecter dynamiquement VLAN.

on distingue deux type de VLAN :

- **VLAN par protocole :**

  Le 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.

- **VLAN par sous réseaux :**

  Les VLANs de niveau 3 permettent de regrouper plusieurs machines suivant le sous- réseau auquel elles appartiennent. La mise en place de VLAN de niveau 3 est conditionnée par l'utilisation d'un protocole routable (IP, autres protocoles propriétaires ...).

  L'attribution des VLANs se fait de manière automatique en décapsulant le paquet jusqu'à l'adresse source. Cette adresse va déterminer à quel VLAN appartient la machine (voir la figure ci-dessous).

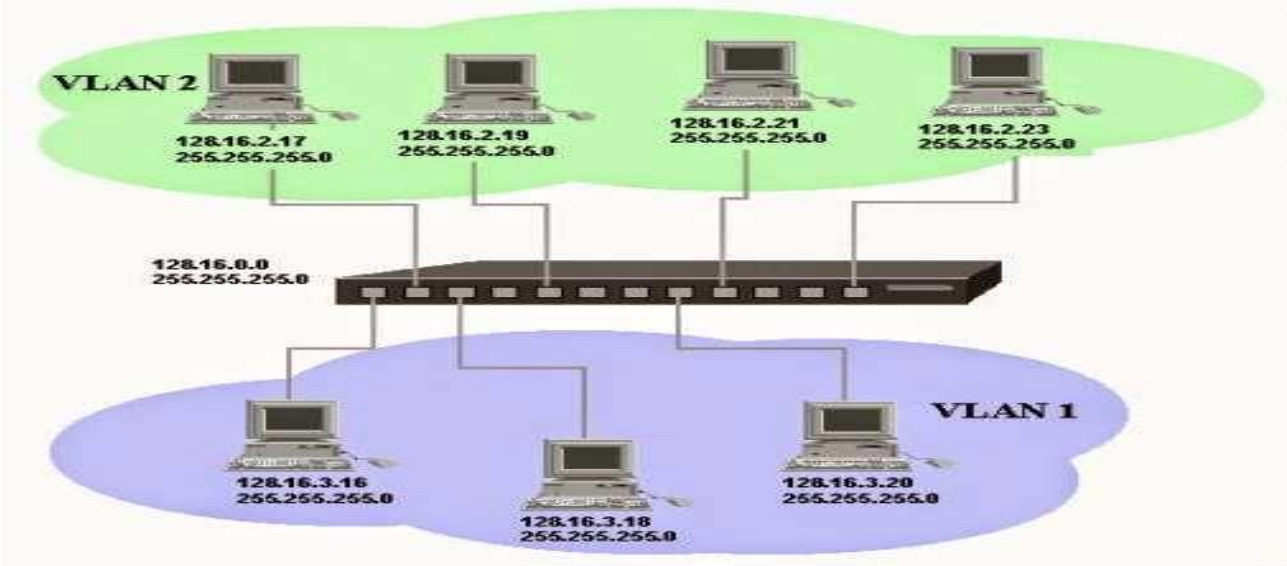

FIGURE 2.3 – VLAN par adresse IP[15].

L'avantage du VLAN niveau 3 est qu'il permet une affectation automatique à un VLAN suivant une adresse IP. Par conséquent, il suffit de configurer les clients pour joindre les groupes souhaités. Il est aussi possible de séparer les protocoles par VLAN.

Inconvénients :

- Les VLANs de niveau 3 souffrent de lenteur par rapport aux VLANs de niveau 1 et 2. En effet, le switch est obligé de décapsuler le paquet jusqu'à l'adresse IP pour pouvoir détecter à quel VLAN il appartient. Il faut donc des équipements plus coûteux (car ils doivent pouvoir décapsuler le niveau 3) pour une performance moindre.

- La sécurité est beaucoup plus faible par rapport aux VLANs de niveau 1 et 2. En effet, l'analyse de l'adresse IP rend le spoofing IP possible. Or le spoofing IP est beaucoup plus simple à réaliser que le spoofing MAC.

- Les VLANs de niveau 3 sont restreints par l'utilisation d'un protocole de routage pour avoir l'identifiant niveau 3, et ainsi se joindre au VLAN correspondant.

Le tableau suivant montre quelques différences entre les trois techniques :

Types de VLANs	Description.
VLAN niveau 1 Basé sur le port	• configuration la plus courante. • Ports affectés individuellement à un ou plusieurs VLANs. • Facile à mettre en place. • Les interfaces de gestion des Switchs permettent une configuration facile.
VLAN niveau 2 Basé sur l'adresse MAC	• Rarement utilisé • Difficile à administrer, à dépanner et à gérer.
VLAN niveau 3 Basé sur le protocole	• L'adresse IP (sous-réseau) détermine l'appartenance à un VLAN. • fréquence d'utilisation et simplicité la compliexité de mise en oeuvre.

TABLE 2.1 – «comparaison entre les 3 techniques».

2.5 les protocoles de transport des VLANs :

2.5.1 le protocole ISL(Inter Switch Link Protocol) :

ISL est un protocole propriétaire de Cisco pour l'interconnexion de plusieurs commutateurs et la maintenance des informations VLAN lorsque le trafic passe entre les commutateurs ISL fournit des capacités de liaison VLAN tout en maintenant des performances à plein débit sur les liaisons Ethernet en mode duplex intégral ou semi-duplex. L'ISL fonctionne dans un environnement point à point et peut prendre en charge jusqu'à 1000 VLAN. Dans l'ISL, la trame d'origine est encapsulée et un en-tête supplémentaire est ajouté avant que la trame ne soit transportée sur une liaison interurbaine. À la réception, l'en-tête est supprimé et la trame est transmise au VLAN attribué (voir la figure ci-dessous) [16].

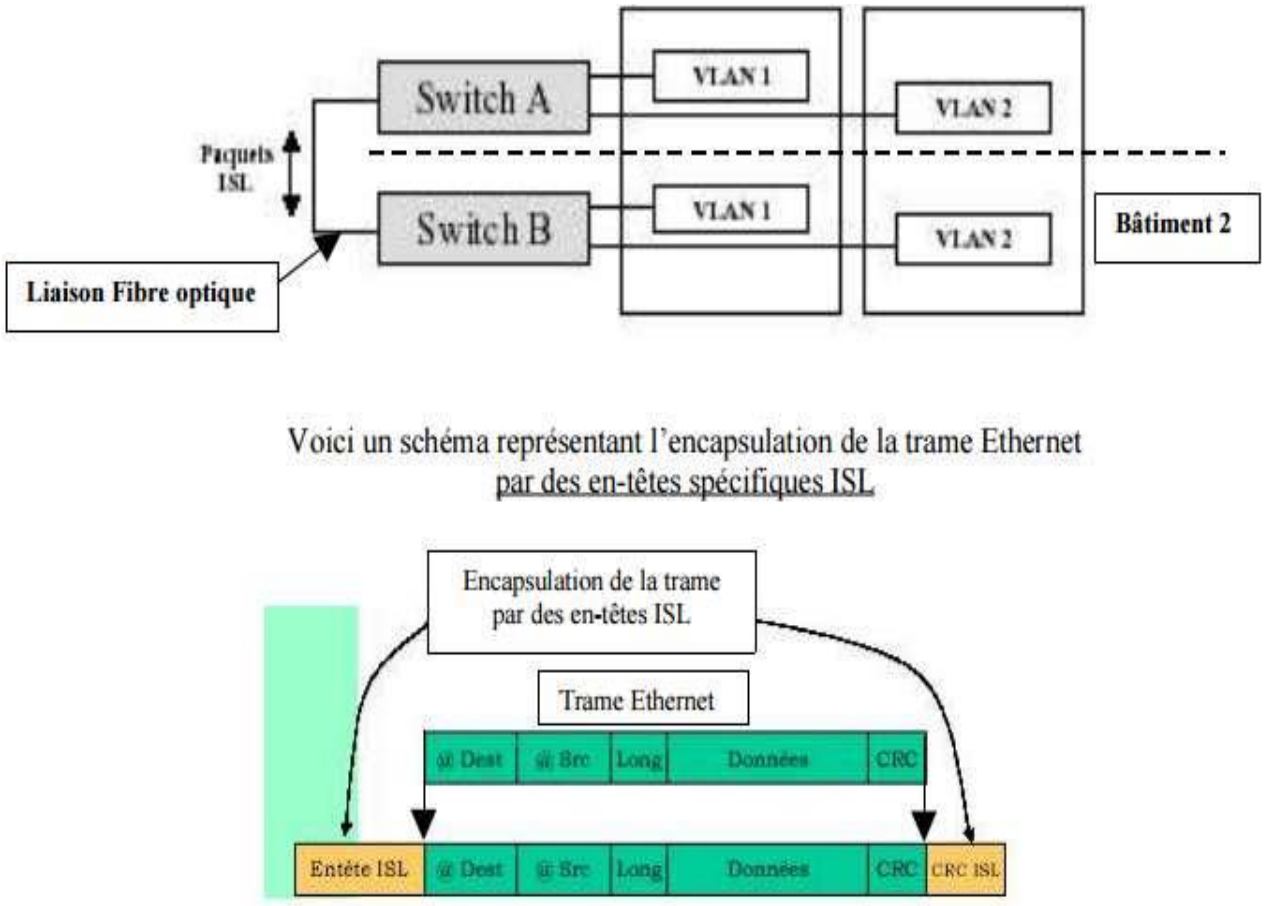

FIGURE 2.4 – la trame Ethernet encapsulé par des en-têtes spécifiques ISL[15]

la structure de la trame ISL :

En-tête ISL

- DA : Adresse multicast de destination (40bits).
- Type : Indique le type de trame (Ethernet, Token Ring, etc.) codé sur 4bits.
- Util : Indique la priorité de traitement de la trame(4bits).
- SA : Adresse MAC source. (48bits).
- LEN : Longueur de la trame encapsulé (16bits).
- AAAA :03 Champ d'une valeur fixe (24bits).
- Bits de poids forts de l'adresse source (24 bits) – Réseau virtuel (16 bits).
- VLAN : Identifiant de VLAN (16bits).
- BPDU : Utilisé par l'algorithme Spanning Tree pour déterminer les informations. topologiques(1bits).
- INDEX : utilsé pour la maintenance (16bits) .

CRC ISL

- CRC (32 bits) (Contrôle à Redondance Cyclique Division polynomiale)

2.5.2 La norme IEEE 802.1Q :

Le standard IEEE 802.1Q fournit un mécanisme d'encapsulation très répondu et implanté dans de nombreux équipements de marques différentes. Comme dans le cas de l'encapsulation ISL précédente, l'en-tête de trame est complété par une balise de 4 octets. Le standard IEEE 802.1Q définit le contenu de la balise de VLAN (VLAN tag) avec laquelle on complète l'en-tête de trame Ethernet. Ce VLAN tag est placé à la suite du champ "Ethertype" de la trame Ethernet, qui lui-même est juste derrière l'adresse MAC Source comme l'illustre la figure qui suit : [15]

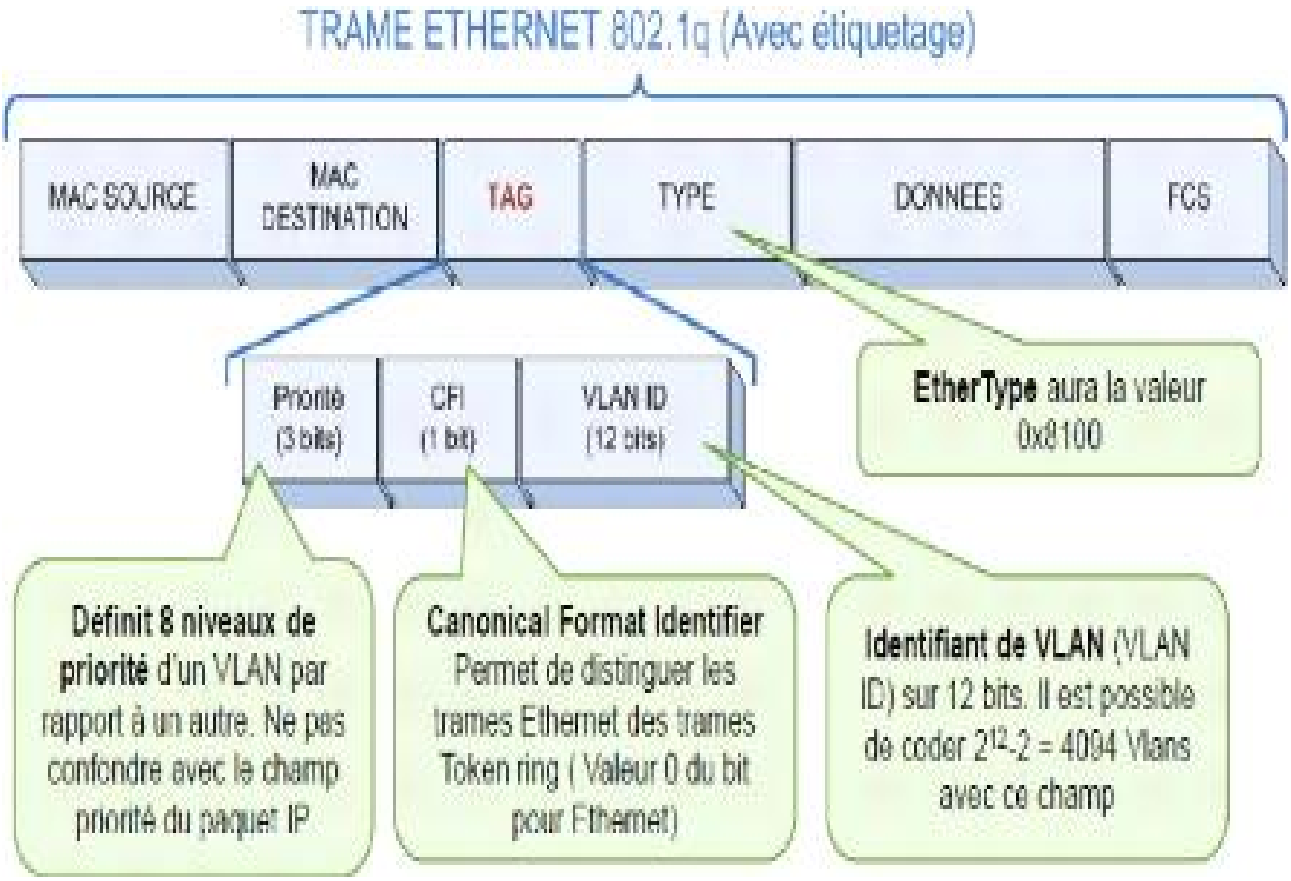

FIGURE 2.5 – La trame IEEE 802.1Q[14]

Tag protocole identifier(TPID) :

C'est la partie qui definie le protocole tag utilisé. Dans le cas de 802.1Q on a la valeur 0x8100.

Tag control information (TCI) :

Elle se compose de trois champs :

- **priorité :** 3 bits utilisés pour definir 8 niveaux de priorité d'un VLAN par rapport a un autre . Il ne faut pas confondre avec le champ priorité du paquet IP.
- **CFI (Canonical Format Identifier) :**Codé sur 1 bit et permet de distinguer les trames ethernet des trames token ring.
- **Identifiant de VLAN :** C'est le champ d'identification du VLAN auquel appartient la trame par l'intermédiare de ce champ de 12 bits. Il est possible de coder 4094 Vlans avec ce champ.

les similitudes entre ISL et IEEE 802.1q,(voir le tableau 2.2)

ISL	IEEE 802.1q.
Encapsule la trame d'origine	Ajoute un en-tête additionnel à la trame d'origine
Comporte un champ d'identification de VLAN de 12 bits	
Utilisation de PVST (Per VLAN Spanning Tree) pour obtenir un arbre STP par VLAN	

TABLE 2.2 – «similitudes entre les deux normes».

2.5.3 le protocole GVRP :

Le protocole GVRP est proposé dans la norme 802.1P. Il permet de diffuser des informations sur les VLANs qui sont déclarés sur les ports d'un switch. Avant toutes choses, il faut savoir que seul les switchs supportant le GVRP peuvent faire du GVRP et que des cartes réseaux peuvent, elles aussi supporter le GVRP parfois.

Si le GVRP est actif sur un commutateur, le protocole GVRP est alors actif au niveau de chaque port du commutateur. Mais le protocole GVRP peut être actif aussi au niveau d'une carte réseau[17].

Le GVRP se décompose en trois parties :

- Une partie applicative que nous appellerons GVRP App. Cette partie contient les informations sur les switchs et les Vlans qu'ils contiennent. Par exemple, on trouvera l'information : "le switch 1 a besoin du Vlan 2".
- Une partie définissant les messages échangés entre les ports d'un même switch que l'on appellera GIP. Cette partie se limite aux échanges internes à un switch.

1. **Les étapes de diffusion d'un Vlan avec le gvrp :**

   Pour bien comprendre le mécanisme de diffusion, nous allons partir d'un exemple ou nous taguons un port à la main.Ce mécanisme est illustré par la figure 2.6

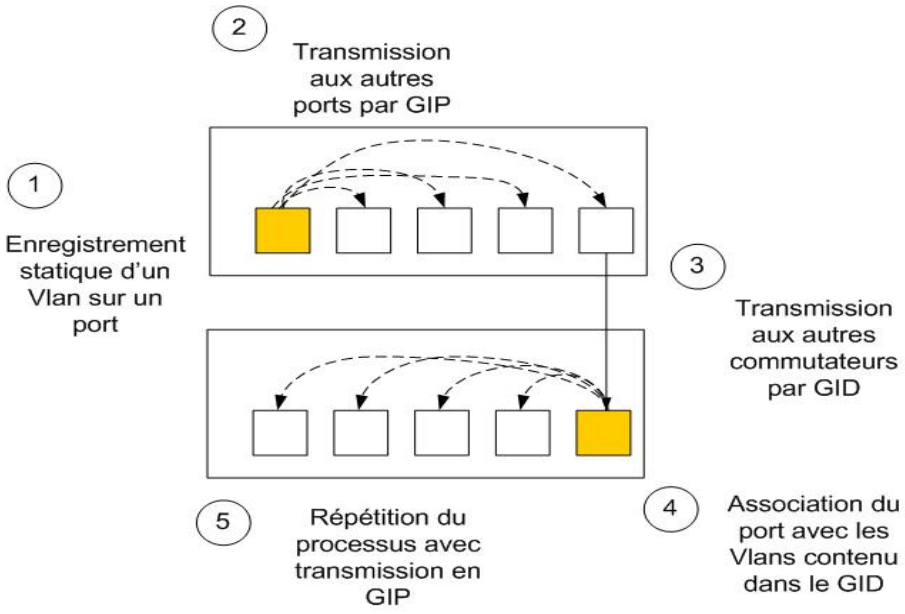

FIGURE 2.6 – Les étapes de diffusion d'un Vlan avec le GVRP [17].

- **Première étape :** le Vlan 2 est configuré sur le port 1 du switch 1. Ce dernier enregistre alors l'information dans sa table de Vlan en associant le Vlan 2 au port 1 et enregistre le Vlan 1 dans sa liste de Vlan.

- **Deuxième étape :** L'information du Vlan 2 est propagé sur les autres ports du switch avec l'information "le port 1 nécessite le Vlan 2".

- **Troisième étape :** si le port n'est pas tagué, il ne se tague pas et envoi l'information aux autres switchs par GID.

- **Quatrième étape :** le switch 2 récupère l'information en l'informant que le switch 1 veut les informations sur le Vlan 2. Il tague donc le port d'ou il a reçu le GID en Vlan 2. Si le Vlan 2 ne fait pas parti de sa liste de Vlan, il l'enregistre et il réemet l'information en GIP comme précédemment.

2. **Limitation de propagation :** il est possible de limiter les transferts GID et GIP sur les ports grâce aux menus de configuration. On peut ainsi placer les états suivants :
   - Le mode apprentissage : c'est le mode par défaut qui fonctionne comme nous l'avons vu précedemment
   - Le mode bloqué : le port ne s'associe pas au Vlan mais le transmet quand même en GID.
   - Le mode non actif : le port ne s'associe pas au Vlan et ne le propage pas.

2.5.4 Le mode trunk :

Un trunk est une connexion physique unique sur laquelle on transmet le trafic de plusieurs réseaux virtuels. Les différents liens constituant ce trunk seront alors utilisés simultanément, permettant ainsi d'augmenter le débit inter-switch. Du point de vue du switch, la connexion à un trunk est vue comme résolution d'adresse source et/ou destination, voire d'une négociation. 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) [18].

Les trunks peuvent être utilisés :

- Entre deux commutateurs : c'est le mode de distribution des réseaux locaux les plus courants.
- Entre un commutateur et un hôte :c'est le mode de fonctionnement à surveiller étroitement.
- 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.

Le schéma ci-dessous illustre la liason trunk entre des commutateurs

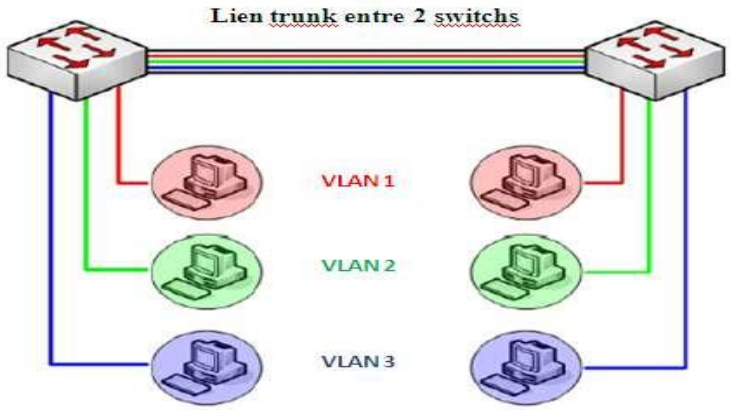

FIGURE 2.7 – Utilisation du trunk entre deux commutateurs [15].

2.6 les Protocoles d'administration des VLANs :

2.6.1 le protocole VTP (Vlan Trunking Protocol) :

Afin de ne pas redéfinir tous les VLANs existant sur chaque commutateur, CISCO a développé un protocole permettant un héritage de VLANs entre commutateurs. C'est le protocole VTP. Celui-la est basé sur la norme 802.1q et exploite une architecture client- serveur avec la possibilité d'instancier plusieurs serveurs [19].

1. **Fonctionnement de VTP :**

   Les messages, VTP diffusent des annonces de création, de suppression ou de modification de VLAN. Lors de chaque création/suppression/modification, une variable appelée RN (Révision Number) s'incrémente (initialement 0 puis 1 puis 2 puis 3, etc.) . Le switch Server envoie un message VTP avec la nouvelle valeur du RN, les autres switchs comparent le RN reçu du switch Server avec le RN qu'ils stockent en local, Si ce dernier est plus petit (logiquement) ,alors les switchs se synchronisent avec le Server et récupèrent la nouvelle base de données des VLANs. Le switch possède 3 modes VTP : client, transparent ou server (voir la figure ci-après) [20] :

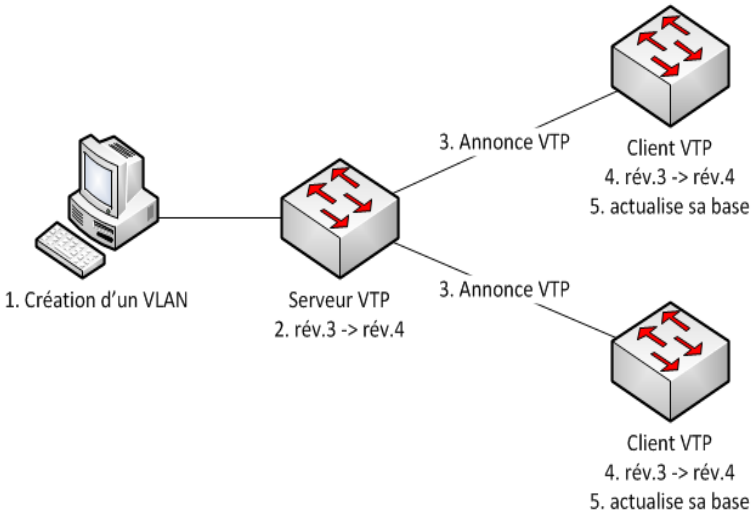

FIGURE 2.8 – Fonctionnement de VTP [20].

2. **Les modes du VTP :**

- **VTP Server :** le switch en mode Server (mode par défaut) , permet à l'administrateur de faire des modifcations sur les VLANs et de les diffuser automatiquement vers tous les switchs du réseau (voir la figure ci-dessous).

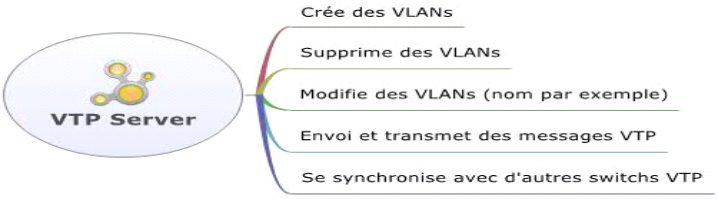

FIGURE 2.9 – VTP server.

- **VTP client :**dans lequel le commutateur applique la configuration émise par un commutateur en mode serveur (voir la figure ci-dessous).

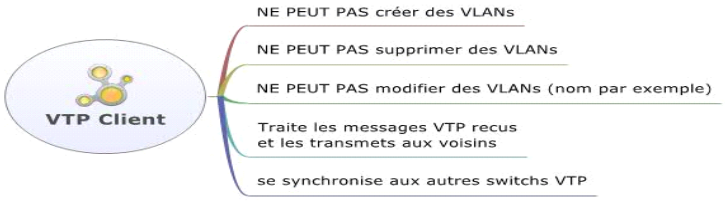

FIGURE 2.10 – VTP client.

- **VTP Transparent :** Le switch en mode Transparent reçoit les mises à jour et les transmet sans les prendre en compte. Il permet à l'administrateur de faire toutes sortes de modifications sur les VLANs (en local uniquement). Donc il ne propage pas ses modifications vers tous les switchs du réseau (voir la figure ci-dessous).

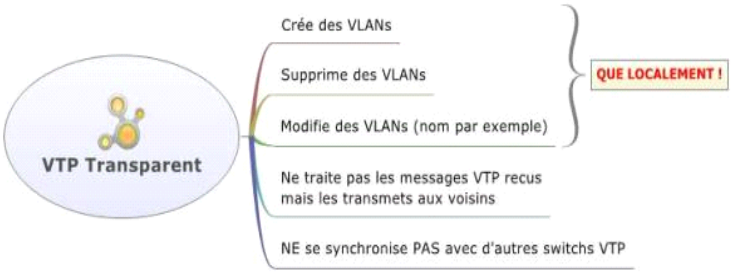

FIGURE 2.11 – VTP Transparent.

2.6.2 Protocole Spanning-Tree :

Le protocole STP (Spanning Tree Protocol) est un protocole de couche deux qui fonctionne sur des ponts et des commutateurs. La spécification du protocole STP est IEEE802.1D. L'objectif principal du protocole STP est de vérifier que vous ne créez pas de boucles lorsque vous avez des chemins redondants dans votre réseau. Les boucles sont fatales pour un réseau [21].

Fonctionnement de STP :

Une topologie physique redondante fournira des chemins multiples visant à améliorer la fiabilité d'un réseau. Toutefois, elle présente le désavantage de créer des boucles dans le réseau. Pour résoudre ce problème, STP crée au sein de cette topologie redondante un chemin sans boucle basé sur le chemin le plus court. Ce dernier est établi en fonction de la somme des coûts de liens entre les commutateurs. Ce coût est une valeur inverse à la vitesse d'un port, car un lien rapide aura un coût moins élevé qu'un lien lent. Aussi, un chemin sans boucle suppose que certains ports soient bloqués et pas d'autres. STP échange régulièrement des informations (appelées des BPDU - Bridge Protocol Data Unit) afin qu'une éventuelle modification de topologie puisse être adaptée sans boucle.

2.6.3 Le protocole DHCP :

DHCP(Dynamic Host Configuration Protocole) :est un protocole qui permet a un ordinateur qui se connect sur un rseau local d'obtenir dynamiquement et automatiquement sa configuration IP. Le but principal étant la simplification de l'administration d'un réseau. On voit généralement le protocole DHCP comme distributeur d'adresses IP,mais il a été conçu au départ comme complément au protocole BOOT(Bootstrap Protocole) qui est utilisé par exemple lorsque l'on installe une machine a travers un réseau (on peut effectivement installer complètement un ordinateur, et c'est beaucoup plus rapide que de le faire a la main).Cette dernière possibilité est très intéressante pour la maintenance de gros parcs machines[22].

2.7 Liste de controle d'accés :

Une liste de contrôle d'accès (ou ACL) est une série de commandes IOS qui déterminent si un routeur achemine ou abandonne les paquets en fonction des informations contenues dans l'en-tête de paquet. Les listes de contrôle d'accès font partie des fonctionnalités les plus utilisées du logiciel Cisco IOS (voir la figure ci-dessous) [23].

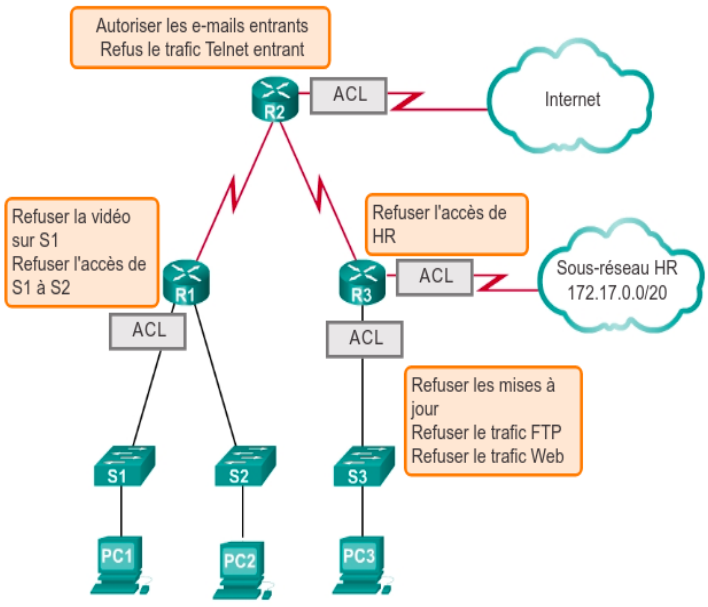

FIGURE 2.12 – Les ACLs [23].

2.7.1 les taches de la liste d'accés :

Une fois que la configuration est faite , les listes de contrôle d'accès assurent les tâches suivantes[23] :

- Elles limitent le trafic réseau pour accroître les performances réseau.
- Elles contrôlent le flux de trafic. Les listes de contrôle d'accès peuvent limiter l'arrivée des mises à jour de routage. Si aucune mise à jour n'est requise vu les conditions du réseau, la bande passante est préservée.
- Elles fournissent un niveau de sécurité de base pour l'accès réseau.
- Elles filtrent le trafic en fonction de son type. Ainsi, une liste de contrôle d'accès peut autoriser le trafic des e-mails, mais bloquer tout le trafic Telnet.
- Elles filtrent les hôtes pour autoriser ou refuser l'accès aux services sur le réseau. Les listes de contrôle d'accès peuvent autoriser ou refuser à un utilisateur l'accès à certains types de fichier, tels que FTP ou HTTP.

2.7.2 Les types des listes de controle d'accés :

Voici les trois types existant de ACL[24] :

1. **Listes de contrôle d'accès standard :**

   Les listes d'accès standard vérifient l'adresse d'origine des paquets IP qui sont routés. Selon le résultat de la comparaison, l'acheminement est autorisé ou refusé pour un ensemble de protocoles complet en fonction des adresses réseau, de sous-réseau et d'hôte.

2. **Listes de contrôle d'accès étendues :**

   Les listes d'accès étendues sont utilisées plus souvent que les listes d'accès standard car elles fournissent une plus grande gamme de contrôle.Les listes d'accès étendues vérifient les adresses d'origine et de destination du paquet, mais peuvent aussi vérifier les protocoles et les numéros de port.

3. **Listes de contrôle d'accès nommées :**

   Les listes de contrôle d'accès nommées IP ont été introduites dans la plate-forme logicielle Cisco IOS version 11.2, afin d'attribuer des noms aux listes d'accès standard et étendues à la place des numéros.

Conclusion

Nous avons vu au cours de ce chapitre que les Vlans vont permettre à l'entreprise de penser à des réorganisations futures sans se soucier de sa situation physique et que les VLANs présentent plusieurs enjeux comme :la sécurité,la limitation de domaines de diffusion et la limitation de cout de déplacement des utilisateurs entre les services au sein de l'entreprise.

CHAPITRE 3 : PRESENTATION DE L'ORGANISME D'ACCUEIL

Chapitre 3

Présentation De L'Organisme D'Accueil

Dans ce chapitre, nous allons présenter l'entreprise d'accueil NAFTAL district carburant de Bejaia , avec ses différentes activités.

3.1 Situation géographique :

NAFTAL CBR,comme le montre la figure 3.1, se trouve à l'entrée de la ville de Bejaia par la RN 12, au lieu-dit Bir Slem , jouxtant la bordure de la route côté droit, soit pour sortir de la ville de Bejaia, soit pour entrer à la ville par le boulevard Krim Belkacem ou bien par Bir Slem.

FIGURE 3.1 – Situation géographique de l'entreprise naftal bejaia.

3.2 Historique de NAFTAL :

Issue de SONATRACH(société nationale pour la recherche, transport, production, transformation, et commercialisation des hydrocarbures)l'entreprise nationale de raffinage et de distribution de produits pétroliers à été crée par le décret N80-101 du 06 avril 1980.

Entrée en activité le 01 janvier1982, elle est chargée de l'industrie de raffinage et de la distribution de produits pétroliers.

Le 04 mars 1985, les anciens districts (Carburants, lubrifiants, pneumatique et bitume) ont été regroupés sous le nom UND (unité NAFTAL de distribution).

En 1987, l'activité raffinage est séparée de la distribution, conformément au Décret n 87-189 du 25 Août 1987 modifiant le décret n80-101 du 6 Avril 1980, modifié, portant création de l'Entreprise nationale de raffinage et de distribution de produits pétroliers, il est créé une entreprise nationale dénommée :
« entreprise nationale de commercialisation et de distribution de produits pétroliers », sous le sigle de « NAFTAL ».

A partir de 1998, elle change de statut et devient société par action filiale a 100 de SONATRACH, en intervenant dans les domaines suivants :

- De l'enfûtage GPL
- De la formulation des bitumes
- De la distribution, stockage et commercialisation des carburants, GPL, lubrifiants, bitumes, pneumatique, GPL /produits spéciaux.
- Du transport des produits pétroliers.

Elle est chargée, dans le cadre du plan national de développement économique et social, de la commercialisation et de la distribution des produits pétroliers et dérivés.

- Le 01 janvier 2000, l'activité GPL enfûtage est séparée de l'activité CLP.

- Par décision n S 554 du 29 mars 2000, il a été procédé à l'organisation générale de la division CLP et l'identification des zones de distribution « CLP » (carburants, lubrifiants et pneumatiques).

- Par décision n S 555 du 29 mars 2000, il a été procédé à la création des zones de distribution CLP.

- Par décision n S 606 du 10 Février 2001, il a été procédé à l'organisation et la classification des centres Bitumes de la Division Bitume.

- Par décision n S 705 du 17 Juin 2002, il a été procédé à la dénomination des zones de distribution CLP et GPL en District.

- Par décision n S 766 du 22 Décembre 2003, il a été procédé à la dissolution de la branche CLPB.

- Par décision n S 770 du 03 Janvier 2004, il a été procédé à la dissolution des districts CLP et création des districts commercialisation.

- A partir du 01.12.2006 l'activité Carburant est séparée de l'activité commercialisation.

3.3 NAFTAL District Carburants de Bejaia :

Le District CBR Bejaia est organisé comme suit :

3.3.1 Direction :

Sont rattachés : Une secrétaire, le responsable de la sécurité industrielle, le laboratoire, le juridique et les différents départements et dépôts carburants.

Ses principales tâches et responsabilités sont :

- Identifier et recenser les infrastructures, équipements et autres moyens matériels (camions, canalisations) relevant de l'activité carburants du district ainsi que les structures d'organisation (services ''maintenance installations fixes", ''surveillance et entretien canalisations", ''reconnaissance produits",etc.) et les moyens humains œuvrant pour l'activité carburante ;
- Suivre les plans établis par la Branche Carburants pour l'approvisionnement et le ravitaillement en carburants des dépôts et communiquer régulièrement les états d'exécution aux structures concernées ;

- Exécuter les programmes de distribution établis par les districts commercialisation pour la livraison de la clientèle ;
- Gérer les stocks en carburants au niveau des dépôts et communiquer régulièrement des points de situation aux structures concernées de la branche ;
- Suivre l'exploitation et la maintenance des infrastructures de stockage et autres moyens (camions, canalisations) carburants de la branche rattachés au district ;
- Est responsable, en liaison avec les structures HSEQ, de la sécurité industrielle des installations, équipements et moyens des centres carburants et canalisations ;
- Est responsable, en liaison avec les responsables concernés des centres carburants et canalisations, de la sûreté interne des installations et moyens ;
- Gérer, en liaison avec les structures de la Branche, les relations avec les directions des raffineries NAFTEC, les directions régionaux STPE et SNTR ;
- Ordonnancer les factures NAFTEC, STPE, cabotage et transport SNTR tiers et les transmettre aux structures de la branche pour règlement ;
- Approuver les bordereaux inter unités (BIU) émis par les districts commercialisation vers le district carburants ;
- Traiter le bon mouvement interne (BMI) en liaison avec les chefs de centres carburants lors des conseils de direction de district ;
- Exécuter les plans, budgets et autres objectifs arrêtés par la Branche et l'entreprise et proposer voire prendre des mesures correctives en cas de dérive ;
- Veiller à la tenue rigoureuse de la comptabilité des flux physiques et financiers et élaborer le bilan consolidé du district ;
- Veiller au respect de la réglementation en vigueur dans les domaines d'activité technique, transport, stockage, sécurité industrielle, protection de l'environnement, finances, comptabilité, fiscalité, assurance, législation et relations de travail ;
- Gérer les relations avec les partenaires locaux (fournisseurs et clients) et les autorités et administrations locales ;
- Prêter assistance, autant que de besoin, aux autres districts dans tous les domaines d'activités.

3.3.2 Département informatique

Le département informatique est assuré par un chef de département.Son rôle principal est de garantir la continuité de service des systèmes informatiques déployés au niveau du district et des centres opérationnels, et de veiller à la mise à disposition des informations de gestion aux structures du district, les branches et les structures centrales.
Le département est divisé en deux services :

1. **Service système et réseaux**

   Ce service est composé d'un(1) chef de service SYS RES, d'un(1) ingénieur informatique et de deux (2) analystes (voir le shéma illustré çi-dessous).

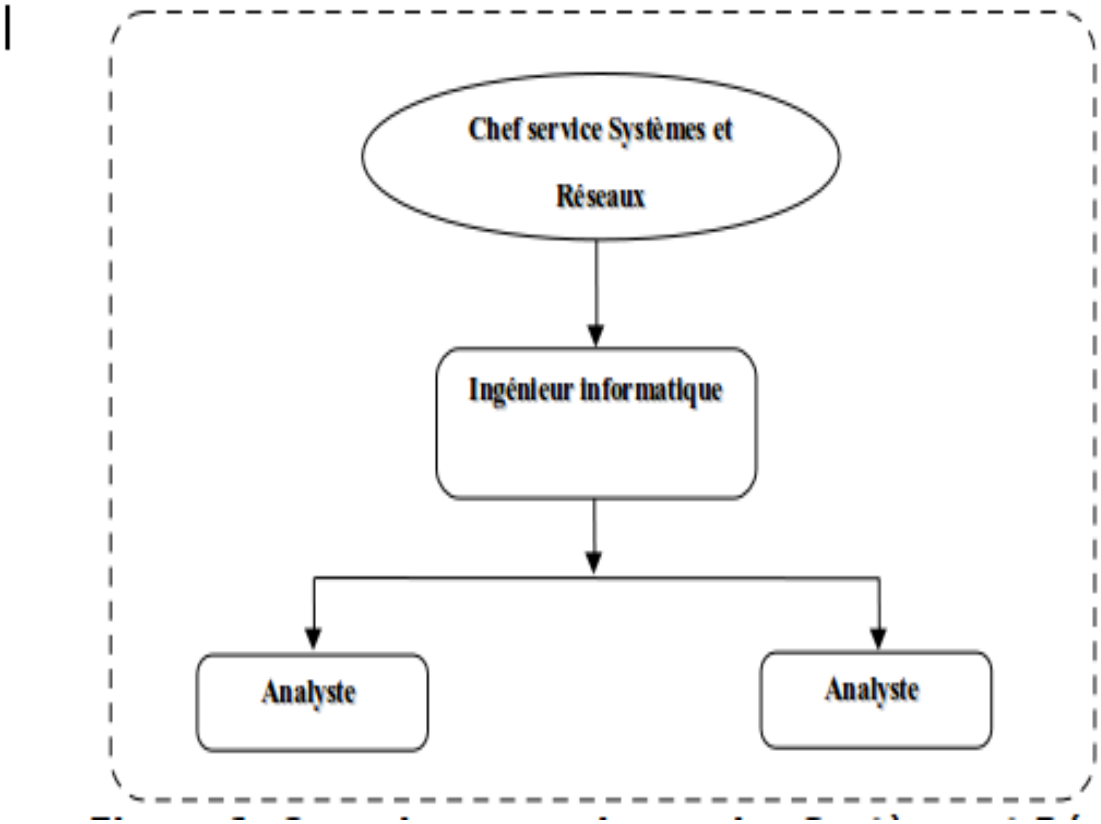

FIGURE 3.2 – Organigramme du service système et réseau.

Le rôle du service systèmes et réseau est de prendre en charge les infrastructures réseaux filaires et Wifi, et des services généralistes (sécurité, distribution logiciel, gestion des postes de travail...).Il assure aussi la maintenance des équipements informatiques et établi des formations sur le fonctionnement de certain logiciels ou applications.

(a) Ce service assure deux taches suivantes :

- **La maintenance informatique :** assure la maintenance corrective de tous types de matériels informatiques. Il analyse les causes des pannes et y apporte la solution adéquate dans les meilleurs délais. Il peut être amené à intervenir sur des logiciels et à effectuer tout ou partie de l'installation et de la mise en route des matériels informatiques. Prendre en chargé aussi l'installation de matériels neufs, de modification et d'adaptation des matériels.
- **La mise en place et la configuration de réseau informatique de l'entreprise** , il intervient à chaque étape de la mise en place d'un réseau local.Il s'occupe intégralement de fournir le matériel nécessaire et de faire :

  A. La pose du câblage informatique.

  B. La configuration des postes utilisateurs, système d'exploitation, messagerie, internet, intranet, FTP.

  C. La gestion des domaines, des groupes et des ressources du réseau.

  D. L'administration les serveurs de réseaux (serveur FTP, messagerie, web,. . .).

2. **Service information de gestion (ING)**

   Ce service est composé d'un(1) chef de service ING et d'un (1) Cadre d'étude (voir la figure 3.3).

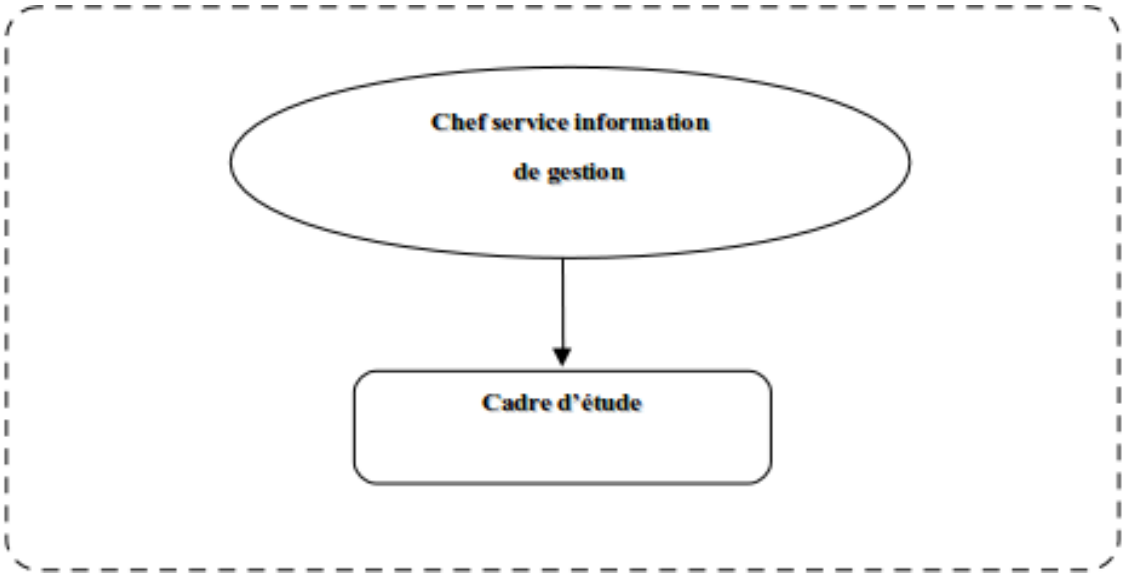

FIGURE 3.3 – Organigramme du service information de gestion.

Les rôles du service information de gestion sont :

- Gérer et mettre à jour une banque de données de toutes les activités du district.
- Procéder au calcul de la PRC (Prime de Rendement du Collectif) des différents collectifs du District.
- Consolider les différents plans et budgets des structures du District.
- Préparer les différentes présentations (COD, réunions de travail, regroupements, actions de communication, etc.).
- Collecter, contrôler et analyser les informations concernant les activités du District.
- Participer à l'élaboration des rapports d'activité périodiques et les tableaux de bord.
- Assurer la diffusion des PV des conseils de direction du district aux membres présents et aux structures centrales de la branche carburants.

3.3.3 Département AMG (administration et moyens généraux)

Les missions du département AMG sont :

— Assurer la gestion des moyens généraux du district ;

— Assurer la gestion des ressources humaines ;

— Assurer la gestion de l'administration ;

— Assurer la gestion des œuvres sociales et culturelles.

Service administration

(a) **Section gestion du personnel :**

— Gestion administrative du personnel ;

— Veiller à l'application de la réglementation ;

— Tenir à jour les différents registres réglementaires (registre du personnel, registre des congés, registre des accidents de travail. . . etc) ;

— Suivi du pointage du personnel permanent et temporaire ;

— Elaboration et suivi du planning des congés annuels ;

— Etablissement des titres de congés annuels et récupérations ;

— Suivi et enregistrement des notes de frais de missions ;

— Etablissement des attestations de travail et Divers documents ;

— Gestion du volet disciplinaire ;
— Gérer les mouvements (congés, maladies, absence, retraite, affectation . . .) ;
— ormalise et suit les prêts véhicules.

(b) **Section gestion paie :**

— Préparation, établissement et vérification de la paie ;
— Etablir les déclarations fiscales et parafiscales (CNAS, impôts) ;
— Etablir les relevés des émoluments.

(c) **Section prestations sociales :**

— Gérer les dossiers (allocation familiale) et procéder a leur paiement ;
— Contrôle des dossiers médicaux et leurs dépôts auprès de la CNAS et MIP ;
— Remboursement des prestations sociales CNAS et MIP ;
— Gestion des dossiers de retraites.

Services ressources humaines

— Gérer les emplois, carrières et niveaux des effectifs ;
— Elaboration des prévisions en matière de salaires et charges patronales du district ;
— Etablissement et suivi des prévisions, des budgets et des plans de formations du personnel ;
— Veille à l'application de la réglementation en vigueur ;
— Tenir à jour le fichier personnel ;
— Elaboration des tableaux de bord ;
— Traitement des requêtes du personnel ;
— Préparation et étude des dossiers de la commission du personnel ;
— Suivi de l'apprentissage ;
— Suivi des stagiaires ;

Services des moyens généraux

Ses activités sont assurées par trois sections :

(a) **Section BOG (bureau d'ordre) :**

— Assurer la réception, l'enregistrement et le dispatching du courrier pour toutes les structures, constituer et actualiser les annuaires téléphoniques et Standards.

(b) **Section entretien bâtiment :**

— Assurer l'entretien des locaux, meubles et immeubles ;
— Assurer la gestion des charges (Electricité, eau, téléphone. . . ..)

(c) **Section économat :**

— la gestion du magasin pour l'approvisionnement en consommable de bureau et informatique et fournir les documents de gestion.

— Satisfaire les commandes des structures.

Cellule OSC (Oeuvres sociales et culturelles)

Elle est chargée de la gestion de :

— Colonies de vacance et camps de toile, prêts sociaux, cures thermales, compétition sportive et OMRA...

— Aide financières aux veuves et orphelins et frais d'obsèques.

3.3.4 Département finances et comptabilité

Le département finances et comptabilité a pour mission de :

— Coordonner et suivre toutes les activités de comptabilité de trésorier, budget et patrimoine ;

— Consolider, analyser les états comptables et veiller à la sincérité des comptes du District ;

— Veiller à la concordance des écritures comptables avec les flux physiques et financiers.

Il comprend trois services à savoir :

1. **Service trésorerie :**

   Il est composé de deux sections, la section recettes et la section dépense.

   Sa mission est de :

   — Suivre et contrôler les flux, recettes et dépenses de trésorerie.

   — Traiter les dossiers de paiement d'investigation, des fournisseurs et d'autres dépenses.

   — Etablir les situations de rapprochement des comptes (recettes et dépenses)

   — Contrôler et effectuer les comptabilisations des comptes et grands livres de trésorerie

   — Etablir des rapports d'activités.

2. **Service comptabilité générale**

   Il est composé de deux sections, la section SVCD et la section comptabilité. Sa mission est de :

   — Procéder aux écritures comptables conformément aux préconisations du plan comptable national.

   — Élaborer les documents comptables (Bilans, balances et livres)

   — Contrôler les arrêtés de comptes et préparer les inventaires et bilans

   — Élaborer les analyses et synthèses comptables

— Procéder aux opérations des clôtures et réouvertures des comptes

3. **Service budgets et coûts**

   Sa mission est de :

   — Elaborer les budgets prévisionnels d'investissement et de fonctionnement du District ;

   — Consolider l'ensemble des charges nécessaires à la détermination du coût ;

   — Contrôler et traiter les situations financières du District ;

   — Procéder aux ajustements des budgets et crédits ;

   — Assurer le suivi régulier de la comptabilité analytique.

3.3.5 Département transport technique

Il a pour mission de :

— Élaborer les plans de maintenance préventive et curative des équipements, dépôts, et canalisation et en suivre l'exécution.

— Élabore les plans annuels et pluriannuels de transport, en prenant en charge les besoins de distribution net ravitaillement des produits commercialisés.

— Suivi de la réalisation des travaux.

— Elaborer les plans et budgets d'investissement (rénovation, extension, remise à niveau, remplacement) des installations fixes, canalisation, réseau de stations-services et autres.

— Etablir un rapport d'activité périodique

Ce département comporte les services suivants :

1. **Service exploitation et maintenance**

   Sa mission est de :

   — Vérifier l'application des prescriptions du règlement d'exploitation, de sécurité des équipements et des installations fixes.

   — Etablir les performances de maintenance.

   — Assurer la maintenance des installations au niveau des dépôts carburants.

2. **Service études et réalisation**

   Sa mission est :

   — D'établir la partie technique des cahiers de charges.

   — De contrôler et diriger les différents travaux.

   — De suivre les travaux programmés ayants traits aux projets.

Le District dispose de deux (02) dépôts carburants à Bejaia, un (01) à TAHER /W.JIJEL, un (01) à Bordj Bou Arreridj et un (01) à M'SILA.

La figure 3.4, représente l'organigramme du district englobant tout les services qui lui appartient :

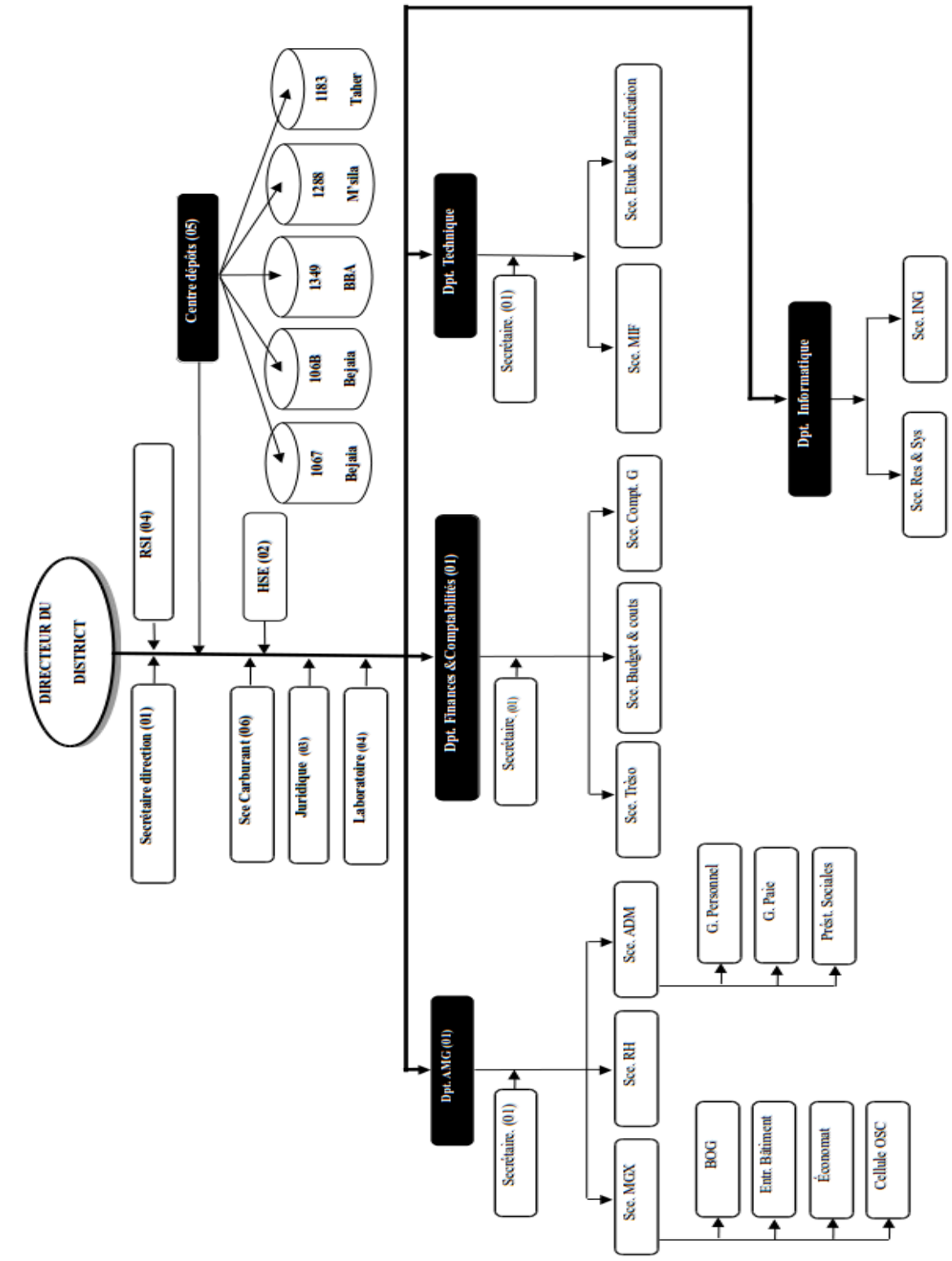

FIGURE 3.4 – Schéma Organisationnel du District CBR BEJAIA.

3.4 Etude de l'exitant :

3.4.1 Architecture existante :

Le réseau local du District CBR de Bejaia interconnecte tous les ordinateurs du parc Informatique et leur permet d'accéder aux ressources du réseau et à internet. Pour adresser facilement les hôtes du réseau, un service DHCP est fonctionnel dans le LAN. Les machines du parc ont trois systèmes d'exploitation, Windows 7,10, et Windows server 2012 pour leurs serveur. Des imprimantes sont mises en réseau pour étre partagées entre les employés afin que ceux- ci puissent y accéder sans avoir à transporter les documents d'un poste a un autre. Il est également à noter que, ce réseau LAN se compose d'un réseau filaire et d'un réseau wifi pour permettre l'accès à internet aux visiteurs. Des onduleurs sont également mis à contribution en cas de coupures brusques du courant électrique. On dénombre un dans chacun des deux services informatiques et d'autre dans les services cités plus haut.

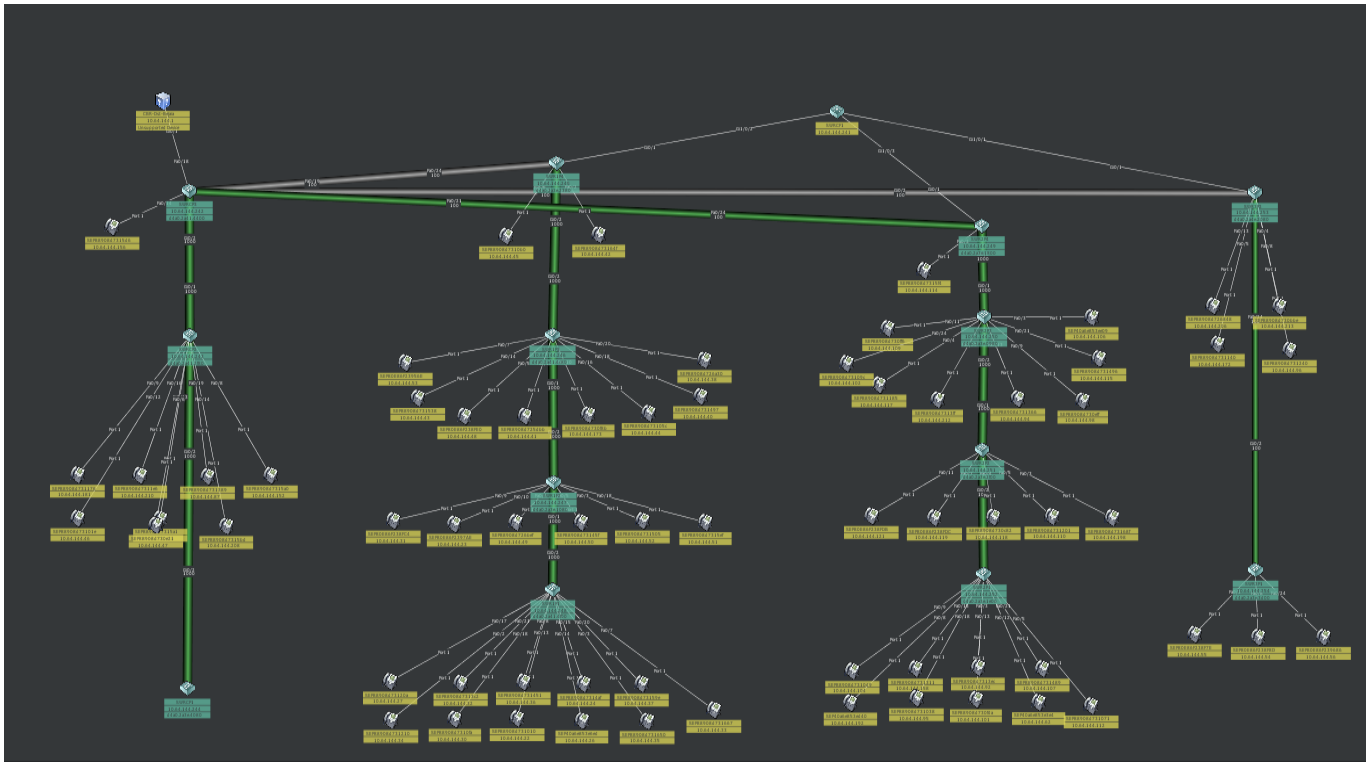

FIGURE 3.5 – Architecture De Réseau De Naftal Détaillé.

3.4.2 Parc informatique

1. Environnement client : le tableau 3.1 présente les équipements client du parc informatique de district

Equipement	Nombre	Type et marque.
PC bureau	89	HP Compac 8300.
PC portable	04	HP Compac 600pro.
Imprimentes	15	EPSON Aculaser M2000 .
Photocopieur	05	Xerox Workcentre 5020 DN.

TABLE 3.1 – « Environnement client».

2. Environnement serveur : le district dispose d'un serveur 2012 qui permet de gérer et de configurer les différents équipements de leur réseaux.
3. Matériels d'interconnexion : les équipements d'interconnexion représentent le coeur du réseau dans une architecture.S'ils sont mal dimensionnés, ils pourront avoir des effets négatifs sur le trafic du réseau, pouvant entrainer la détérioration de celui-ci. Dans notre cas d'étude, l'infrastructure du réseau de district embryonnaire, comporte 13 commutateurs CISCO CATALYSTE 2960 de 24 ports et un commutateur fibre optique CISCO 2911 pour l'interconnexion des différents clients et d'un routeur CISCO 3750.

3.4.3 Les applications

Le système d'exploitation utilisé par les machines au sein du district est Windows 10 et 7 pour les ordinateurs de bureau et portable.Un certain nombre d'applications sont utilisées, il s'agit :

SD-COM :système informatique pour la gestion de l'activité distribution et commercialisation au sein des CDS.

NAFT-GD :contrôlée des stations-service en gérance direct.

WINCANAL :système de comptabilité analytique.

NAFTimmologiciel de gestion des biens mobile et immobile (véhicule, Bureau, table, pc. . ..).

POSTPAIE :gestion Paie des employés.

NOVACH RH :application web pour la gestion du personnels.

GIF :application web pour la gestion des installations fixe (pompe, vane,. . .etc)

V15 :application web pour établissement des bons de chargement volume a 15.

REF TRANSPORT :application web pour le suivie des transporteurs.

SGC : Logiciel de gestion des créances.

BASSMA : Application pour la gestion pointage des employés.

3.4.4 Problématique :

Durant notre période de stage au sein du district CBR de Béjaia, nous avons remarqués qu'elle dispose d'un réseau local de taille importante composé d'une plateforme de services reliant les différents départements et composants de ce district Nous avons pu mettre le point sur manquement du réseau à savoir :

- un seul et unique domaine de diffusion ce qui implique une grande surcharge sur le réseau.

La figure ci-dessous montre l'architecture simplifiée du réseau de naftal.

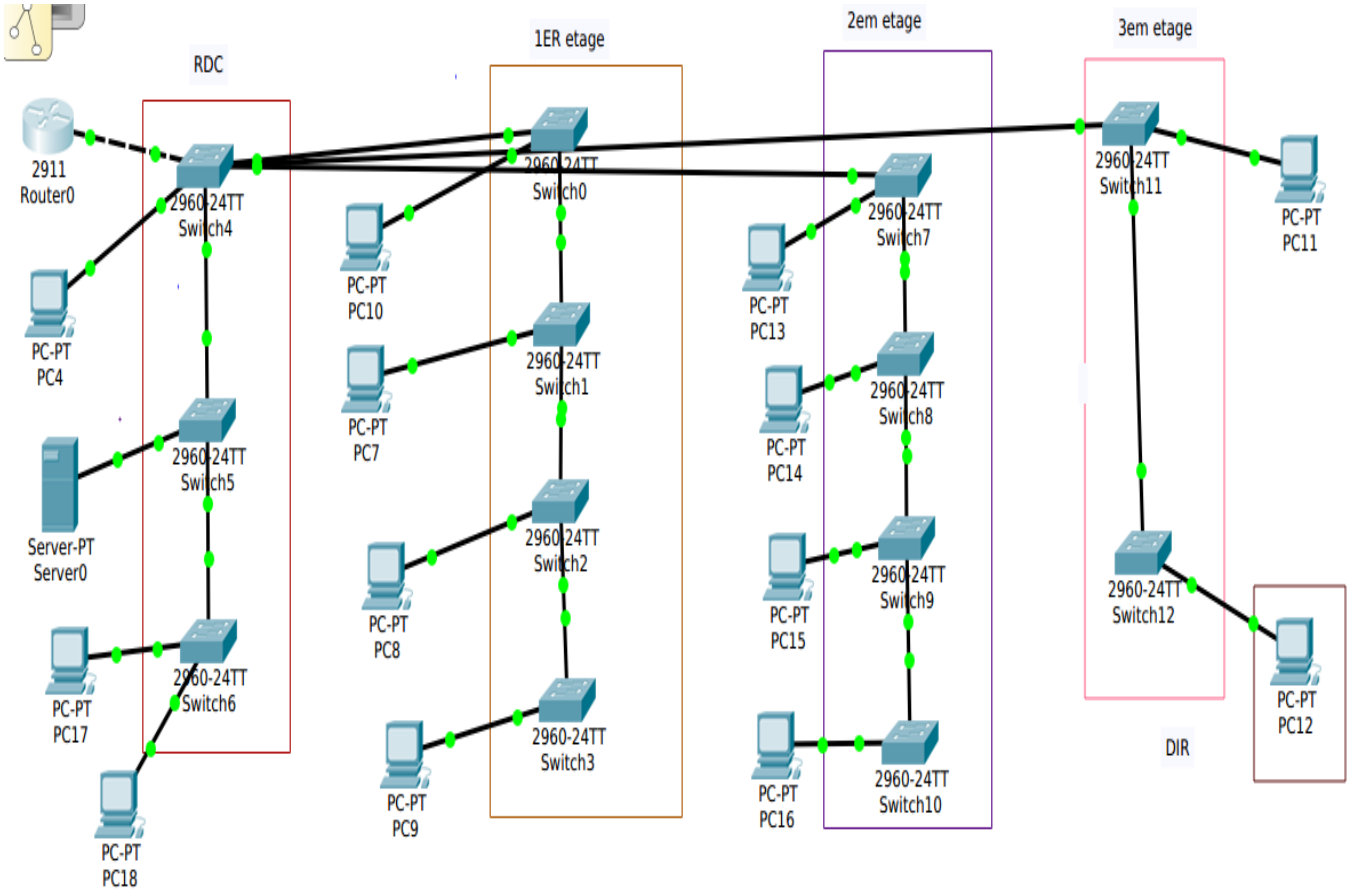

FIGURE 3.6 – Architecture du réseau sans vlans

3.5 Contexte du projet a réaliser :

3.5.1 Présentation du projet :

Notre projet s'intitule :" Etudes et proposition d'une solution VLAN au sein de l'entreprise Naftal CBR ", qui consiste à mettre en place une solution VLAN d'un réseau local au sein de district CBR de bejaia afin d'apporter des améliorations au réseau de l'entreprise et de le bien gérer.

Notre objectif principal est de garantir une meilleure exploitation et attribution du réseau, ainsi remédier aux problèmes rencontrés durant notre petite période de stage et d'essayer de trouver une solution optimale pour la gestion du réseau local du district.

3.5.2 Solution proposée :

Le but de notre projet est d'offrir une bonne organisation de réseau En effet une bonne organisation permettra une optimisation du réseau en terme d'efficacité et de performance. l'organisation du réseau au sein de l'entreprise NAFTAL Carburants se fera a l'aide de segmentation en VLAN.En effet cette solution est la meilleure et le plus adéquate, en vue des avantages qu'elle offre.

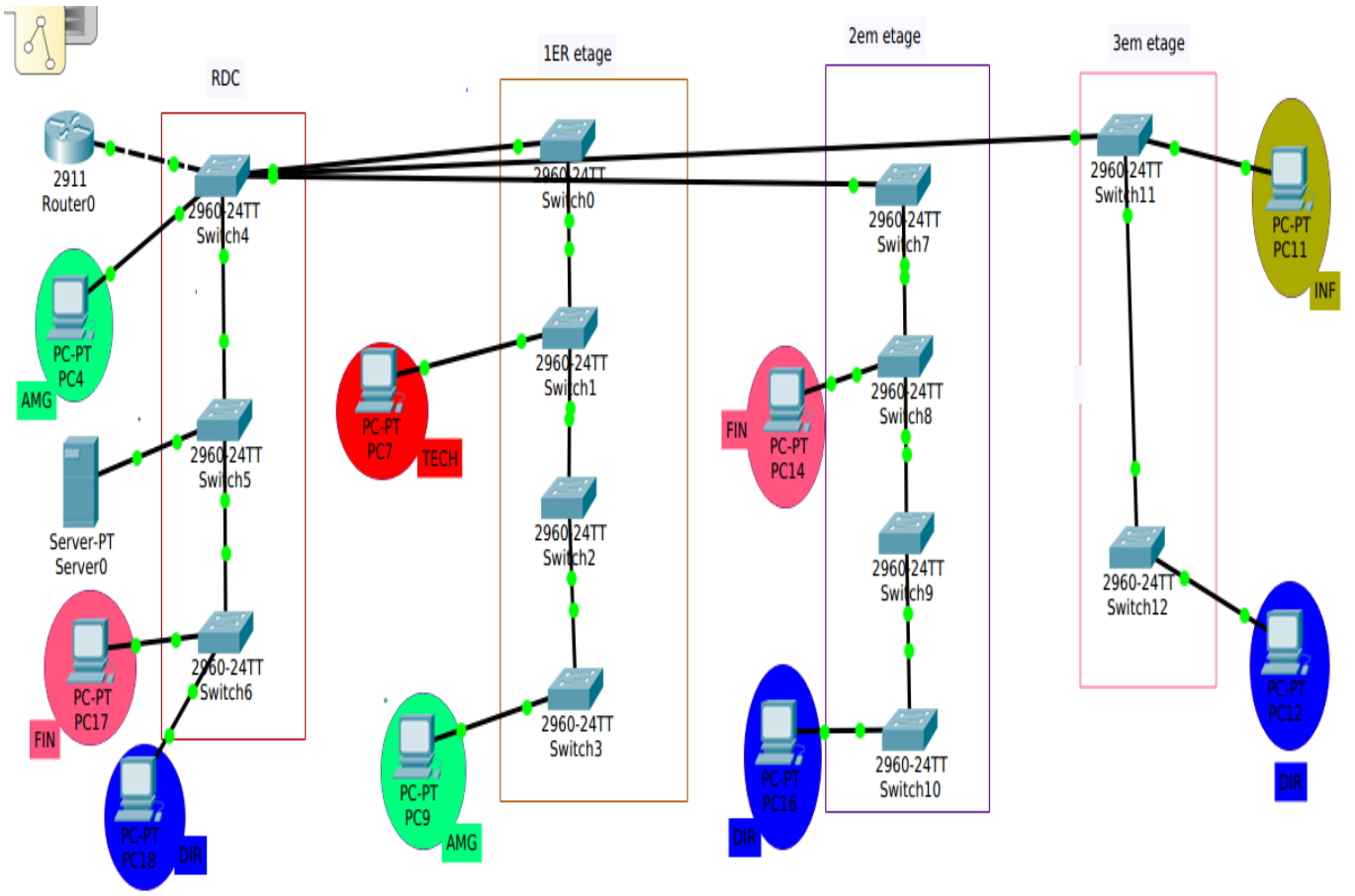

FIGURE 3.7 – Architecture du réseau avec vlans

Conclusion

A travers ce chapitre,nous avons présenté l'organisme d'acceil ainsi que le service informatique de l'entreprise dans lequel on est sensé accomplir notre stage.

On a aussi entamer l'étude de l'éxistant qui nous a permis de nous accoutumer avec le district. Le prochain chapitre ,sera consacré pour la réalisation et la mise en place de notre solution.

CHAPITRE 4
REALISATION

Chapitre 4

Réalisation

4.1 Introduction

Aprés avoir detecté la problématique du district,nous nous consacrons dans ce chapitre à l'implementation de la solution proposé précédemment avec le simulateur cisco packet tracer ainsi que les configurations necéssaires.

4.2 Présentation du simulateur « Cisco Packet Tracer »

Packet Tracer est un simulateur de réseau puissant développé par "Cisco Systems" pour faire des plans d'infrastructure de réseau en temps réel. Il offre la possibilité de créer,de visualiser et de simuler les réseaux informatiques. L'objectif principal de simulateur, est de schématiser, configurer et de voir toutes les possibilités d'une future mise en œuvre réseau. Cisco Packet Tracer est un moyen d'apprentissage, de la réalisation de divers réseaux et de découvert de fonctionnement des différents éléments constituant un réseau informatique[25].
La Figure suivant est une image montrant l'interface principale du simulateur Cisco Packet Tracer :

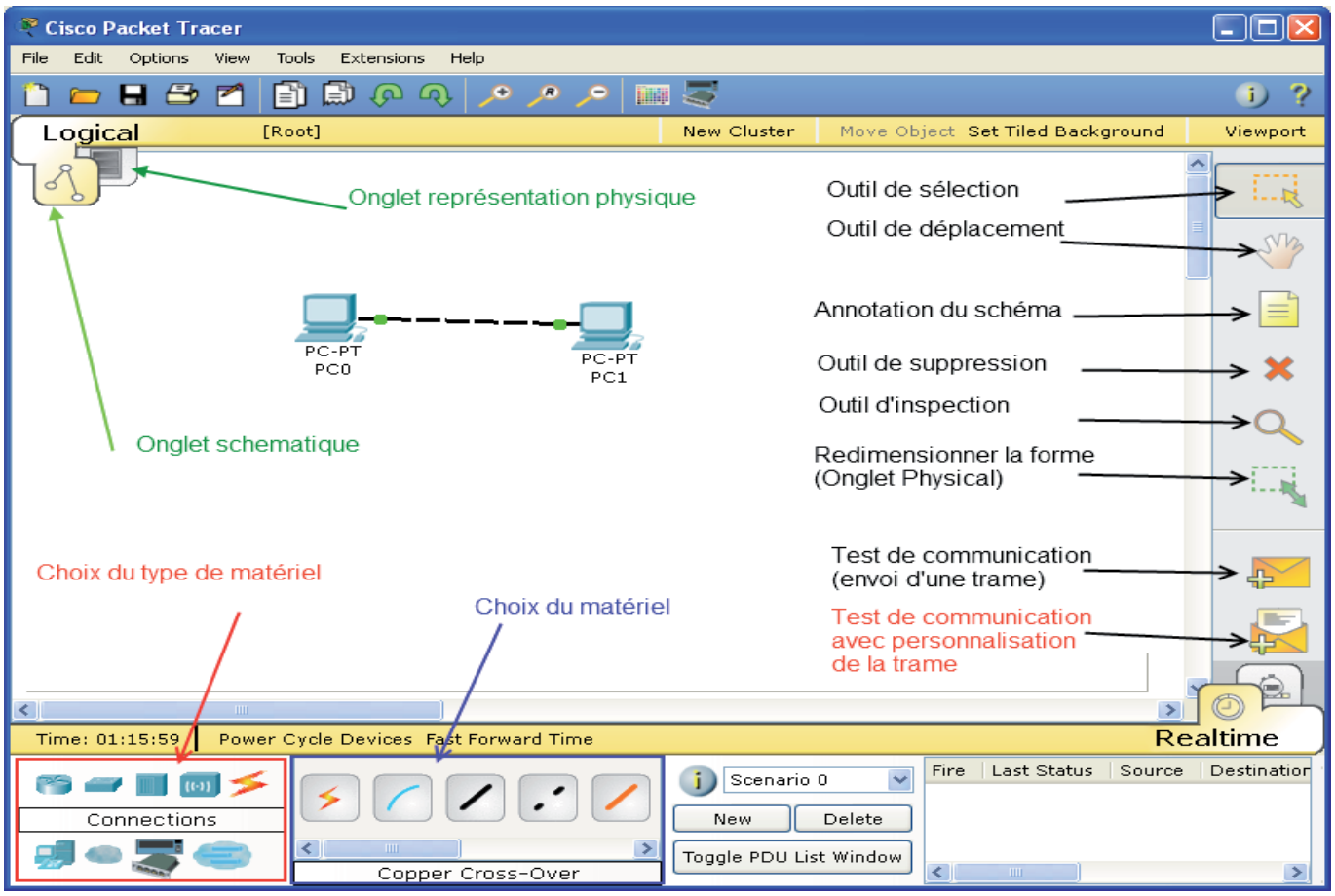

FIGURE 4.1 – L'interface du simulateur « Cisco Packet Tracer ».

4.3 Interface commande de Packet Tracer

Toutes les configurations des équipements du réseau, c'est au niveau de CLI (Command Language Interface) quelles seront réalisées. CLI est une interface de simulateur Packet Tracer qui permet la configuration des équipements du réseau à l'aide d'un language de commandes, c'est-à-dire qu'à partir des commandes introduites par l'utilisateur du logiciel, que la configuration est faite[25]

La Figure suivante est l'interface CLI du Packet Tracer :

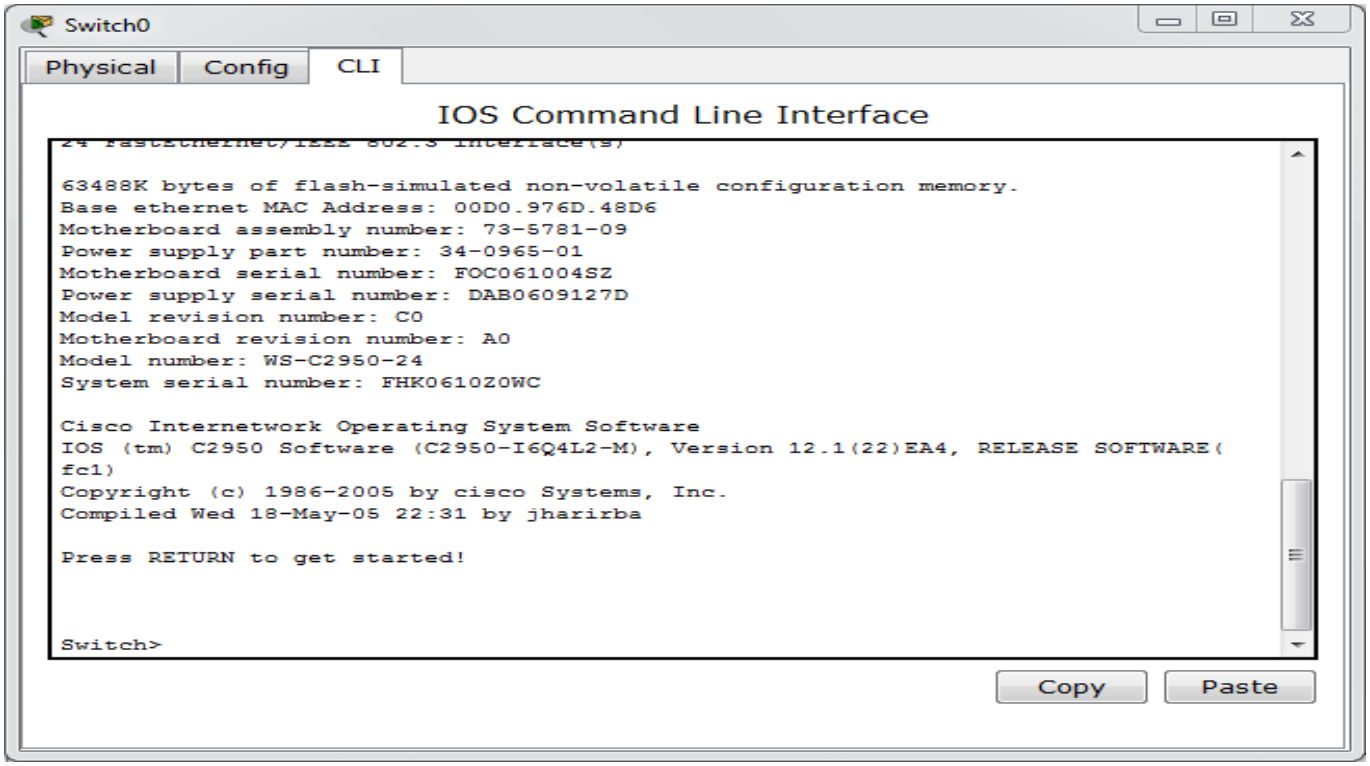

FIGURE 4.2 – Interface CLI

4.4 Configurations des équipements

Dans cette rubrique, on va configurer les equipements constituant le réseau local de l'etreprise ; chaque configuration est suivi par un exemple et pour cela nous allons suivre les étapes de configuration suivantes

- Configuration des commutateurs
- Configuration du routeur
- Test de validation des configurations

4.4.1 Configuration des commutateurs

Cette configuration contiendra un ensemble de point a configurer tel que les noms des commutateurs ,les VLANs,les interfaces. Ainsi les protocole comme le vtp et le stp .

1. **Affectation des adresses aux vlans**

   Le tableau suivant représente l'affectation des adresse ip pour chaque vlan

NOM	Id Vlan	Address du réseau	Masque de réseau.
Informatique	VLAN 100	10.64.50.0	255.255.255.0
Fin	VLAN 200	10.64.100.0	255.255.255.0
AMG	VLAN 300	10.64.200.0	255.255.255.0
TECH	VLAN 400	10.64.150.0	255.255.255.0
Direction	VLAN 500	10.64.250.0	255.255.255.0

TABLE 4.1 – «Affectation des adresse aux vlan».

2. **Création des VLANS**

   Nous allons commencer par la création des VLANs,sachant qu'on a 5 (100,200,. . . ,500),comme le montre la figure suivante :

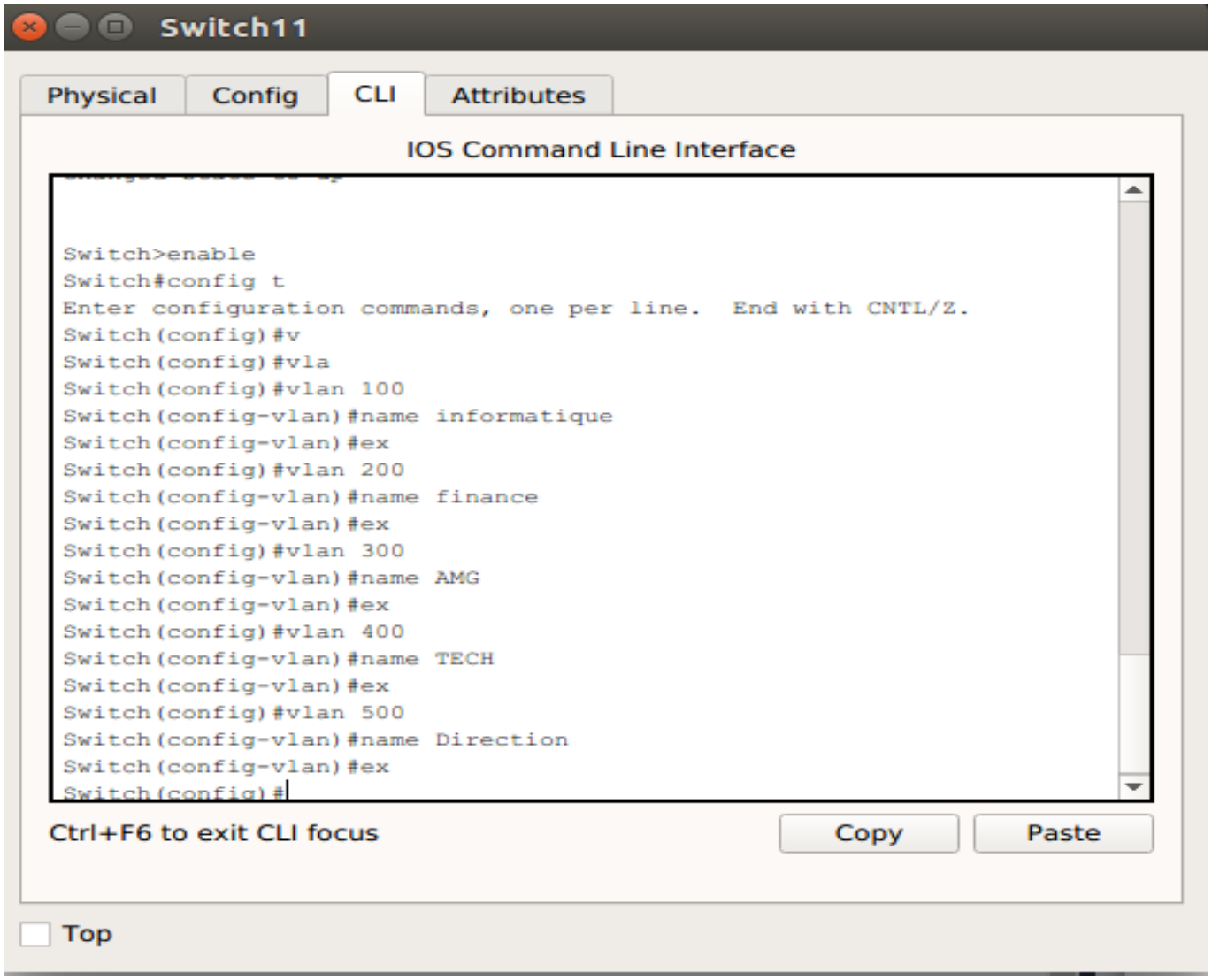

FIGURE 4.3 – Création des VLANs.

3. **Hostname**

   Cette configuration est faite pour donner des noms significatifs pour les commutateurs, en effet on a choisi un exemple(swich11) :

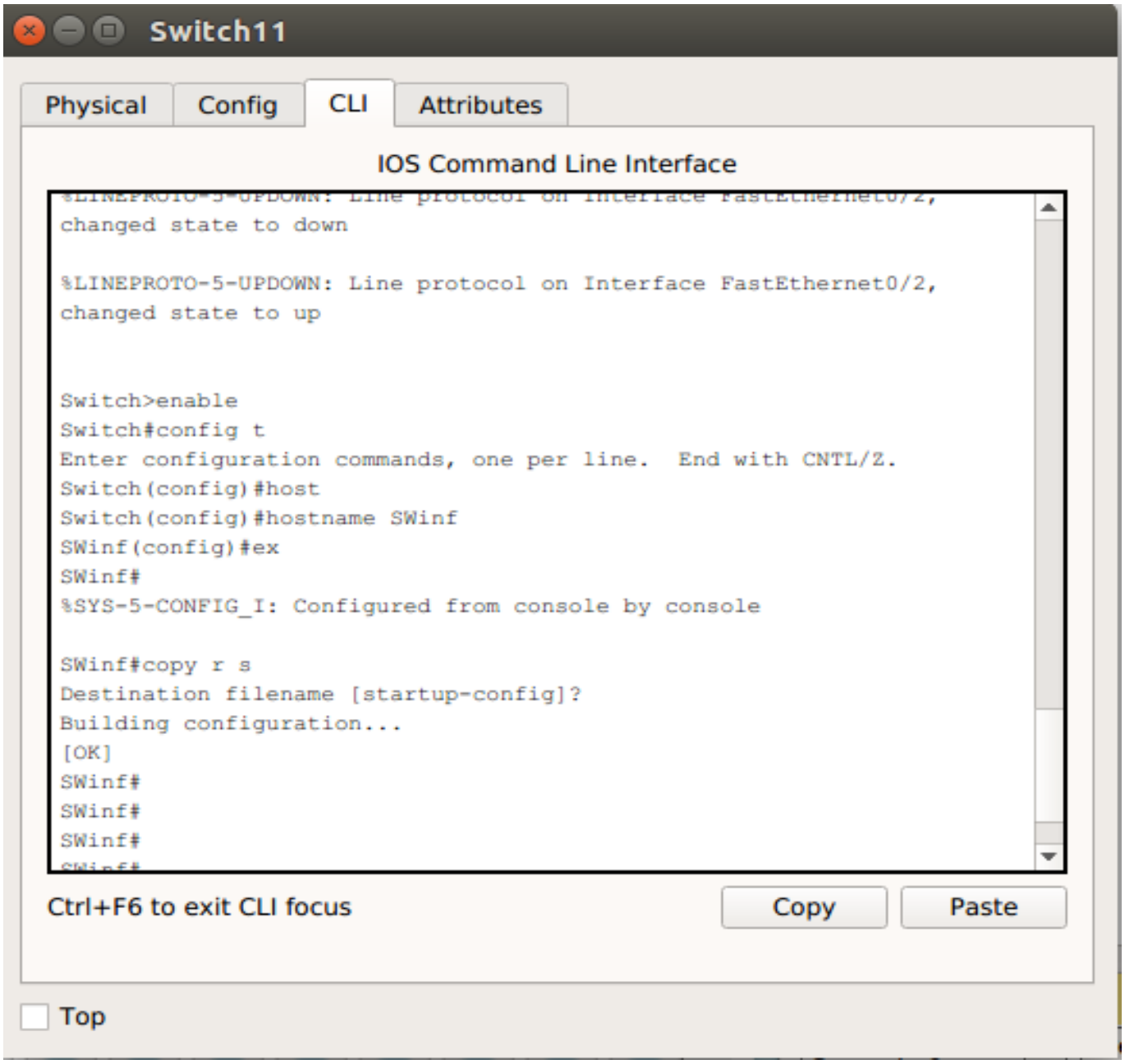

FIGURE 4.4 – Hostname.

4. **Configuration des mots de passe :**

maintenant on passera à la configuration des mots de passe

(a) **Sécuriser l'accès à la ligne de console :**

On a choisi le mot de passe ''naftalcbr". On a pris un exemple du commutateur ''S-Winf'' ;comme le montre la figure ci-dessous.

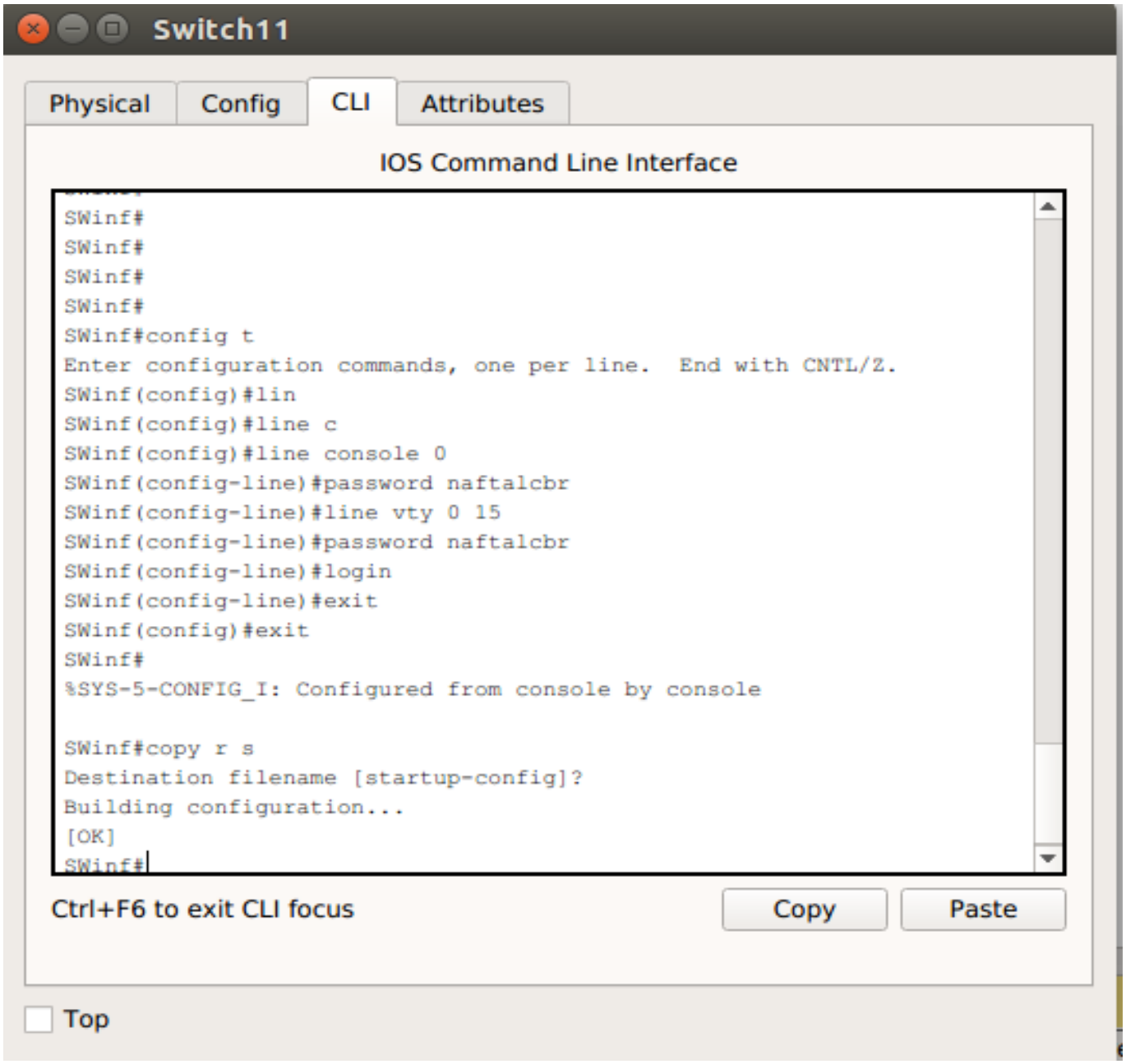

FIGURE 4.5 – Mot de passe console au SWinf.

(b) **Sécuriser l'accès en mode privilégie :**

Nous avons choisi pour le mode previligie le mot de passe :"naftal" (voir la figure 4.6) :

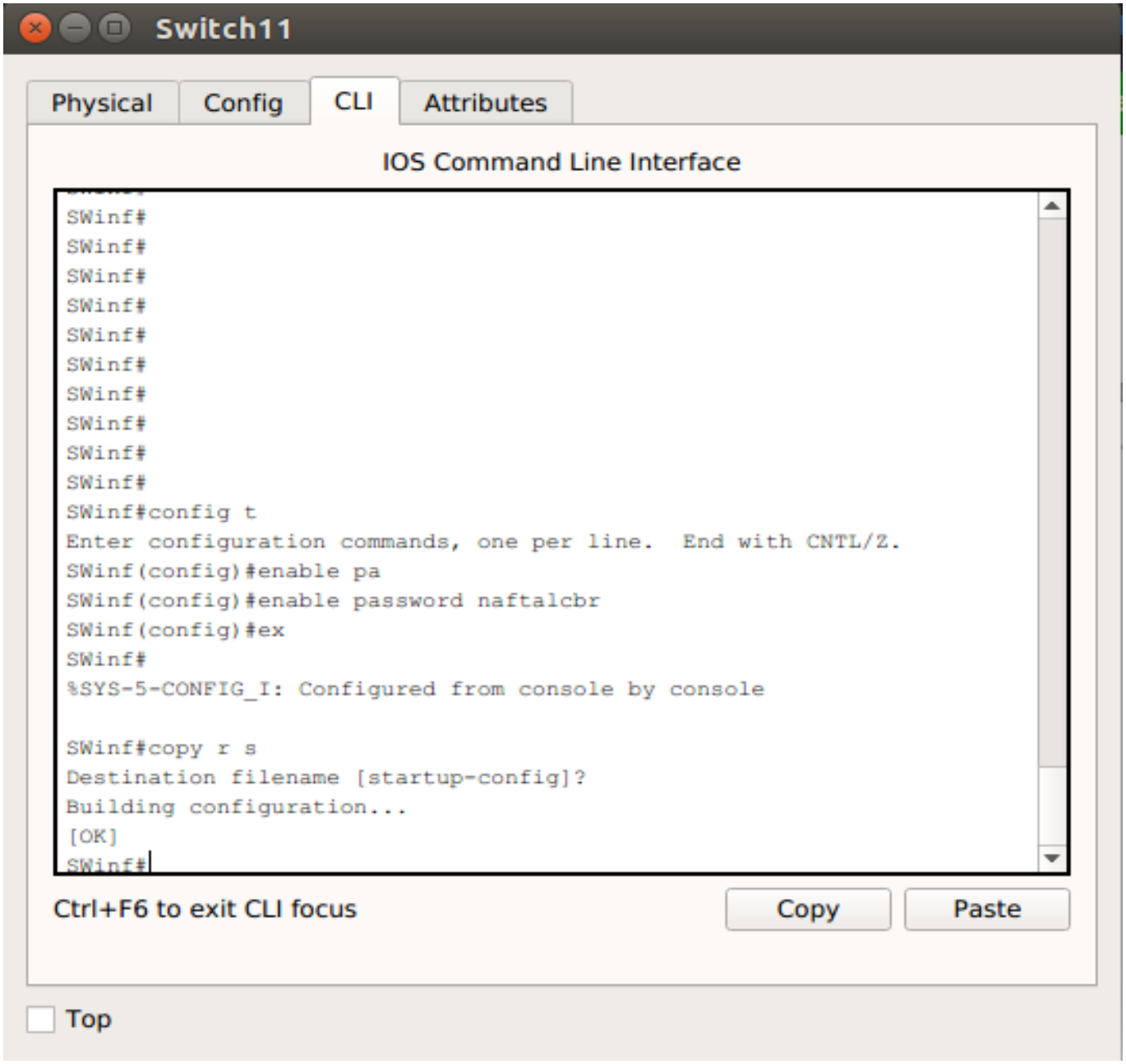

FIGURE 4.6 – Mot de passe pour le mode privilégié.

(c) **Configurer un mot de passe chiffré pour sécuriser l'accés au mode privilégié :**

Le mot de passe d'activation (enable) doit être remplacé par le mot de passe secret chiffré à l'aide de la commande enable secret (voir la figure 4.7).

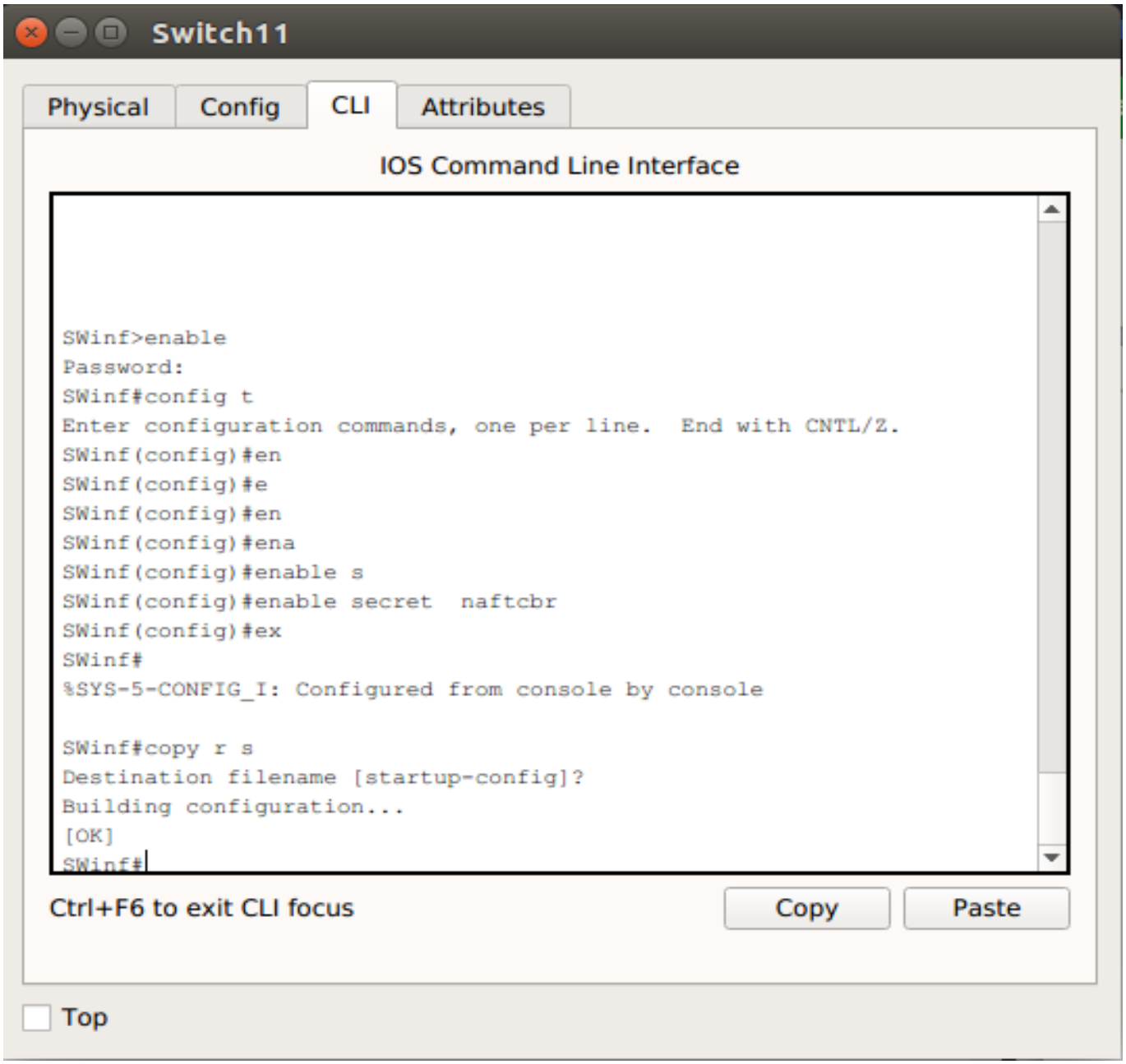

FIGURE 4.7 – Mot de passe secret.

(d) **Sécuriser l'accès à distance :**

On préfère utiliser l'accès à distance avec SSH par rapport à sa fiabilité en terme de sécurité (voir la figure ci-dessous) :

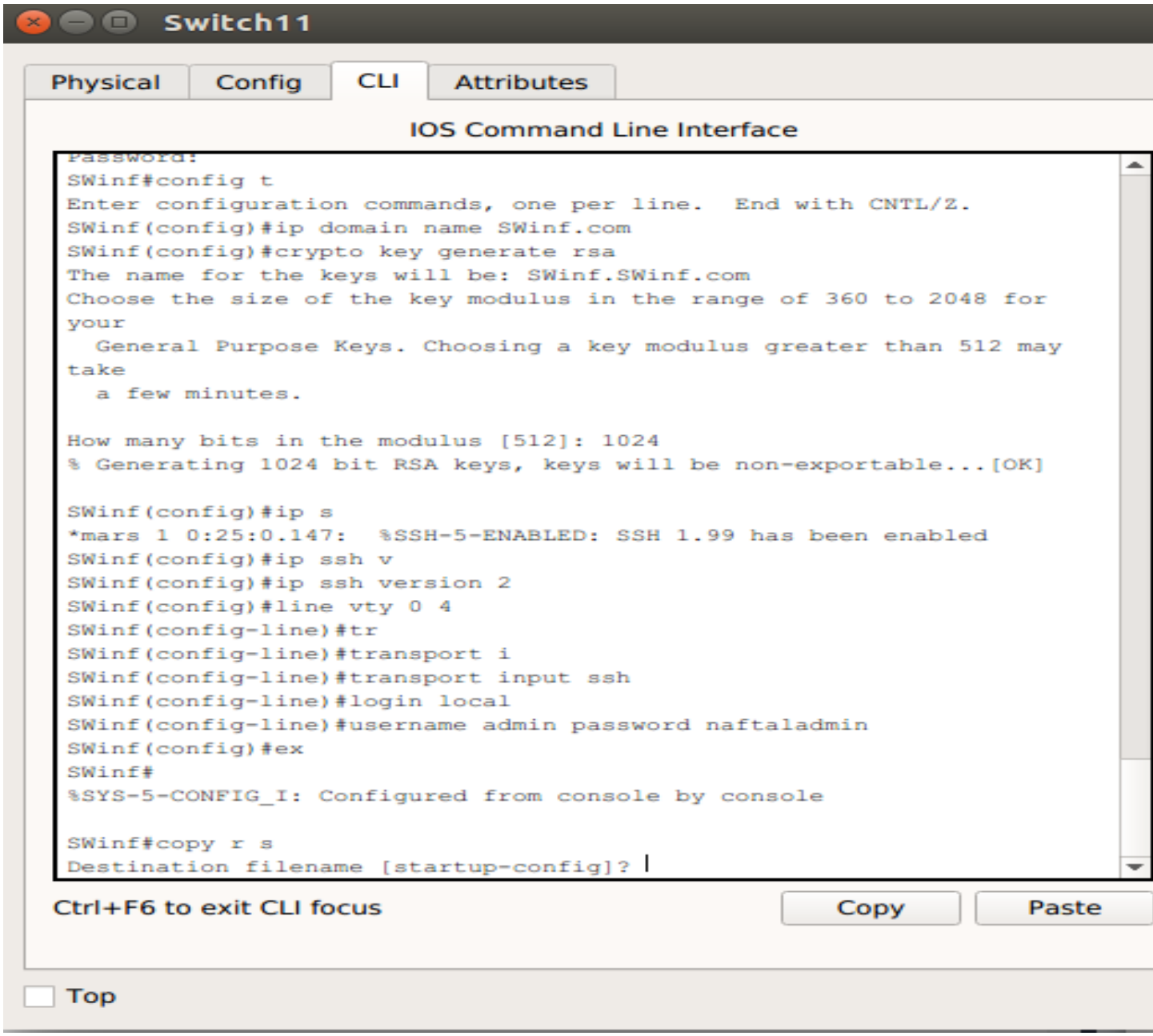

FIGURE 4.8 – Configuration de SSH.

5. **Configuration des Vlans :**

On attribue les adresses IP de passerelle pour chaque commutateur.

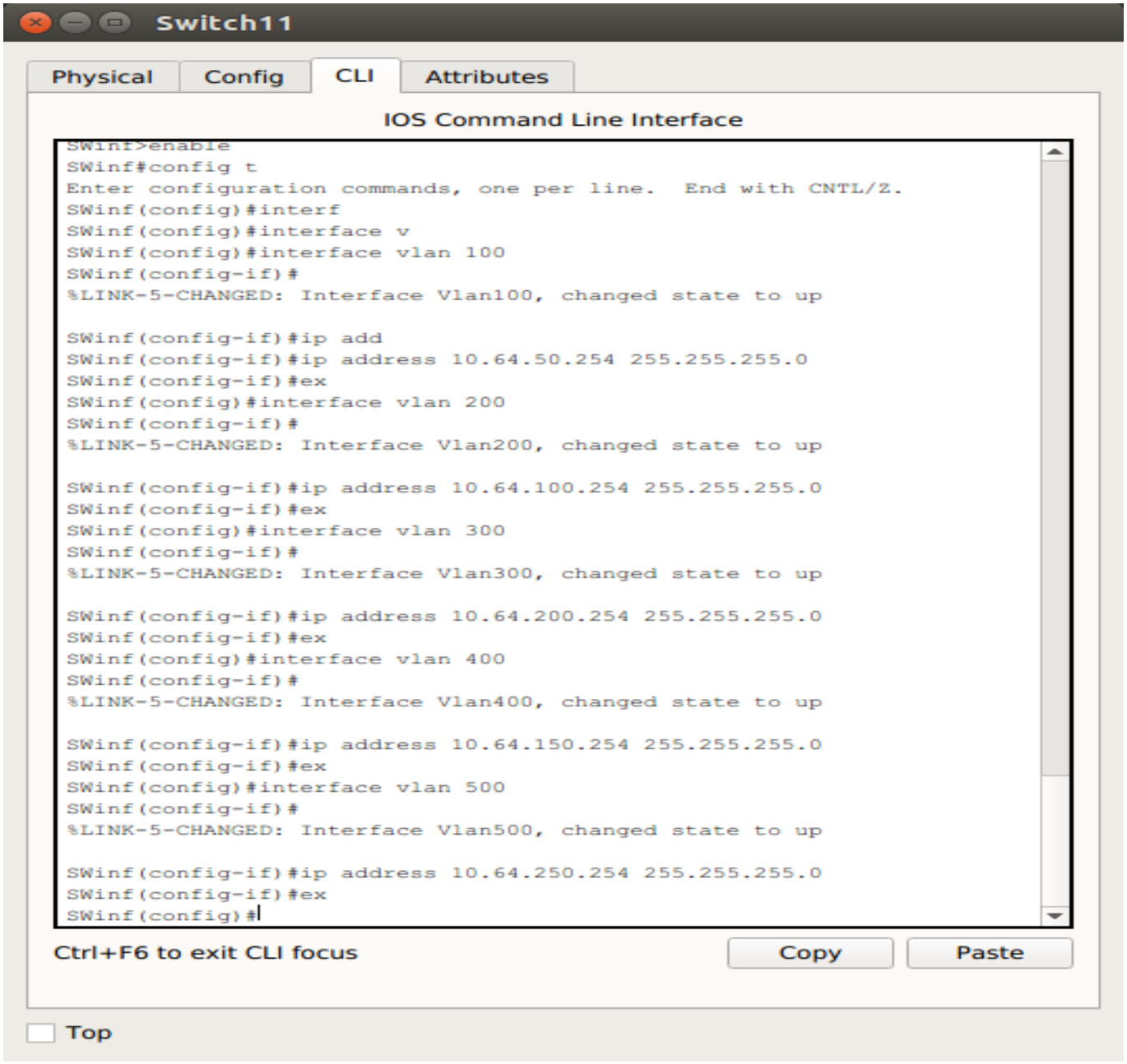

FIGURE 4.9 – Configuration des VLANS.

6. **Configuration des interfaces :**

On passera à la configuration des interfaces avec ces deux mode(trunk et access).

(a) **mode trunk**

Les interfaces d'équipements à configurer en mode trunk sont tous des commutateurs reliés entre eux et aussi entre le commutateur principale et le routeur (voir la figure ci-dessous).

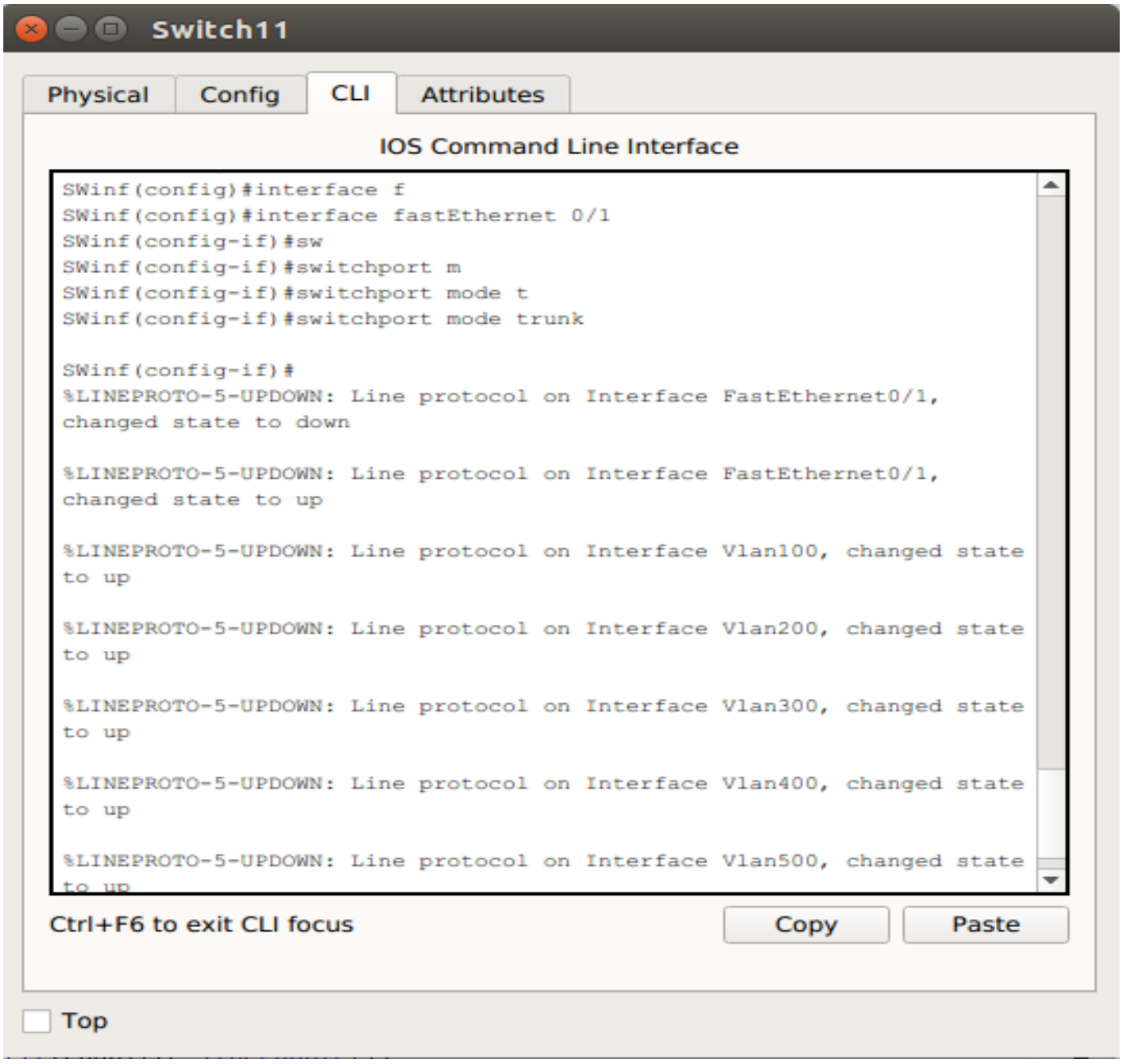

FIGURE 4.10 – Configuration des liens Trunk.

(b) **mode access**

Par contre ici on va configurer en mode access tous les commutateurs reliés au PCs,chaque port d'un commutateur appartiendra à un VLAN donné (voir la figure 4.11).

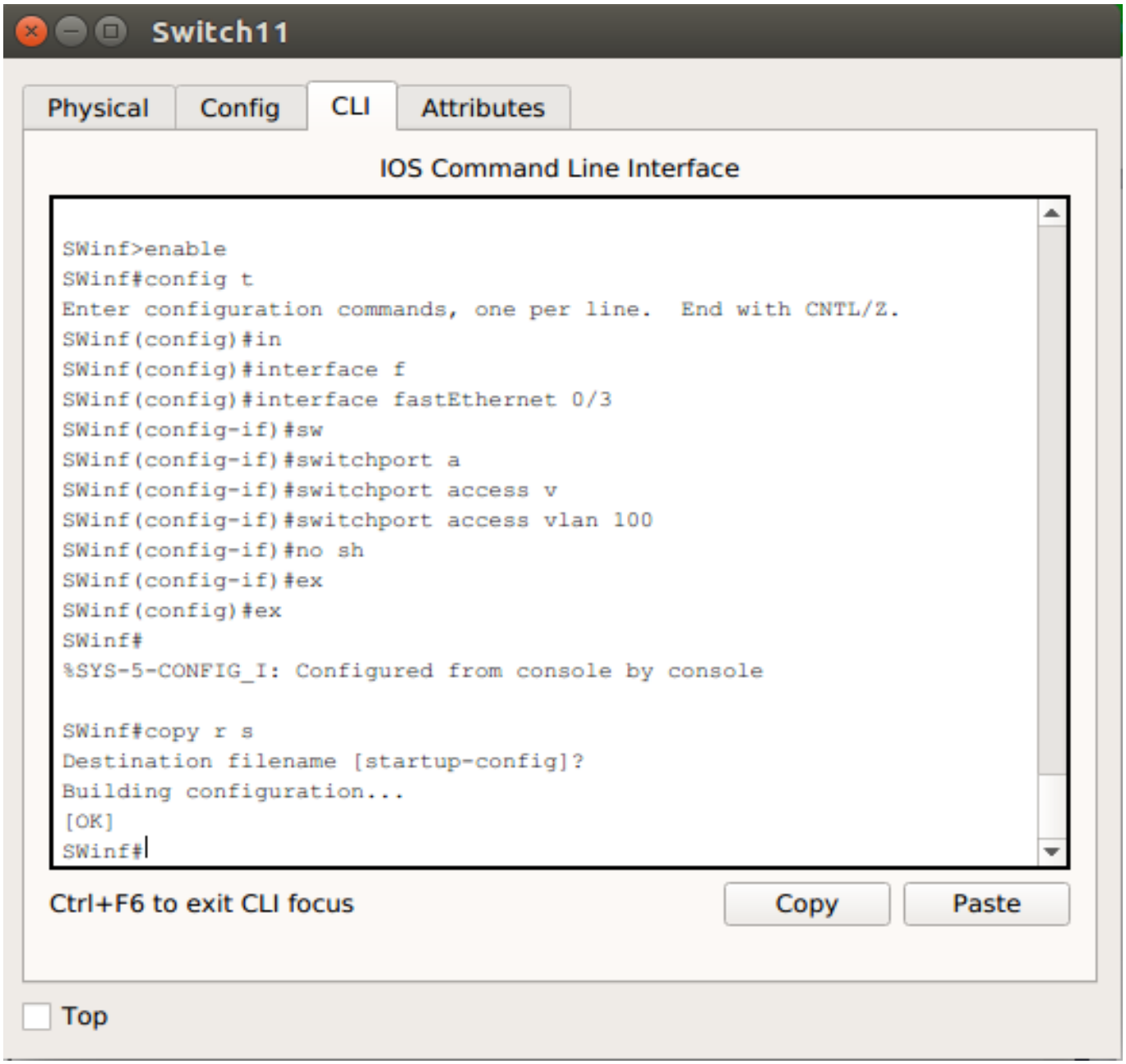

FIGURE 4.11 – attribution des ports au vlans.

7. **Configuration du VTP :**

Nous avons configuré le SWinf en "mode serveur " qui permet de gérer l'administration de l'ensemble des vlan ,on lui a attribué un nom de domain qui est "naftcbr" et un mot de passe "1901".(voir la figure ci-dessous).

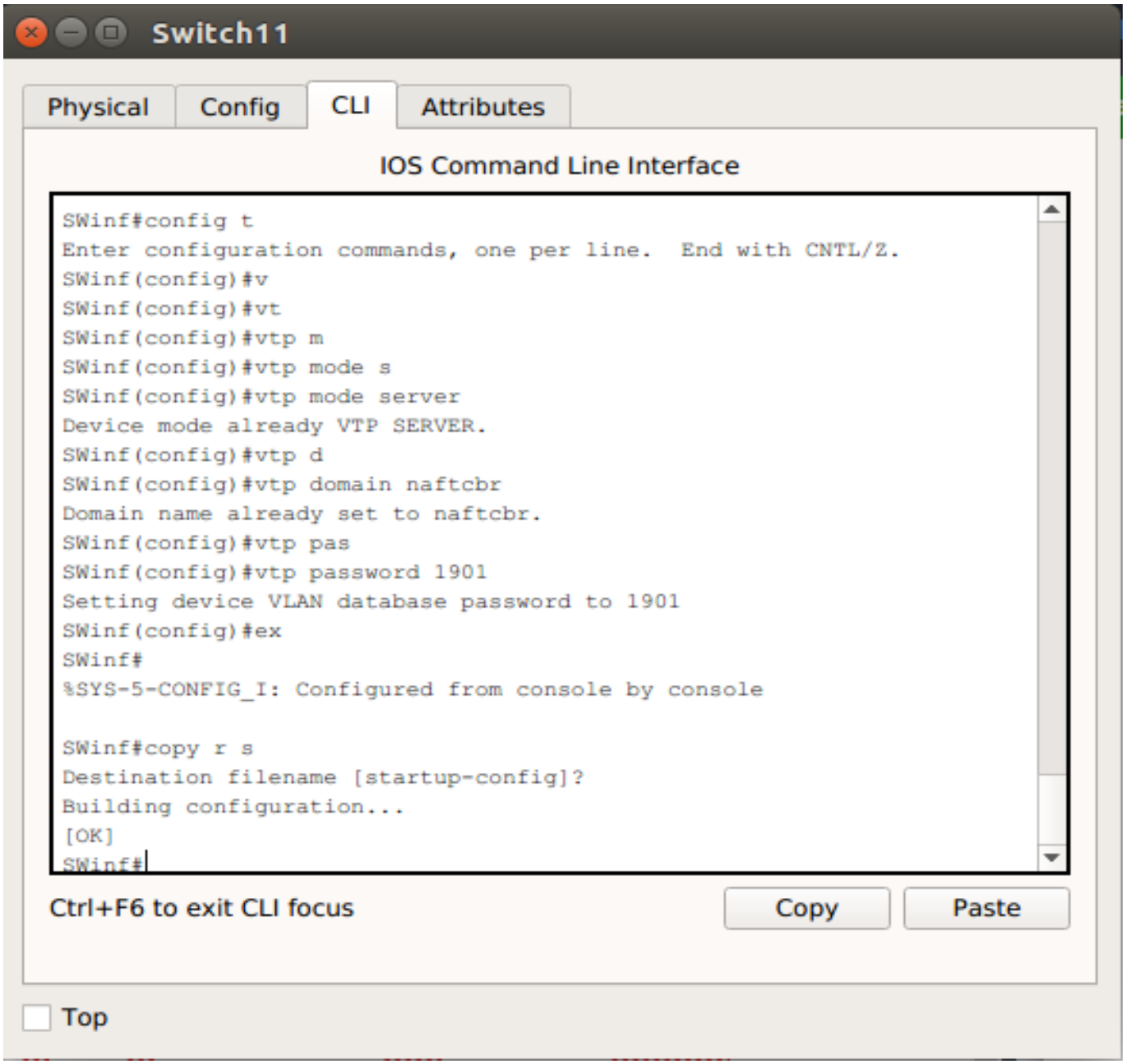

FIGURE 4.12 – Configuration du VTP-Server..

et pour les autres commutateurs nous allons les configurer en mode client.

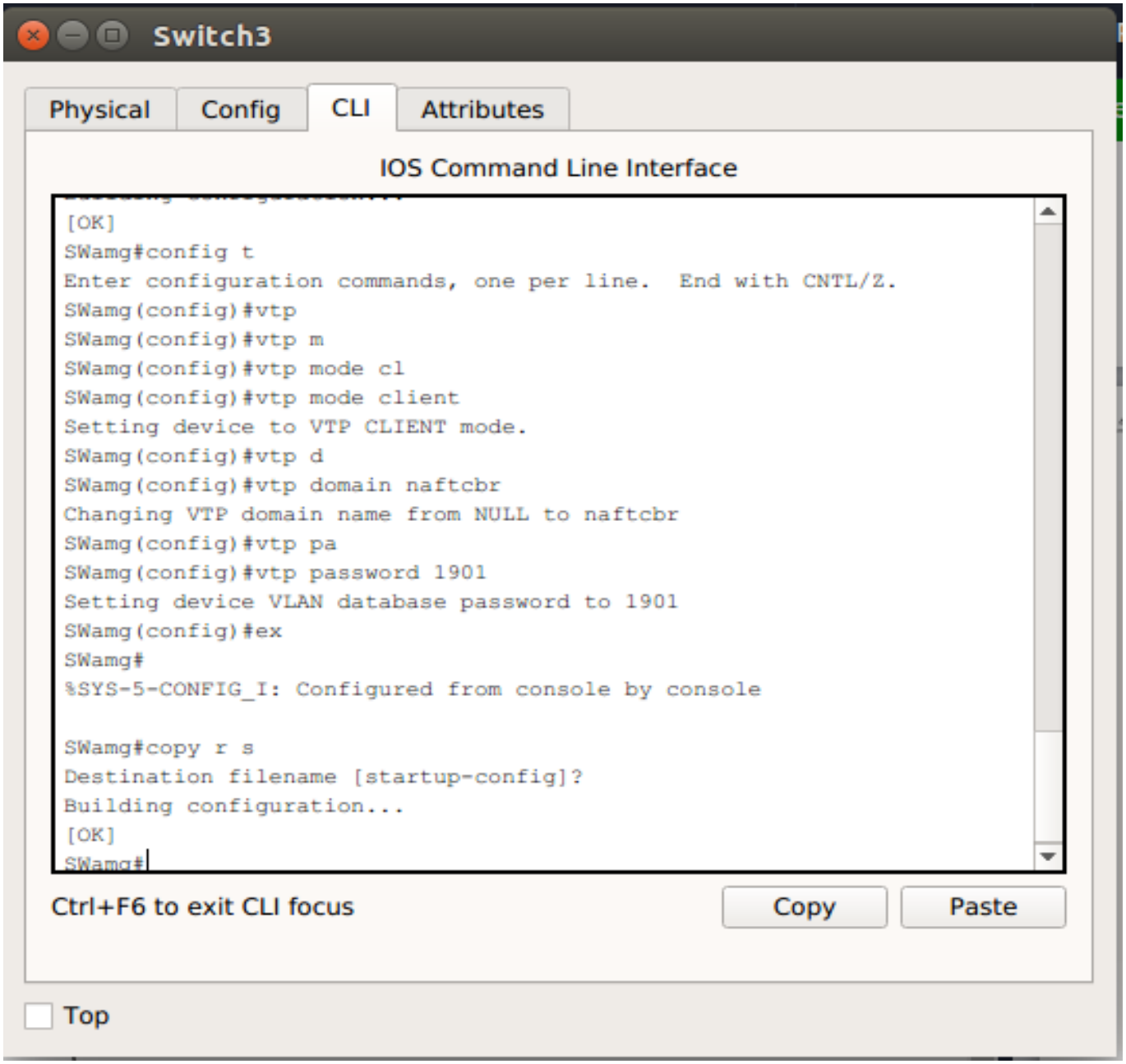

FIGURE 4.13 – Configuration du VTP-Client.

aprés avoir configuré tous les commutateurs en mode client ,toute la configuration qui est faite au niveau du commutateur "SWinf" sera propagée vers tous les autres commutateurs en mode client (voir la figure 4.14).

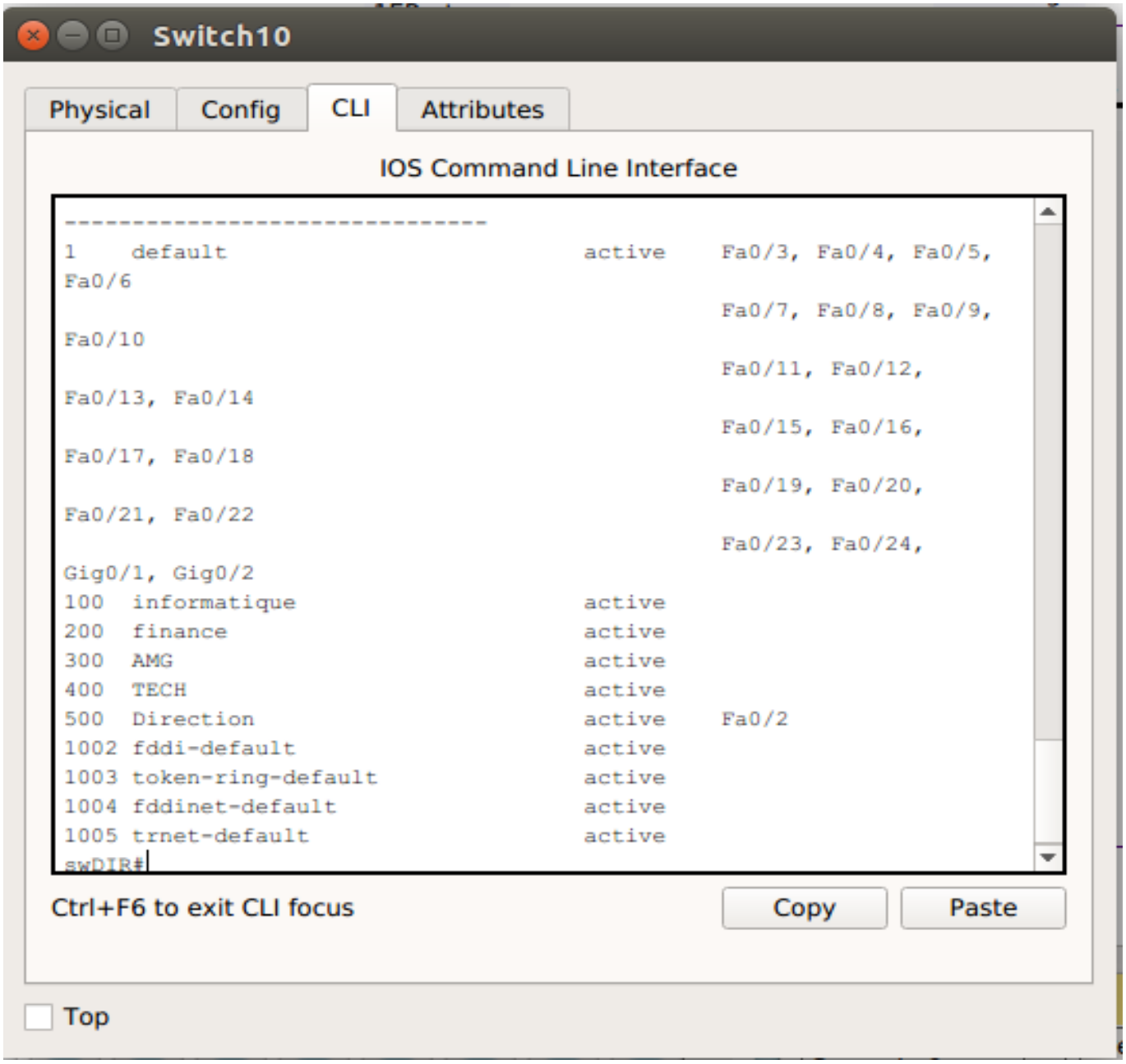

FIGURE 4.14 – Les VLANs crées après la configuration du VTP-Client.

8. **Configuration du STP :**

   Nous allons configurer le protocole Spanning-Tree pour définir un Switch racine. (Voir la figure 4.15) :

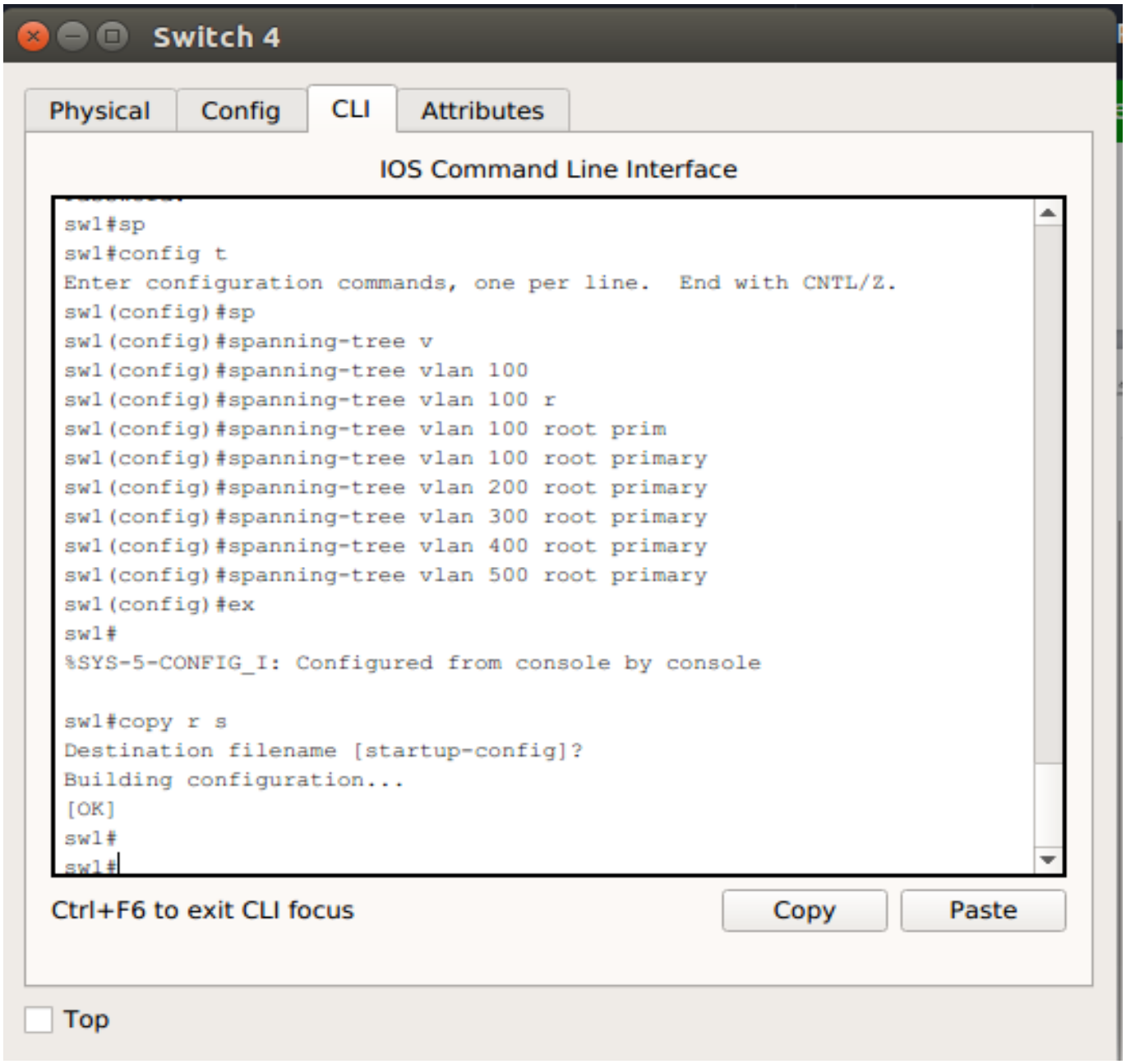

FIGURE 4.15 – Configuration de Spanning-Tree..

9. **Affectation d'addresses fixes pour les switchs**

   Affectation des adresses fixe pour les commutateurs.

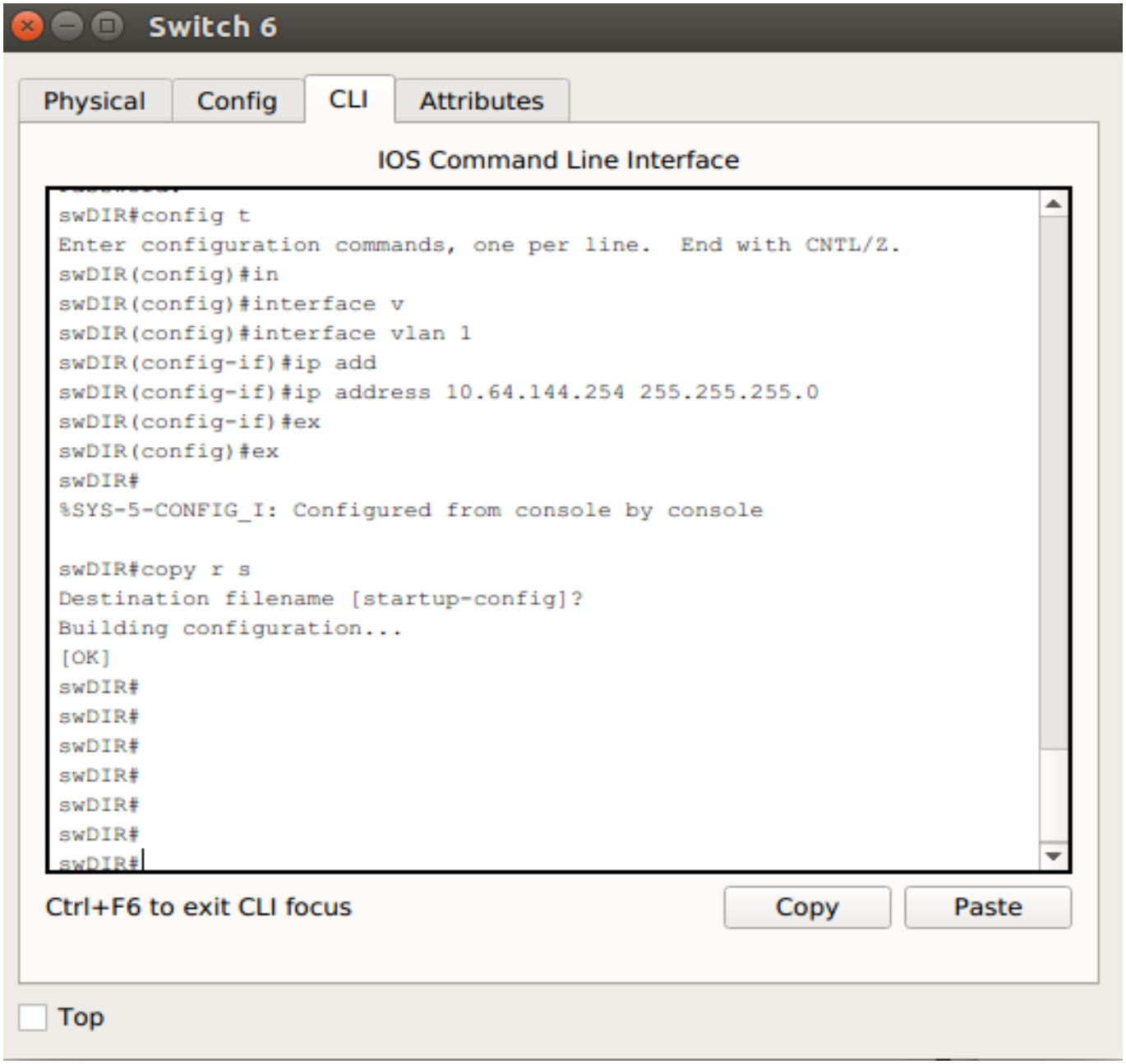

FIGURE 4.16 – Affectation d'adresses fixe au switch .

4.4.2 Configuration du routeur

dans cette partie en va configurer le protocole dhcp,les listes de controle d'accées et le routage inter-vlan.

1. **Configuration du dhcp**

   Pour cette topologie on va créer 5 pool c'est a dire, pour chaque vlan on lui crée son propre pool.

   La figure suivante présente la configuration correspondante.

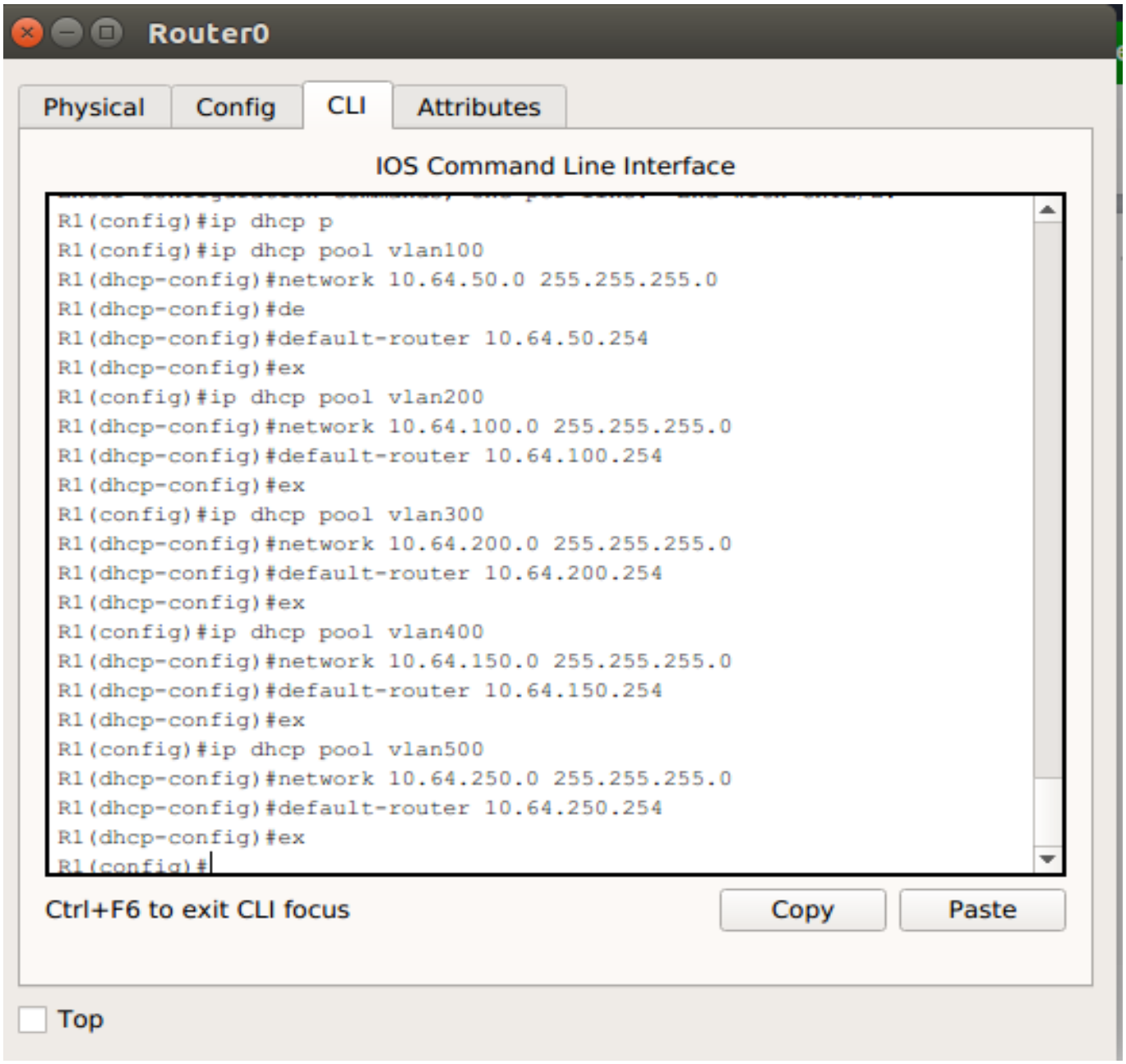

FIGURE 4.17 – Configuration du protocole dhcp.

voici l'affèctation des adresses aux PCs à l'aide de protocole dhcp

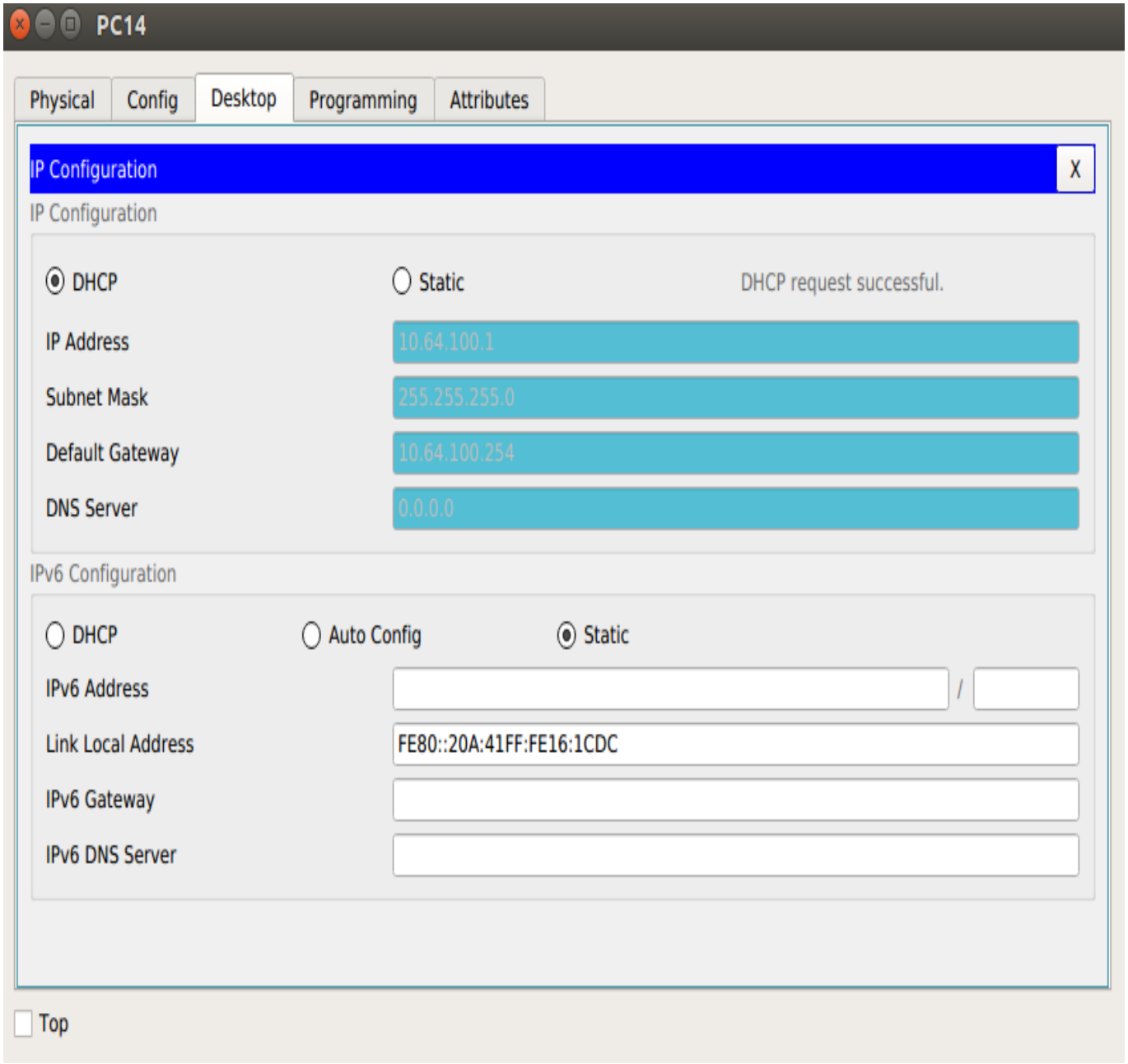

FIGURE 4.18 – l'affèctation d'adresse aux PCs.

2. **Configuration inter-vlan :**

Nous allons faire un routage inter-vlans pour conquérir des communications entre les différents Vlans qui existe. A voir les commandes a suivre dans la figure ci-dessous :

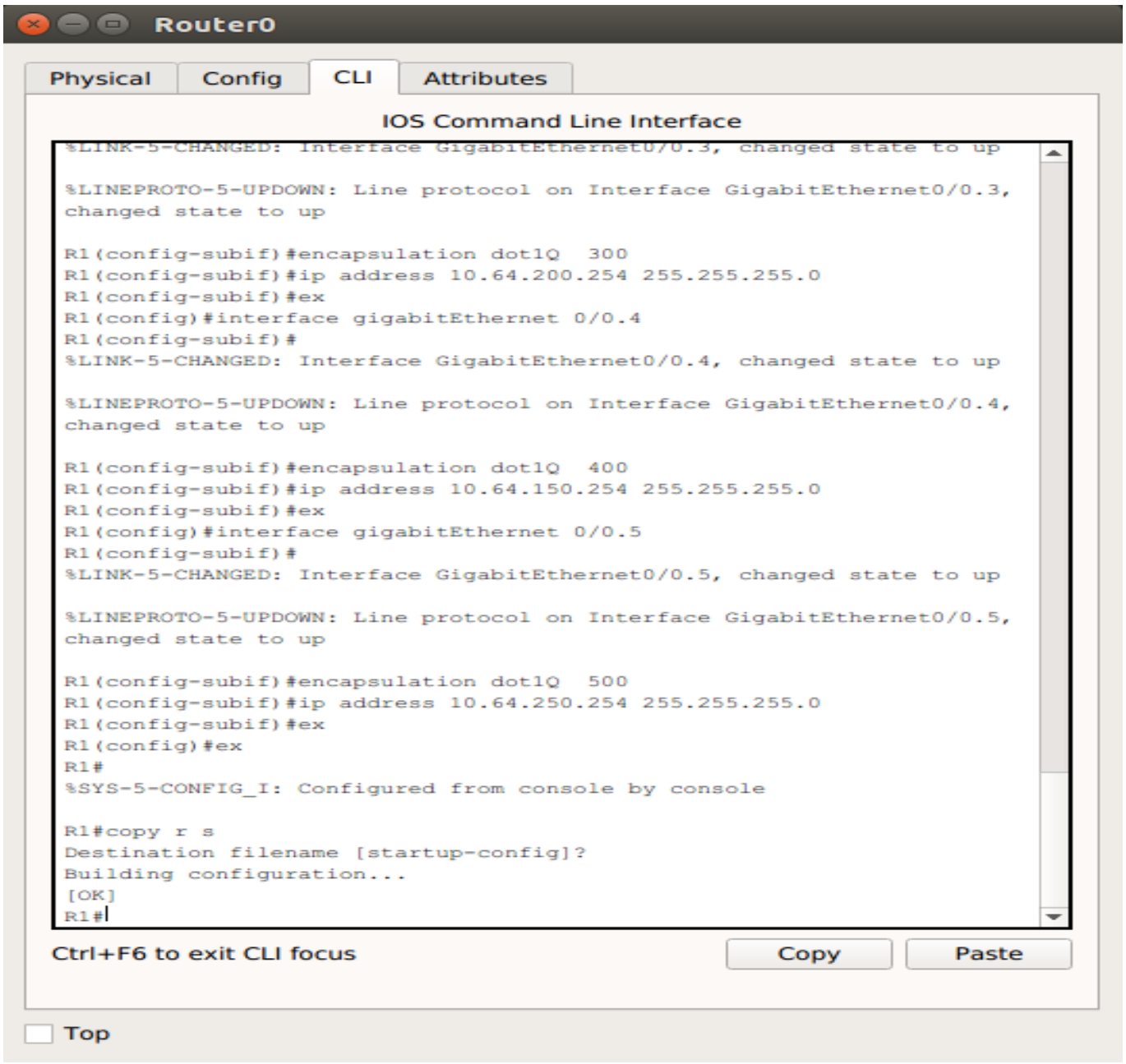

FIGURE 4.19 – Configuration de routage inter-vlan.

3. **Configuration des ACLs :**

Nous allons maintenant utiliser les listes des contrôles d'accèes afin de limiter la communication entre certains VLANs. comme le montre la figure 4.19,nous avons pris comme exemple ,le vlan 100 qui peut accéder à tous les autres vlans mais le contraire est bloqué.

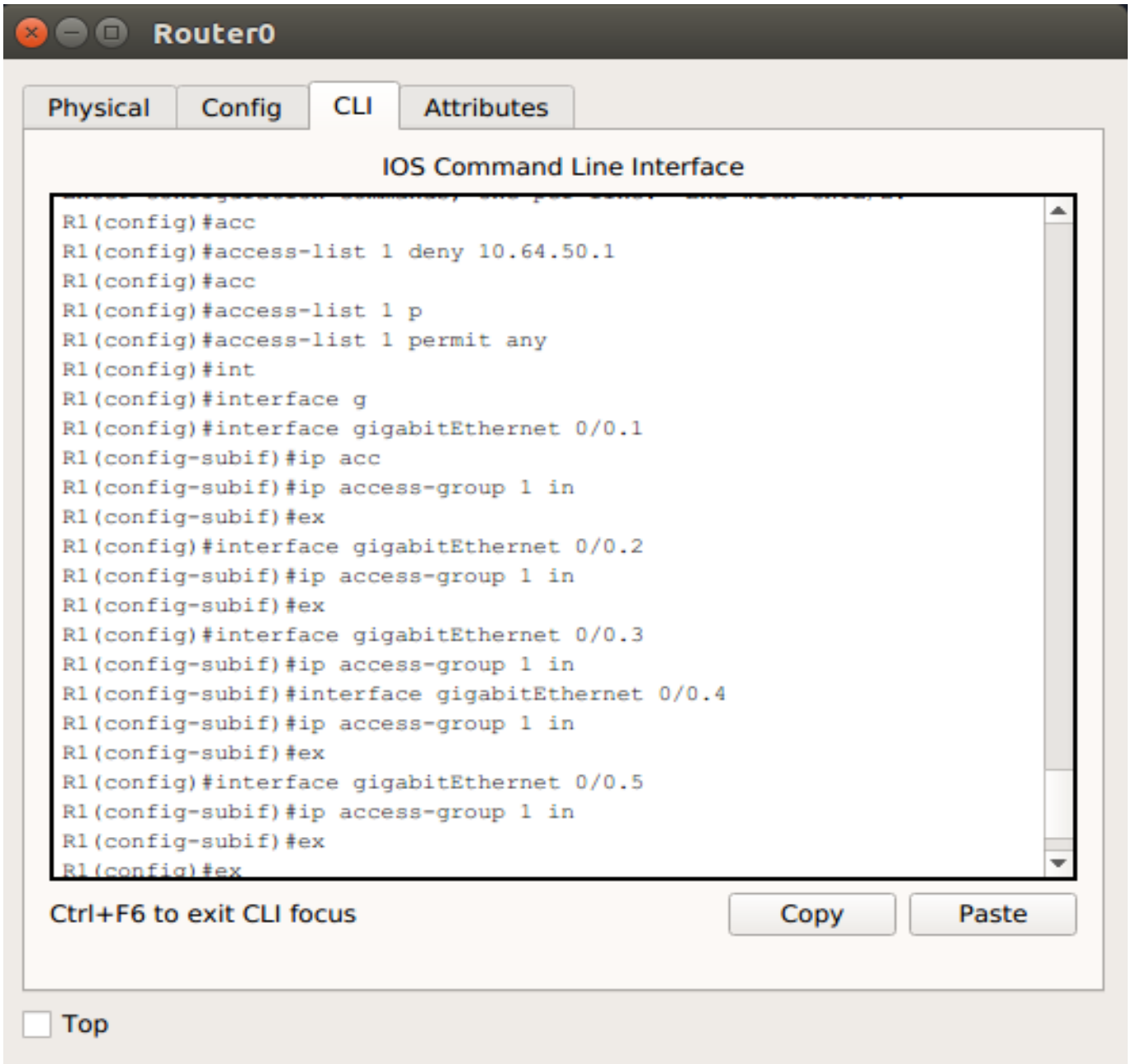

FIGURE 4.20 – Configuration d'une liste de controle d'accée.

4.4.3 Test de validation de configuration

- **Test intra-vlan**

  On verifie la communication entre deux PCs situés dans le meme VLANs nous avons choisi le

  VLAN200 qui est assigné au departement finance le pc17(10.64.100.2) et le pc14(10.64.100.1).

  Dans la figure ci-dessous,on va faire ce test avec la commande ping

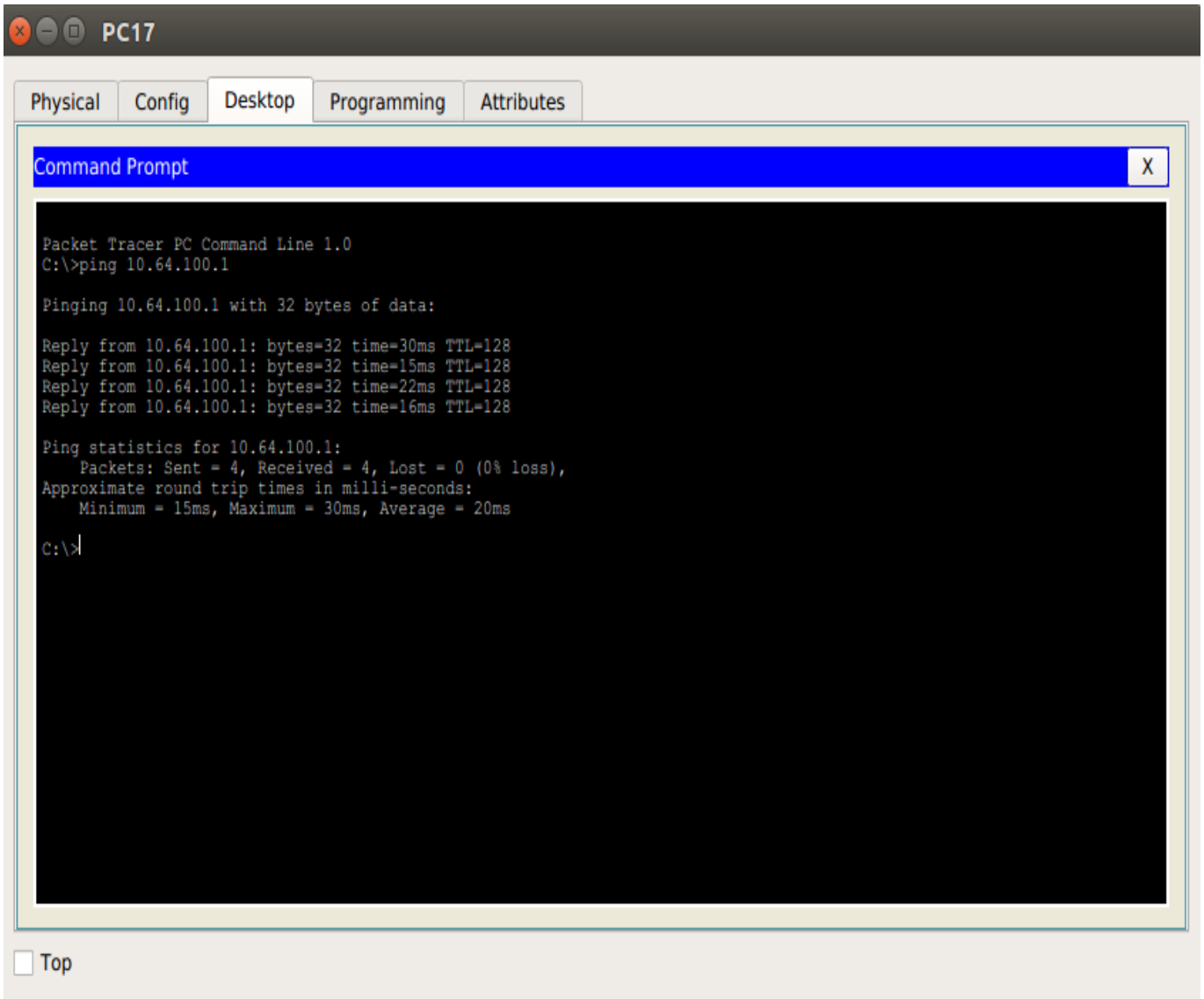

FIGURE 4.21 – Ping réussi entre le pc17 et le pc14

- **Test inter-vlan**

  On verifie la communication entre deux PCs situés dans deux VLANs différent.

  Ping reussi entre le pc16(10.64.250.1) qui appartient aux vlan direction et le pc14(10.64.100.2) du vlan finance (comme le montre la figure suivante).

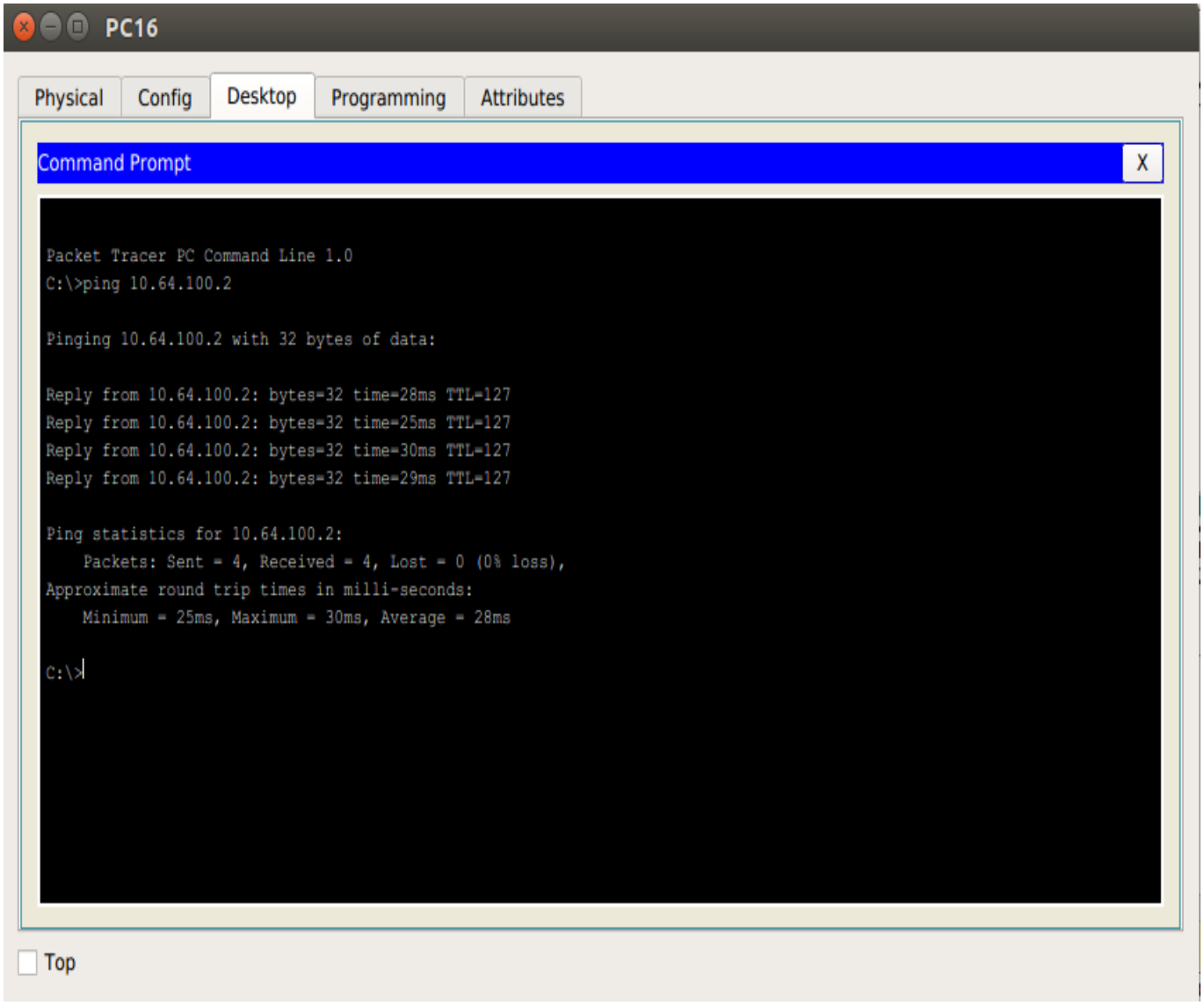

FIGURE 4.22 – Ping réussi entre le pc16 et le pc14

- **Test des ACL**

  Le but de la configuration des ACLs est d'autoriser ou d'interdire l'accés d'un VLAN à un autre .Nous avons pris comme exemple le VLAN 100 qui est le département informatique

  Notre exemple indique que :

— le département informatique (VLAN 100) à accés pour tous les autres departements.

ping réussi entre le PC11 (10.64.50.1) et le pc14 (10.64.100.1).

(voir la figure 4.23).

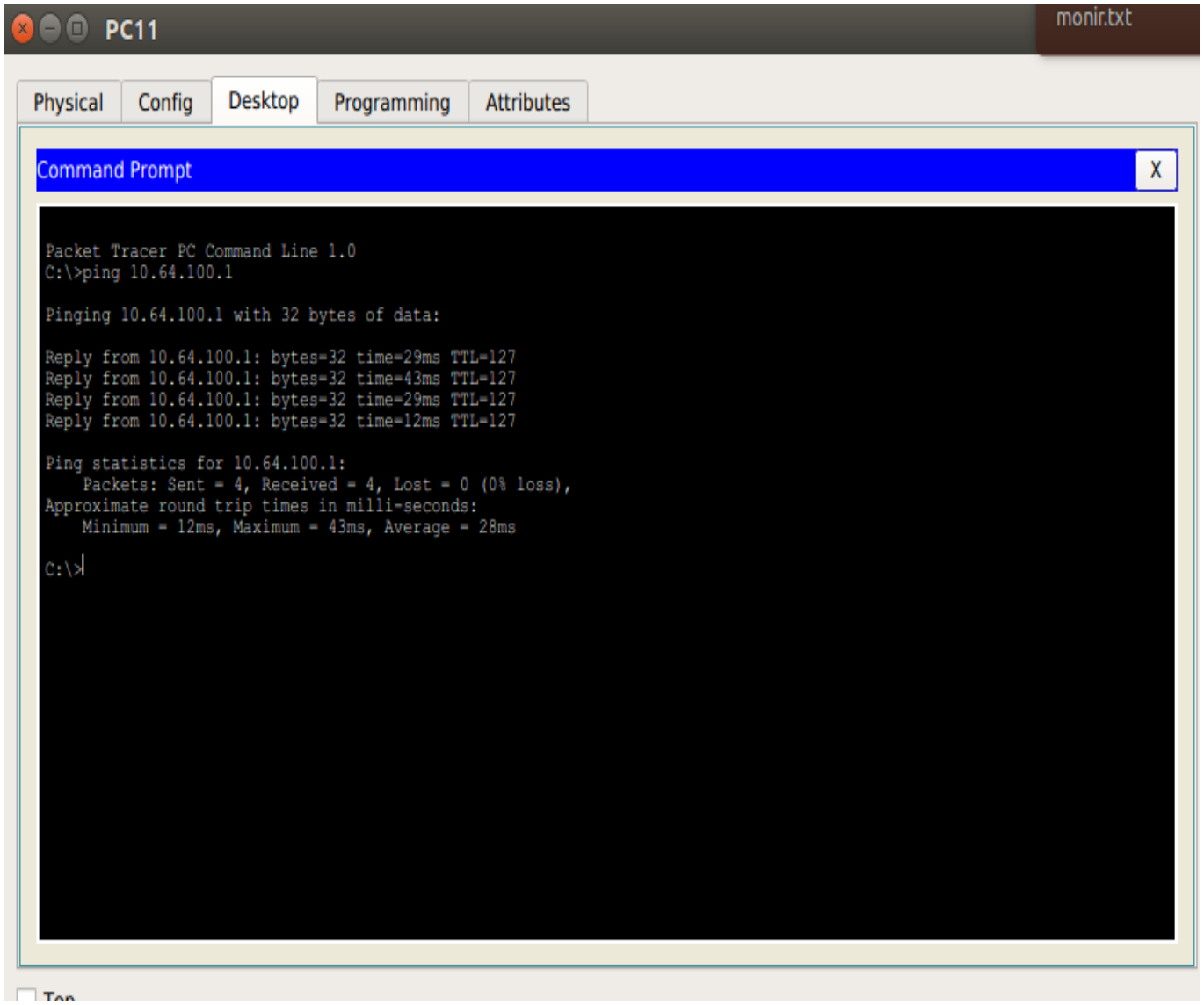

FIGURE 4.23 – Accés autorisé entre le pc14 et PC11

— mais vice-versa est interdit,commme le montre la figure ci-dessous.

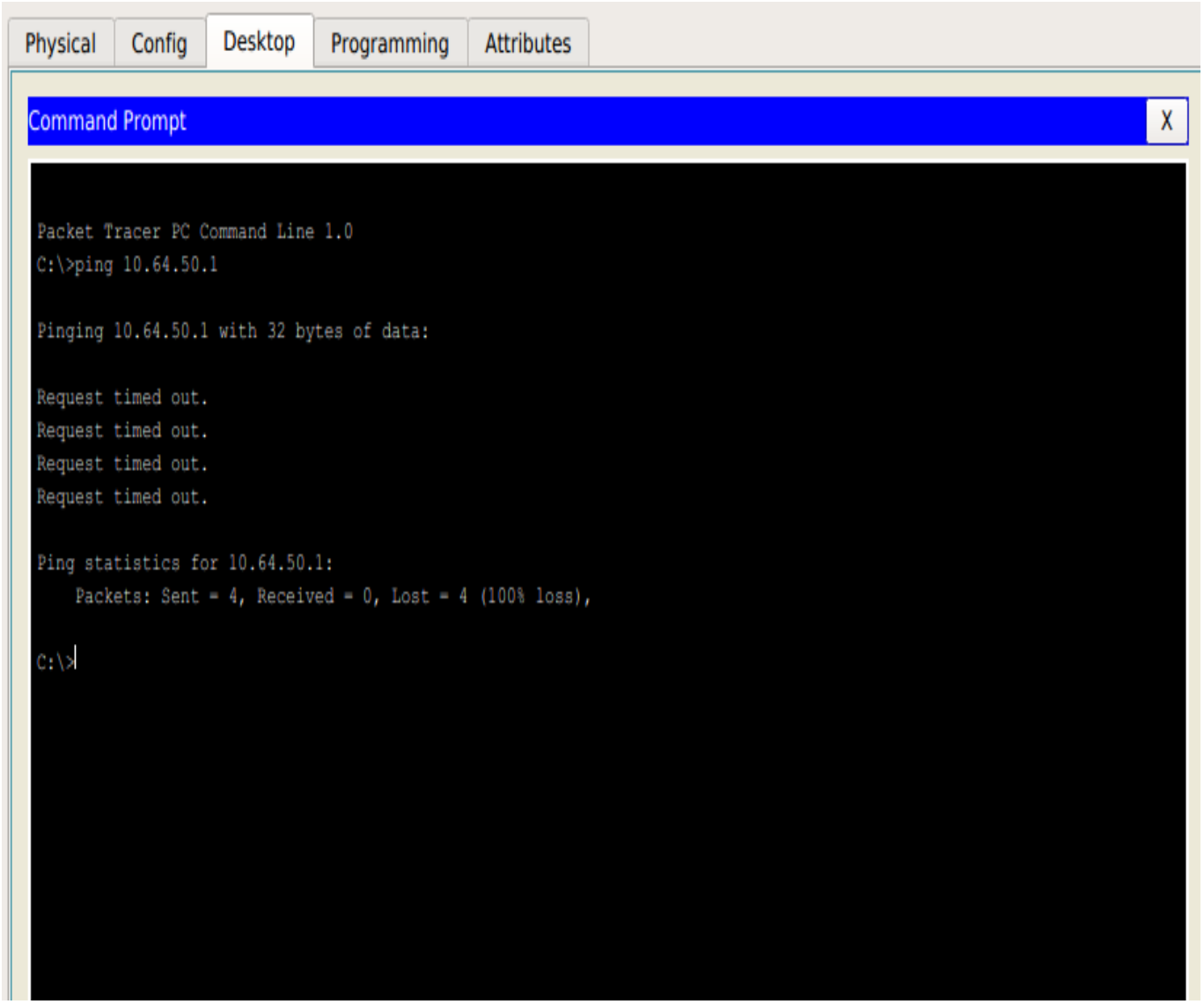

FIGURE 4.24 – Accés interdit entre le pc14 et PC11

Conclusion

Ce chapitre est consacré à la réalisation de notre projet.Nous avons commencé par la présentation du simulateur cisco packet tracer,dans lequel nous avons construit notre architecture réseaux du district naftal,puis nous avons expliqué comment nous avons configuré

Enfin,nous avons éffectué un ensemble de test de validation et de verification afin de valider la solution proposée

CONCLUSION GÉNÉRALE

Conclusion générale

Tout au long de la préparation de notre projet de fin de cycle, nous avons simuler la mise en place de la technologie des vlans au sein de l'entreprise NAFTAL avec le simulateur ''Packet Tracer".

Notre travail au sein de l'entreprise NAFTAL concernont l'étude du réseau de l'entreprise avec son architecture. Et la description de la solution du réseau local virtuel (VLAN) proposeé afin d'entamer la réalisation(sachant qu'on a été présent au sein de l'entreprise que pour deux séances ,à cause des restrictions sanitaire due au COVID-19).

En effet, le déploiement de la solution VLAN dans l'ensemble de l'entreprise NAFTAL, a permis d'offrir un enchainement de données à la fois sécurisé et optimisé.

Enfin, nous espérons que notre travail apportera une validation pratique et donnera une bonne cause pour mieux explorer ce domaine et mettre en œuvre les possibilités réseautiques au profit des entreprises et organisations.

Bibliographie

[1] R. CIREDDU. cours sur la topologie des réseaux. lycée La Matinière Monplaisir.

[2] https//doc.lagout.org/programmation/La20topologie20des20reseaux.pdf.Consulté le 20/05/2020.

[3] G. PUJOLLE. Initiation aux reseaux. Edition eyrolles, 2014.

[4] Philippe Atelin. Réseaux informatiques Notions fondamentales (Normes, Architecture, Modèle OSI, TCP/IP, Ethernet, Wi-Fi,...). Editions ENI, 2009.

[5] http//ista02.blogspot.com/2015/03/Modele-TCPIP-et-protocoles.html,consulté le 03/10/2020.

[6] Philippe Latu. Technologie rnis. 2000 .

[7] Philippe Atelin and José Dordoigne. TCP/IP et les protocoles Internet. Editions ENI, 2006.

[8] Dean .T,.Réseaux Informatique. Edition RYNALD GOULET. 2001.

[9] F. Rihani,F.Bouarroudj,Mémoire de fin d'étude,Utilisation des Tics dans la sécurité.

[10] A.EL GUERAA,I.DANI,Mémoire de fin d'étude,L'audit de sécurité du réseau Marsa Maroc

[11] http//perso.modulonet.fr/placurie/Ressources/BTS2-AMSI/Chap-8-Les20VPN.pdf,consulté le 20 Septembre 2020.

[12] http ://mariepascal.delamare.free.fr/IMG/pdf/VLAN-CM.pdf, consulté le 07 avril 2020.

[13] https//shmsprod.s3.amazonaws.com/media/editor/143832/Advantages-and-Disadvantages-of-VLANs.pdf consulté le 07 avril 2020.

[14] A.DIALLO H.TALL., Etude el Dlise en plate d'UD réseau informatique séturisé à l'hôpital de jour du tenlre Hospifalier Universitaire Sanou Souro de Bobo-Dioulasso.

[15] I.GADOUCHE H. BABA HAMED ,Installation mise en place des VLANs sécurisation des ports,

[16] https//www.cisco.com/c/en/us/support/docs/lan-switching/8021q/17056-741-4.html, consulté le 01 mai 2020 .

[17] http//www-igm.univ-mlv.fr/ dr/XPOSE2006/SURZUR-DEFRANCE/802.1q.html,consulté le 07/06/2020.

[18] Paul C. Rollins, "Virtual Local Area Networks and Wireless Virtual Local Area Networks", 3 May 2001.

[19] F.Nolot. cours5-VTP. Académie Cisco, 2007.

[20] Steve A Rouiller. Virtual lan security : weaknesses and countermeasures. available at uploads.askapache. com/2006/12/vlan-security-3. Pdf , 2006.

[21] K.TRABELSI H.AMARA ,Mise en place des réseaux LAN interconnectés en redondance par 2 réseaux WAN.

[22] I.REDOUANE Y.AMOUCHE, Mémoire de fin d'étude , Proposition d'une nouvelle architecture LAN et implémentation D'une solution VLAN.

[23] https ://summarynetworks.com/ccna/ccna2/course/module9/9.1.1.1/9.1.1.1.html,consulté le 07/09/2020.

[24] https//clubtutoinformatique.blogspot.com/2012/09/les-listes-de-controle-daccesacl.html,consulté le 07/09/2020

[25] http//sen.arbezcarme.free.fr/atelier/3.3-Rotation-3-ToutEnBois/3.3.6-Simulation-du-fonctionnement-d-un-reseau-informatique/TP20Cisco20Packet20Tracer.pdf,consulté le 07/09/2020.

Résumé

La revolution technologique dans le monde actuel a bouleversé le domaine des réseaux en procédant vers la segmentation et la virtualisation dont la technologie des VLANs dispose.

D'ailleurs, l'usage des réseaux locaux virtuels est devenu systématique dans les infrastructures d'interconnexion contemporaines.

L'objectif de notre travail consiste a implémenter une solution en utilisant la technologie des Vlans afin de segmenter et sécuriser le réseau intranet de l'entreprise NAFTAL, en le simulant avec le ''PACKET TRACER".

Mot clés :Réseau local, Vlan, segmentation, sécuriser, Packet tracer.

Abstract

The technological revolution in today's world has revolutionized the field of networks by moving towards the segmentation and virtualization that VLAN technology has to offer.

Moreover, the use of virtual local area networks has become systematic in contemporary interconnection infrastructures.

The objective of our work is to implement a solution using Vlan technology to segment and secure the intranet network of the company NAFTAL, simulating it with the "PACKET TRACER".

Keywords : Local Area Network, Vlan, Segmentation, Secure, Packet tracer.