République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique
UNIVERSITE ABDERRAHMANE MIRA – BEJAIA
FACULTE DES SCIENCES EXACTES
DEPARTEMENT D'INFORMATIQUE

Mémoire de fin de cycle

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

Option : Administration et Sécurité des Réseaux

THEME

Proposition d'une nouvelle architecture LAN et implémentation d'une solution VLAN
Cas : SARL « ifri »

Soutenus devant le jury composé de :

Président :
Mr. ACHROUFENE Achour

Examinateur :
Mr. CHENNA Abdelbasset

Encadrant :
Mr KADJOUH Nabil

Encadrant du stage :
Mr MEZIANI Nabil

Réalisé par :
REDOUANE Idir
AMAOUCHE Youva

Promotion 2015/2016

REMERCIMENTS

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

Un chaleureux merci pour notre cher promoteur Mr N.KADJOUH d'avoir accepté de nous encadrer tout au long du semestre, et de travailler avec nous pour la réalisation de ce projet.

Un grand merci pour l'organisme d'accueil « ifri » qui nous ont acceptés comme stagiaires et qui nous a donnés une chance pour découvrir le domaine professionnel. Ainsi, que pour tous les travailleurs qui nous ont aidés de près ou de loin durant notre période su stage.

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

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

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

Enfin, nous tenons à exprimer nos meilleurs remerciements à nos parents, nos frères et sœurs, ainsi, que toute personne qui nous à soutenue et encouragée.

DÉDICACES

Je dédie ce modeste travail et ma profonde gratitude à toute ma grande famille et à mes proches amis, Qu'ils trouvent ici l'expression de ma reconnaissance :

À mes très chers grands-parents.

À mes très chers parents, pour leurs amour et sacrifices.

Je le dédie aussi à tous mes oncles et tantes.

À mes adorables frères, sœur pour leur patience.

À chaque cousins et cousines.

Je le dédie particulièrement à la mémoire de mon oncle Omar et mon grand père Ali qu'Allah vous ouvre les portes du paradis.

À mes chers amis Karim SAKER et Adel BAA.

A mon binôme Youva et sa famille.

À tous les étudiants de la promotion informatique de l'université de Béjaïa.

Enfin je le dédie à tous mes amis et à tous ceux qui me connaissent.

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

Idir.

DÉDICACES

Je dédie ce travail, à ma famille, à mes très chers parents, auxquels je souhaite une longue vie et une bonne santé, à mes frères, mes sœurs, à mes deux familles paternelle et maternelle.

Une dédicace à tous mes amis, avec qui j'ai passé d'agréables moments pendant mon parcours universitaire.

Une dédicace spéciale à mes deux amis, Karim SAKER et Adel BAA, avec lesquels je partage des bons souvenirs que je n'oublierai jamais.

A la famille de mon binôme Idir, avec qui j'ai eu le plaisir de réaliser ce projet, nous avons passé des périodes riches d'émotions.
Le plus important, est que nous avons pu réussir à faire notre projet ensemble, un travail d'équipe.

Enfin, je le dédie à mon frère Samir alias L'Algérino avec qui j'ai beaucoup d'affinité.

Et à tous ceux qui ont contribué à la réussite de ce projet.

Youva.

Table des Matières

Liste des Figures

Liste des Tableaux

Liste des abréviations

ACL Access Control List

BOOTP Bootstrap Protocol

CFI Canonical Format Identifier

CLI Command Language Interface

CRC Cyclic Redundancy Codes

DHCP Dynamic Host Configuration Protocol

FTP File Transfer Protocol

HTTP HyperText Transfer Protocol

IOS Internetwork Operating System

IP Internet Protocol

IPV4 Internet Protocol version 4

IPX Internetwork Packet Exchange

ISL Inter Switch Link Protocol

ISO International Standards Organisation

LAN Local Area Network

MAC Media Access Control

MAN Metropolitan Area Network

OSI Open System Inteconnection

RIP Routing Information Protocol

RSTP Rapid Spanning Tree Protocol

STP Spanning Tree Protocol

TCI Tag Control Information

TCP Transmission Control Protocol

TPID Tag Protocol Identifier

VLAN Virtual Local Area Network

VTP Vlan Trunking Protocol

WAN Wide Area Network

INTRODUCTION GÉNÉRALE

Introduction Générale

En ces temps modernes, nombreuses sont les entreprises qui se sont dotées d'un réseau informatique. Ce dernier se présente comme un ensemble de ressources mises en place pour offrir un nombre important de service. Ces dernières années, l'évolution des services et du trafic a suscité un développement technologique permettant d'augmenter la capacité et les fonctionnalités des ressources.

Au sein d'une organisation, un réseau informatique est peut être vu comme le cœur de la majeure partie de son activité. Il met en relation des équipements terminaux (ordinateurs, imprimantes, stations de travail, terminaux passifs), et des serveurs. Tous ces éléments sont entièrement sous la responsabilité de l'entreprise.

En effet, l'utilisation d'un réseau local est primordiale au bon fonctionnement d'une entreprise car il facilite la transmission, la duplication, le partage des dossiers et des périphériques. Il permet aussi le traitement et la consultation des bases de données et une transmission rapide et fiable des données.

Parallèlement, le développement de l'entreprise entraine de nombreuses contraintes pouvant réduire les performances de son réseau local : accroissement du nombre des utilisateurs, volume important du trafic sur le réseau, peu de sécurité et d'agilité dans l'administration du réseau.

Cependant, l'évolution des réseaux locaux a vu l'introduction d'un concept appelé VLAN, réseau local virtuel, afin de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.).

A travers notre projet de fin de cycle, nous allons proposer une nouvelle architecture pour le réseau local du site principal de la SARL « ifri » tout en le segmentant grâce essentiellement à l'implémentation des VLANs dans le but d'assurer le fonctionnement optimal de ses ressources réseaux et assurer à ses membres un accès rapide à l'information et un partage facile des données au quotidien, également une souplesse dans l'administration et la gestion du réseau.

Dans le présent mémoire, nous présenterons en détail les étapes que nous allons suivre afin de réaliser notre projet, structuré en quatre chapitres organisés comme suit :

- Le premier chapitre s'intitulant « ***Généralités sur les réseaux informatiques*** **»**, définit quelques notions théoriques de base, qui aideront et seront utiles pour la compréhension de la problématique posée, à savoir la définition d'un réseau, les topologies, les types, etc.
- D'autre part, le second chapitre nommé « ***Introduction aux réseaux locaux virtuels*** », porte sur l'état de l'art sur les réseaux informatiques virtuels ou nous allons faire le point sur le concept des VLANs, une description de leurs types, leurs utilités et quelques protocoles permettant leurs gestions.

- Le troisième chapitre « ***Présentation de l'organisme d'accueil*** », est basé sur la présentation de l'entreprise « ifri », en indiquant quelques informations nécessaires, comme l'organigramme des directions, le matériel informatique existant ainsi que la présentation du réseau existant dans le but de détecter les problèmes qu'il rencontre, puis proposer une solution à adopter.

- Le dernier chapitre « ***Conception et Simulation*** », est constitué de 2 parties telles que :

  - Partie 1 : Basée sur la conception du modèle type
  - Partie 2 : La simulation contenant une présentation de l'outil de travail à savoir « Cisco Packet Tracer » ainsi que toutes les configurations appliquées des solutions et des tests de validation.

Enfin, à travers la conclusion générale, nous ferons une récapitulation du travail effectué ainsi que l'expérience acquise durant ce projet.

CHAPITRE I

GÉNÉRALITÉS SUR LES RÉSEAUX INFORMATIQUES

CHAPITRE I

GENERALITES SUR LES RESEAUX INFORMATIQUES

Introduction

Un réseau informatique permet de relier un ensemble de matériels par des supports de transmission qui leur permettent d'échanger des données entre eux. Pour bien mener notre projet, comprendre les notions de bases sur les réseaux informatiques est très important afin de bien maitriser son sujet.

L'objectif de ce chapitre est de présenter quelques concepts de bases sur les réseaux informatiques, pour bien aider à mieux assimiler le fonctionnement des réseaux. Donc, toutes les notions nécessaires seront présentées, tirant exemple de la classification des réseaux, la topologie, le modèle OSI et TCP/IP ainsi les périphériques réseaux.

I.1. Définition d'un réseau

Un réseau (network) est un ensemble des moyens matériels et immatériels mis en œuvre pour assurer les communications entre ordinateurs, stations de travail et terminaux informatiques.

Les réseaux informatiques permettent aux utilisateurs de communiquer entre eux et de transférer des informations. Ces transmissions de données peuvent concernées l'échange de messages entre utilisateurs, l'accès à distance aux bases de données ou encore le partage de fichiers [1].

I. 2. Les différents types de réseaux

On distingue différents types de réseaux selon leur taille (en terme 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 [2] selon leur échelle géographique :

- LAN (local area network)
- MAN (metropolitan area network)
- WAN (wide area network)

I.2.1. LAN (Local Area Network):

Un réseau local (Local Area Network) est un réseau informatique a une échelle géographique relativement restreinte, il est utilisé pour relier entre eux les ordinateurs : par exemple d'une habitation particulière, d'une entreprise, d'une salle informatique et d'un bâtiment. L'infrastructure est privée et est gérée localement.

Les LANs classiques offrent des dédits de l'ordre de Mbps sur de courtes distances, les plus évolués permettent d'atteindre 100Mbps, les réseaux à 1Gbpas sont même annoncés aujourd'hui.

I.2.2. MAN (Metropolitan Area Network)

Les MAN (Metropolitan Area Network) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer comme si 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).

I.2.3. WAN (Wide Area Network)

Un WAN (Wide Area Network ou réseau étendu) interconnecte plusieurs LANs à travers de grandes distances géographiques.

Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles.

Les WAN fonctionnent grâce à des routeurs qui permettent de "choisir" le trajet le plus approprié pour atteindre un nœud du réseau. Le plus connu des WAN est Internet.

I.3. Topologies des réseaux

I.3.1. Topologie en Bus

C'est l'organisation la plus simple d'un réseau. En effet tous les ordinateurs sont reliés à une même ligne de transmission (Bus) par l'intermédiaire de câble, généralement coaxial. La connexion poste-câble constitue un nœud et un message est émis à partir de n'importe quel poste et dans les deux sens. [3]

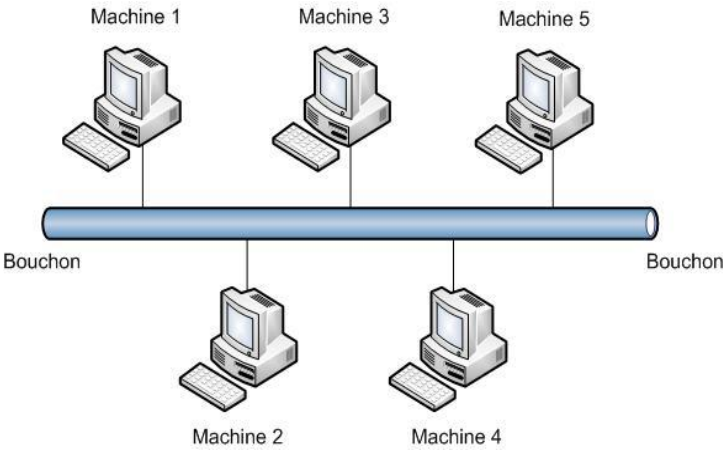

Figure I.1 : Topologie en bus.

I.3.2. Topologie en Anneau

Cette topologie équivaut fonctionnellement à un Bus dont le câble se referme sur lui-même. Les ordinateurs du réseau communiquent chacun à leur tour, on a donc une boucle d'ordinateurs sur laquelle chacun va "avoir la parole" successivement.

Cette topologie a l'inconvénient suivant :

Si le câble présente un défaut, le réseau ne fonctionne plus.

Cette topologie est beaucoup moins utilisée car elle est très chère. En réalité, dans une topologie anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un **répartiteur** qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre-eux un temps de parole [3].

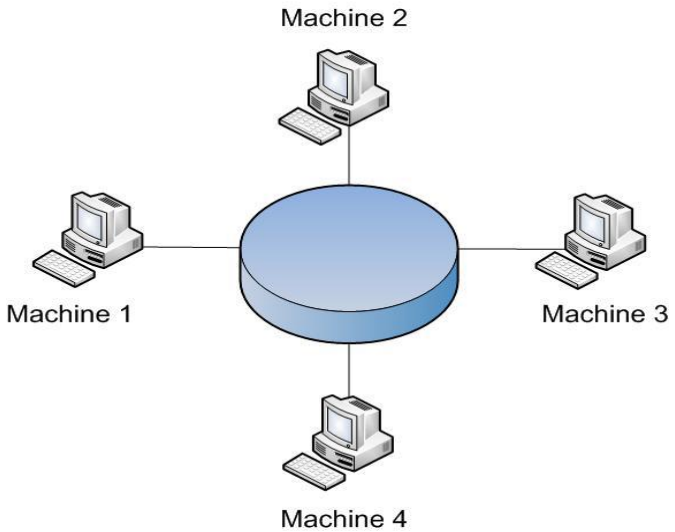

Figure I.2 : Topologie en anneau

I.3.3. Topologie en Etoile

Dans cette topologie, chaque machine est reliée par un câble différent à un nœud central appelé "**Hub**" ou "**Concentrateur**".

Le Hub contient un certain nombre de ports sur lesquels sont branchées les machines du réseau. Il propage les signaux arrivant sur chacun de ses ports vers tous les autres ports. Ainsi les signaux émis par chaque ordinateur atteignent tous les autres ordinateurs.

Cette topologie offre plus de tolérance de panne, car une coupure dans un câble n'affecte que l'ordinateur qui est branché dessus et non pas le reste du réseau [3].

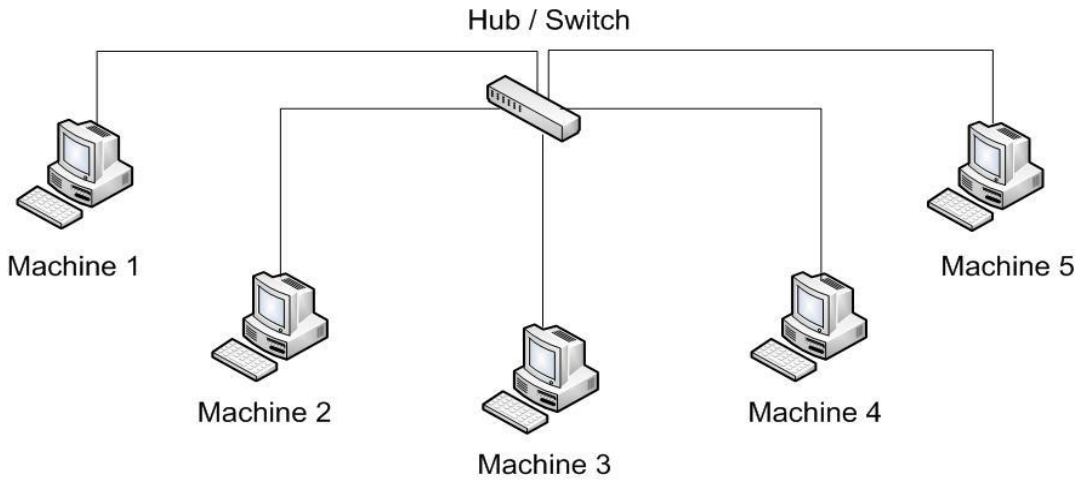

Figure I.3 : Topologie en étoile

I.3.4. Topologie en Arbre

La topologie en arbre repose sur une hiérarchie des équipements réseaux. Cette topologie se base en grande partie sur des concentrateurs/commutateurs (Switch/Hub), c'est-à-dire qu'un hub ou qu'un Switch se trouve être le père (comprendre tout en haut de la hiérarchie), puis que plusieurs hubs/Switchs lui sont connectés qui à leurs tours possèdent des périphériques enfants [4] :

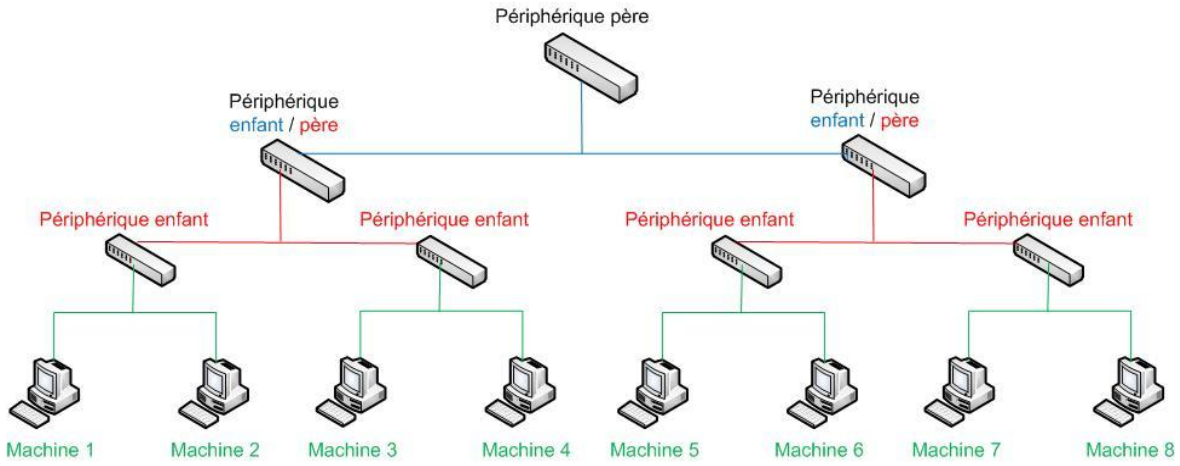

Figure I.2 : Topologie en arbre.

Dans un réseau de type Ethernet, on peut connecter jusqu'à 4 niveaux de concentrateurs/commutateurs. Cette topologie fonctionne de la même façon qu'une topologie en étoile sauf qu'elle est bien plus étendue.

I.4. Modèle OSI (Open System Interconnection)

Pour faciliter l'interconnexion des systèmes, un modèle dit d'interconnexion des systèmes ouverts, appelé encore OSI (Open System Interconnection) a été défini par ISO (International Standards Organization) [5].

Le modèle OSI décrit un ensemble de spécifications pour une architecture réseau permettant la connexion d'équipements hétérogènes. Le modèle OSI normalise la manière dont les matériels et les logiciels coopèrent pour assurer la communication réseau. Ce modèle est organisé en sept couches successives [5].

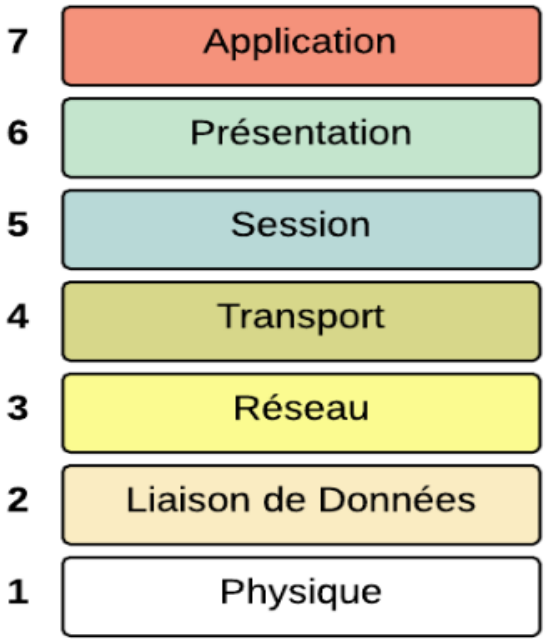

Figure I. 3 : Le Modèle OSI.

- **Couche physique :** Cette couche gère la transmission des bits sur un support physique.
- **Couche liaison de données :** Cette couche assure le contrôle de la transmission des données, elle gère la fiabilité du transfert de bits d'un nœud à un autre du réseau, comprenant entre autres les dispositifs de détection et correction d'erreurs, ainsi que les systèmes de partage des supports. L'unité de données à ce niveau est appelée trames.
- **Couche réseau :** Cette couche assure la transmission des données sur les réseaux. C'est ici que la notion de routage intervient, permettant l'interconnexion de différents réseaux. En plus du routage, cette couche assure la gestion des congestions. L'unité de données à ce niveau est appelée paquet.
- **Couche transport :** Cette couche gère le transport fiable des paquets de bout en bout.
- **Couche session :** Cette couche assure l'établissement, maintien et la terminaison des sessions de communication.
- **Couche présentation :** conversion de données en un format standard. A ce niveau il y a la compression et cryptage de données.
- **Couche application :** Cette couche est source et destination de toutes les informations à transporter, elle rassemble toutes les applications qui ont besoin de communiquer par les réseaux : messagerie électronique, transfert de fichiers, gestionnaire de base de données, etc.

I.5. Le modèle TCP/IP

I.5.1. Présentation de TCP/IP

Même si le modèle de référence OSI est universellement reconnu, historiquement et techniquement, la norme ouverte d'Internet est le protocole TCP/IP (pour Transmission Control Protocol/Internet Protocol). Le modèle de référence TCP/IP et la pile de protocoles TCP/IP rendent possible l'échange de données entre deux ordinateurs, partout dans le monde, à une vitesse quasi équivalente à celle de la lumière [6].

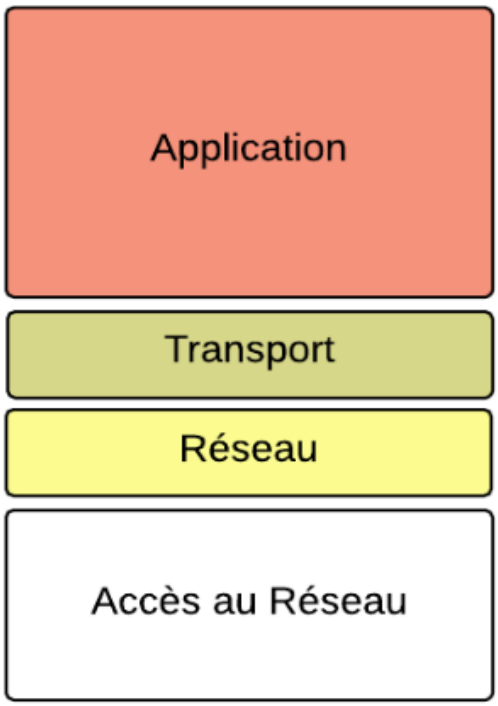

Figure I. 4 : Modèle TCP/IP.

I.5.2. Description des couches TCP/IP :

- **La couche application :** Le modèle TCP/IP regroupe en une seule couche tous les aspects liés aux applications et suppose que les données sont préparées de manière adéquate pour la couche suivante.
- **La couche transport :** La couche transport est chargée des questions de qualité de service touchant la fiabilité, le contrôle de flux et la correction des erreurs. L'un de ses protocoles, TCP (Transmission Control Protocol - protocole de contrôle de transmission), fournit d'excellents moyens de créer, en souplesse, des communications réseau fiables, circulant bien et présentant un taux d'erreurs peu élevé.

- **La couche Internet :** Le rôle de la couche Internet consiste à envoyer des paquets source à partir d'un réseau quelconque de l'inter réseau et à les faire parvenir à destination, indépendamment du trajet et des réseaux traversés pour y arriver. Le protocole qui régit cette couche est appelé protocole IP (Internet Protocol). L'identification du meilleur chemin et la commutation de paquets ont lieu au niveau de cette couche.

- **La couche d'accès au réseau :** Le nom de cette couche a un sens très large et peut parfois prêter à confusion. On lui donne également le nom de couche hôte-réseau. Cette couche se charge de tout ce dont un paquet IP a besoin pour établir une liaison physique, puis une autre liaison physique. Cela comprend les détails sur les technologies LAN et WAN, ainsi que tous les détails dans les couches physiques et liaison de données du modèle OSI [6].

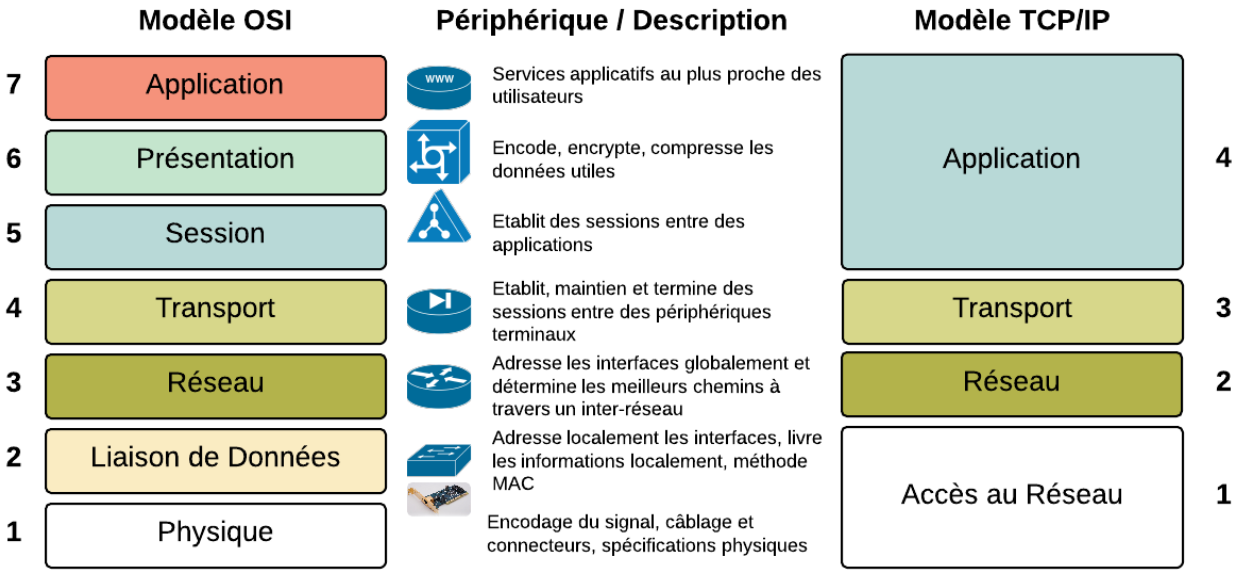

Figure I. 5 : Correspondance des couches (TCP/IP et OSI) [7].

I.6. L'Interconnexion d'un réseau local

On distingue plusieurs types de composants d'interconnexion [8]:

- **La carte réseau** : Elle constitue l'interface physique entre l'ordinateur et le câble réseau. Les données transférées du câble à la carte réseau sont regroupé en paquet composé d'une entête qui contient les informations d'emplacement et des données d'utilisateurs. Souvent la carte réseau est intégrée dans la carte mère. (il faut bien noter que la carte réseau ne fait pas partie des équipements d'interconnexion des réseaux).

- **Le concentrateur** : Le concentrateur (appelé Hub en anglais) est un élément matériel qui permet de relier plusieurs ordinateurs entre eux. Son rôle c'est de prendre les données binaires parvenant d'un port et les diffuser sur l'ensemble des ports.

- **Les répéteurs** : Le répéteur (en anglais repeater) est un équipement utilisé pour régénérer le signal entre deux nœuds du réseau, afin d'étendre la distance du réseau. On peut l'utiliser pour relier deux câbles de types différents.

- **Le pont (bridge)** : Le pont (bridge) est un dispositif matériel permettant de relier des réseaux travaillant avec le même protocole. Il reçoit la trame et analyse l'adresse de l'émetteur et du destinataire et la dirige vers la machine destinataire.

- **Les commutateurs**: Comme le concentrateur, le commutateur (en anglais Switch) est un élément matériel qui permet de relier plusieurs ordinateurs entre eux. Sa seule différence avec le Hub, il est capable de connaître l'adresse physique des machines qui lui sont connectés et d'analyser les trames reçues pour les diriger vers la machine de destination.

- **Les passerelles :** La passerelle est un système matériel et logiciel permettant de relier deux réseaux, servant d'interfaces entre deux protocoles différents. Lorsque un utilisateur distant contact un tel dispositif, celui-ci examine sa requête, et si celle-ci correspond aux règles que l'administrateur réseaux a défini, la passerelle crée un pont entre les deux réseaux. Les informations ne sont pas directement transmises plutôt traduite pour assurer la transmission de deux protocoles. Ce système permet de relier deux systèmes informatiques qui n'utilisent pas la même architecture.

- **Les routeurs :** Le routeur est un matériel de communication de réseau informatique qui permet de choisir le chemin qu'un message va emprunter. Il est utilisé pour relier des réseaux locaux de technologie différente (par exemple Ethernet et token ring). Il intervient sur la couche réseau.

Conclusion

Au cours de ce chapitre, nous avons défini les réseaux informatiques, leurs différents types et leurs topologies, ensuite nous avons donné une description globale du modèle OSI et TCP/IP et cité les équipements d'interconnexion dans un réseau local afin de bien aborder le chapitre suivant qui sera consacré aux réseaux virtuels (VLANs).

CHAPITRE II

INTRODUCTION AUX RÉSEAUX LOCAUX VIRTUELS

CHAPITRE II

INTRODUCTION AUX RESEAUX LOCAUX VIRTUELS

Introduction

Les réseaux locaux virtuels (Virtual LAN) sont apparus comme une nouvelle fonctionnalité dans l'administration réseau avec le développement des commutateurs.

En effet, dans un réseau local, la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (Vlans), il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage,...). En définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses M AC, numéros de port, protocole, etc.).

Dans ce chapitre, nous allons présenter les principales notions d'un réseau local virtuel et des protocoles VTP, STP et DHCP.

II.1. Segmentation VLAN

Un VLAN (Virtual Local Area Network) est une technologie permettant de créer des segments logiques, indépendamment de l'implantation géographique par une configuration logique à l'aide de matériels et logiciels spécifiques. Elle consiste à regrouper les éléments du réseau (utilisateurs, périphériques, etc.) selon des critères logiques (fonction, partage de ressources, appartenances à un département, etc.) sans se heurter à des contraintes physiques (dispersion des ordinateurs, câblage informatique inapproprié, etc.).

Indépendamment de l'emplacement où se situent les nœuds, les stations peuvent communiquer comme si elles étaient dans le même segment. Un VLAN est assimilable à un domaine de diffusion (broadcast). Ceci signifie que les messages de diffusion émis par une station d'un VLAN ne sont reçu que par les stations de ce VLAN. La communication entre VLANs n'est possible que par l'intermédiaire d'un périphérique de la couche 3 en assure le routage. Il peut s'agir d'un routeur traditionnel ou d'un commutateur de couche 3 [9].

II.2. Les avantages des VLANs

Les VLANs ont beaucoup d'avantages qui permettent une meilleure organisation d'un réseau local, ainsi d'améliorer son fonctionnement en termes de performances et d'efficacité. Ces avantages sont cités ci-dessous [10] :

- **Limiter la propagation du trafic au seul VLAN concerné :** Un flux originaire d'un VLAN donné n'est transmis qu'aux ports qui appartiennent à ce même VLAN. Chacun des VLANs constitue ainsi un domaine de diffusion propre.. C'est pourquoi le trafic doit être routé pour être acheminé entre différents VLANs. C'est-à-dire que la communication inter-VLAN doit se faire par le passage par un routeur pour acheminer le trafic entre les équipements appartenant à des VLANs différents.

- **Meilleures performances :** La création de domaine de diffusion plus petit amène une diminution de la quantité de trafic inutile sur le réseau, qui résulte une augmentation des performances.

- **Flexibilité de segmentation de réseau :** Les utilisateurs et les ressources peuvent être regroupées sans devoir prendre en considération leur localisation physique. C'est-à-dire de se faire connecter à un groupe logique des stations du travail, même si ces dernières ne sont pas géographiquement proches les unes des autres.

- **Simplicité de l'administration du réseau :** Les postes du travail appartenant à un même VLAN peuvent être déplacés d'un lieu à l'autre ou d'une zone à une autre sans devoir à modifier les connexions physique. Ainsi que de nouveaux segments ou utilisateurs peuvent être ajoutés grâce à une simple configuration des commutateurs, soit par la création de nouveaux VLANs, soit par l'affectation de nouveaux utilisateurs à un VLAN.

- **Organisation du réseau :** Les VLANs permettent de constituer autant de réseaux logiques que l'on désire sur une seule infrastructure physique, donc, cela conduit à une organisation efficace du réseau (mieux organiser son réseau).

- **Augmentation de la sécurité :** Grâce à la notion des groupes, qui conduit à l'isolement de certains d'eux, certaines ressources seront alors protégées, ainsi il y aura un renforcement considérable de la sécurité du réseau.

II.3. Types de VLAN

II.3.1. VLANs implicites

Lorsqu'un message Ethernet passe d'un commutateur (Switch). Tout élément connecté à un Switch peut accéder à tout autre élément du même VLAN connecté sur le même Switch. Le mode de transmission du Switch permet de mettre directement en relation deux postes [11].

II.3.2. VLANs explicites

Une étiquette (tag) d'appartenance à un VLAN est ajoutée à chaque Ethernet.

Pour définir des VLANs, il faut que les commutateurs supportent cette extension de la technologie Ethernet (IEEE 802.1q) [11].

II.4. Méthode d'implémentation des VLANs

L'attribution des VLANs dans un commutateur est faite selon trois techniques, tel que chaque technique est associée à un niveau donné du modèle OSI. Cette attribution est faite soit par le numéro de port, l'adresse mac ou le sous-réseau [12].

- **VLAN par port (VLAN niveau 1) :** Chaque port du commutateur est affecté à un VLAN donné. L'affectation des ports est statique, donc l'administrateur peut savoir directement le VLAN d'appartenance d'un équipement. Cette technique est efficace dans les réseaux où les déplacements sont rares et contrôlés. En effet, une source externe ne peut y accéder au réseau, sauf si elle se branche sur le port appartenant au VLAN voulu à accéder, donc, un renforcement de la sécurité. Par contre, son inconvénient est sa lourdeur d'administration. En effet, si un matériel est déplacé et que l'on désire qu'il soit toujours dans le même VLAN, il faudra alors configurer le nouveau port [12].

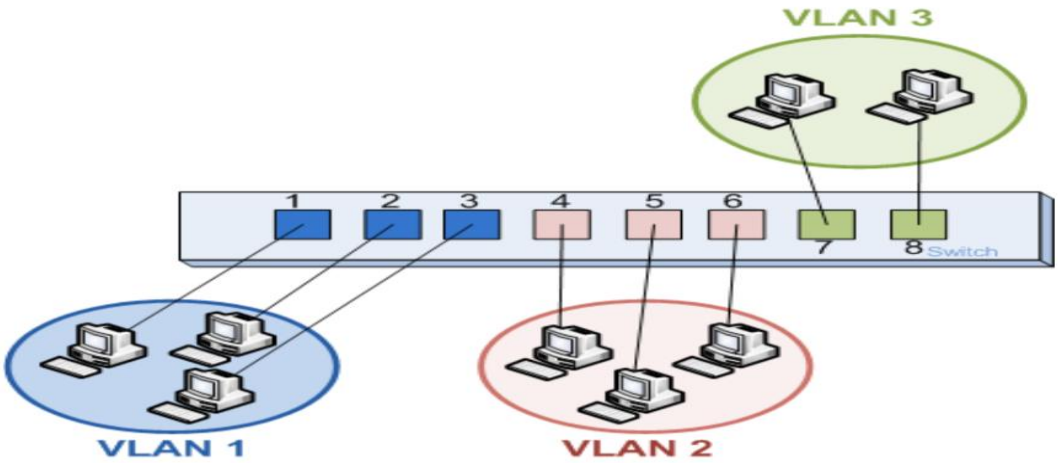

Figure II.1 : VLAN par port [13].

- **VLAN par adresse MAC (VLAN niveau 2) :** Chaque adresse MAC est affectée a un VLAN. En effet, une table (adresse MAC/VLAN) sur le commutateur doit être remplie, et l'affectation (Port/VLAN) s'effectue à l'aide des premiers paquets portant l'adresse MAC source. L'avantage de cette technique est que les déplacements d'une station se fait sans devoir à reconfigurer les commutateurs et la station continue toujours à appartenir au même VLAN, si par exemple un Par contre, l'inconvénient majeur de ce type de VLAN est que l'administration est complexe pour la configuration et la mise en place de la base de données. En effet, lorsque le nombre d'éléments devient important, le maintien de la base de données devient plus difficile lors de l'ajout de nouveaux équipements ou lors de la réaffectation d'une adresse MAC à un autre VLAN [12].

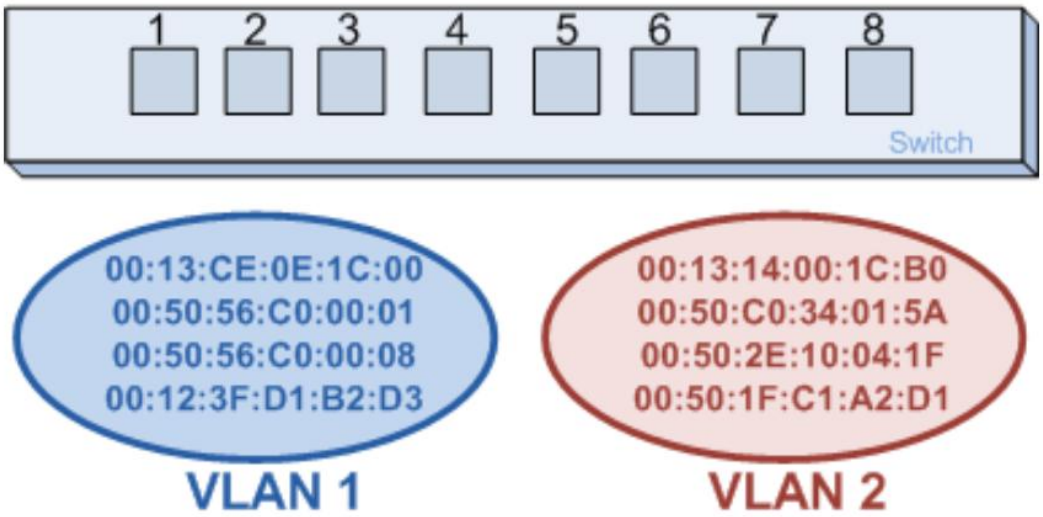

Figure II.2 : VLAN par adresse MAC [13].

- **VLAN par adresse IP (VLAN niveau 3) :** chaque station est affecté a un VLAN en fonction de son adresse IP. Dans ce cas, une table (adresse IP/VLAN) est construite sur le commutateur. L'association (Port/VLAN) est faite d'une manière automatique, en décapsulant le paquet jusqu'à l'adresse source. Dans ce type de VLAN, les commutateurs apprennent automatiquement la configuration des VLANs en accédant aux informations de couche 3.
  L'avantage de cette solution est le déplacement des équipements sans reconfiguration, car, affectation est automatique à un Vlan suivant une adresse IP. Par contre, une légère dégradation des performances aura lieu, et cela est dû à une analyse plus profonde des informations contenues dans les paquets lors de la décapsulation afin de déterminer le VLAN d'appartenance, d'où, l'obligation d'utiliser un équipement plus couteux pouvant décapsuler le niveau3 [12].

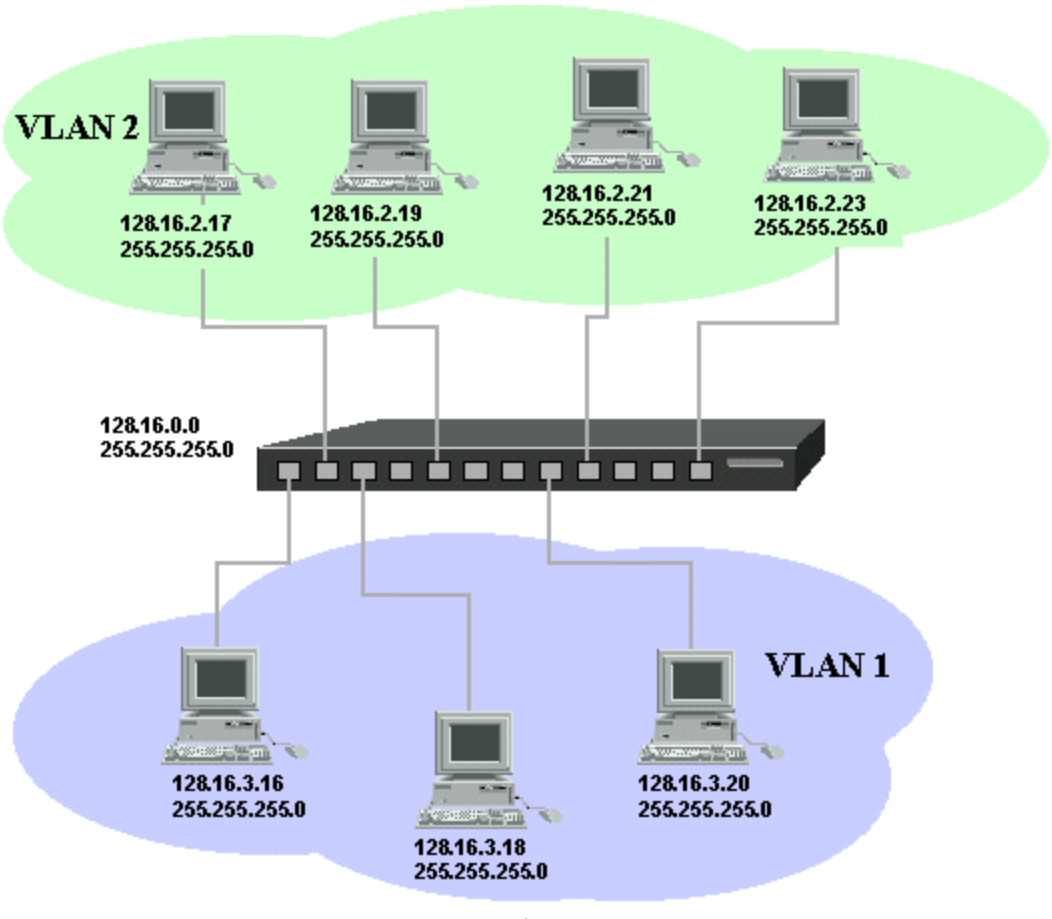

Figure II. 3 : VLAN par adresse IP [13].

Le Tableau suivant montre quelques différences existantes entre les trois techniques d'implémentation VLAN :

Type de VLAN	Description
VLAN par port	• Méthode de configuration la plus courante. • Ports affectés individuellement à un ou plusieurs VLANs. • Facile à mettre en place.
VLAN par adresse MAC	• Rarement utilisé. • Chaque adresse doit être saisie dans le commutateur et configurée individuellement. • Difficile à administrer et à gérer.
VLAN par adresse IP	• Une légère dégradation de performances peut se faire sentir dans la mesure de décapsulation des paquets. • Utilisation d'un équipement supportant la décapsulation du niveau3.

Tableau II.1 : Les différentes techniques d'implémentation VLAN **[**12].

II.5. Les protocoles de transport des VLANs :

II.5.1. La norme 802.1q

Ici, l'idée serait d'arriver à ce que certains ports du Switch puissent être assignés à plusieurs VLANs, ça fera économiser du câble (et aussi des ports sur le SWITCH).

Le principe consiste à ajouter dans l'en-tête de la trame Ethernet un marqueur qui va identifier le VLAN. Il existe quelques solutions propriétaires pour réaliser ceci, mais le système s'est avéré tellement intéressant qu'une norme a été définie, il s'agit de la norme 802.1q [14].

II.5.1.1. Description de la norme

La figure suivante illustre la modification de la trame Ethernet et l'ajout d'un champ sur 4 octets par la norme 802.1Q :

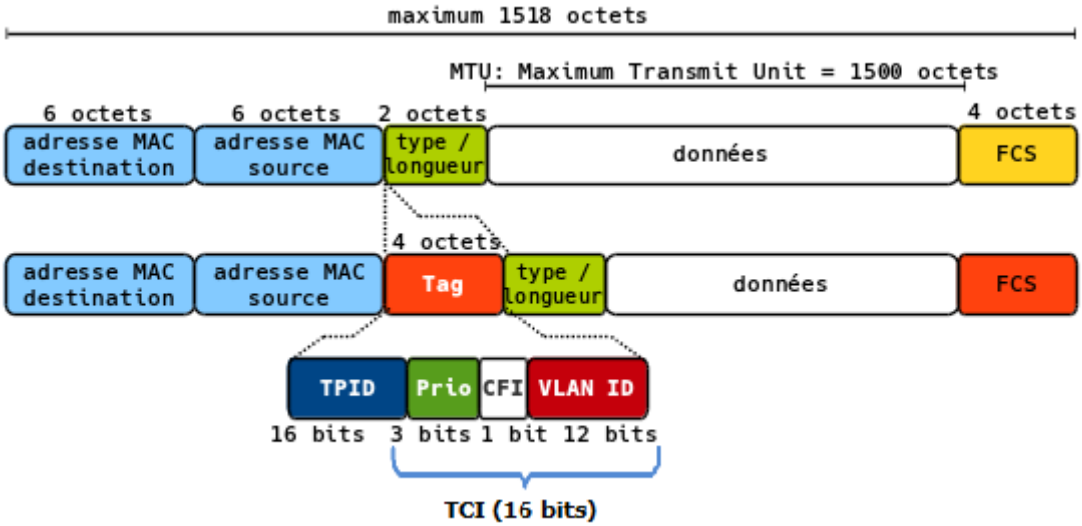

Figure II.4 : Extension de la trame Ethernet modifiée par la norme 802.1Q [14].

II.5.1.2. Tag Protocol Identifier (TPID)

C'est la partie qui définit le protocole de tag utilisé. Dans le cas du 802.1Q on trouvera comme valeur (en notation hexadécimale) : 0x8100.

II.5.1.3. Tag Control Information (TCI)

Cette partie se compose de trois champs :

- **User Priority :** 3 bits utilisés pour coder 8 niveaux de priorité (de 0 à 7). On se sert de ces 8 niveaux pour fixer la priorité des trames d'un VLAN par rapport à d'autres.
  (Exemple d'utilisation : on favorise un VLAN sur lequel on utilise la visioconférence (nécessitant beaucoup de bande passante) par rapport à un VLAN où l'on ne fait qu'envoyer et recevoir des mails).

- **Canonical Format Identifier(CFI) :** Ce champ d'un bit assure la compatibilité entre adresses MAC Ethernet et Token Ring. Un commutateur Ethernet fixe cette valeur à 0 [19].

- **VLAN ID (VID) :** C'est le champ d'identification du VLAN auquel appartient la trame par l'intermédiaire de ce champ de 12 bits, on peut coder 4094 VLAN (les valeurs 0 et FFF sont réservées). La valeur par défaut est 1.

II.5.2. Le protocol ISL (Inter Switch Link Protocol)

Pour étendre les réseaux virtuels sur plus d'un commutateur, CISCO a mis au point son propre protocole ISL. Ce protocole achemine les informations d'appartenance aux réseaux virtuels. ISL représente en fait une structure de trame et un protocole qui, en plus de transport des informations d'appartenance aux réseaux virtuels, permet à ces réseaux d'échanger des trames [14].

II.5.2.1. Présentation générale

Pour identifier les réseaux virtuels, ISL utilise un mécanisme de marquage explicite des paquets. Un commutateur qui utilise ce marquage encapsule la trame reçue dans un paquet dont l'en-tête contient un champ d'appartenance aux VLAN et l'adresse MAC de la trame, permettent d'acheminer le paquet vers le routeur et les commutateurs appropries. Lorsqu'elle atteint le réseau destination, on supprime l'en-tête et la trame est acheminée vers l'équipement récepteur.

II.5.2.2. Structure des trames ISL

Les trames ISL comprennent trois champs principaux :

- Un en-tête qui est constituée de plusieurs champs.
- Trame encapsulée dont la longueur est comprise entre 1 et 24575 octets.
- Champ CRC, ce champ qui est ajoute à la fin du paquet ISL, porte sur l'intégrité du paquet.

II.5.3. Le mode Trunk

Le réseau local est distribué sur différents équipements via des liaisons dédiées appelées Trunks. Un trunk est une connexion physique unique sur laquelle on transmet le trafic de plusieurs réseaux virtuels. Les trames qui traversent le trunk sont complétées avec un identificateur de réseau local virtuel (VLAN id). Grâce à cette identification, les trames sont conservées dans un même VLAN (ou domaine de diffusion) [15].

Les trunks peuvent être utilisés [15]:

- entre deux commutateurs : C'est le mode de distribution des réseaux locaux le plus courant.
- entre un commutateur et un hôte : C'est le mode de fonctionnement à surveiller étroitement. Un hôte qui supporte le trunking a la possibilité d'analyser le trafic de tous les réseaux locaux virtuels.
- entre un commutateur et un routeur : C'est le mode de fonctionnement qui permet d'accéder aux fonctions de routage ; donc à l'interconnexion des réseaux virtuels par routage inter-VLAN.

Ce schéma ci-dessous (Figure II.5), nous illustre la liaison de Trunk entre des commutateurs :

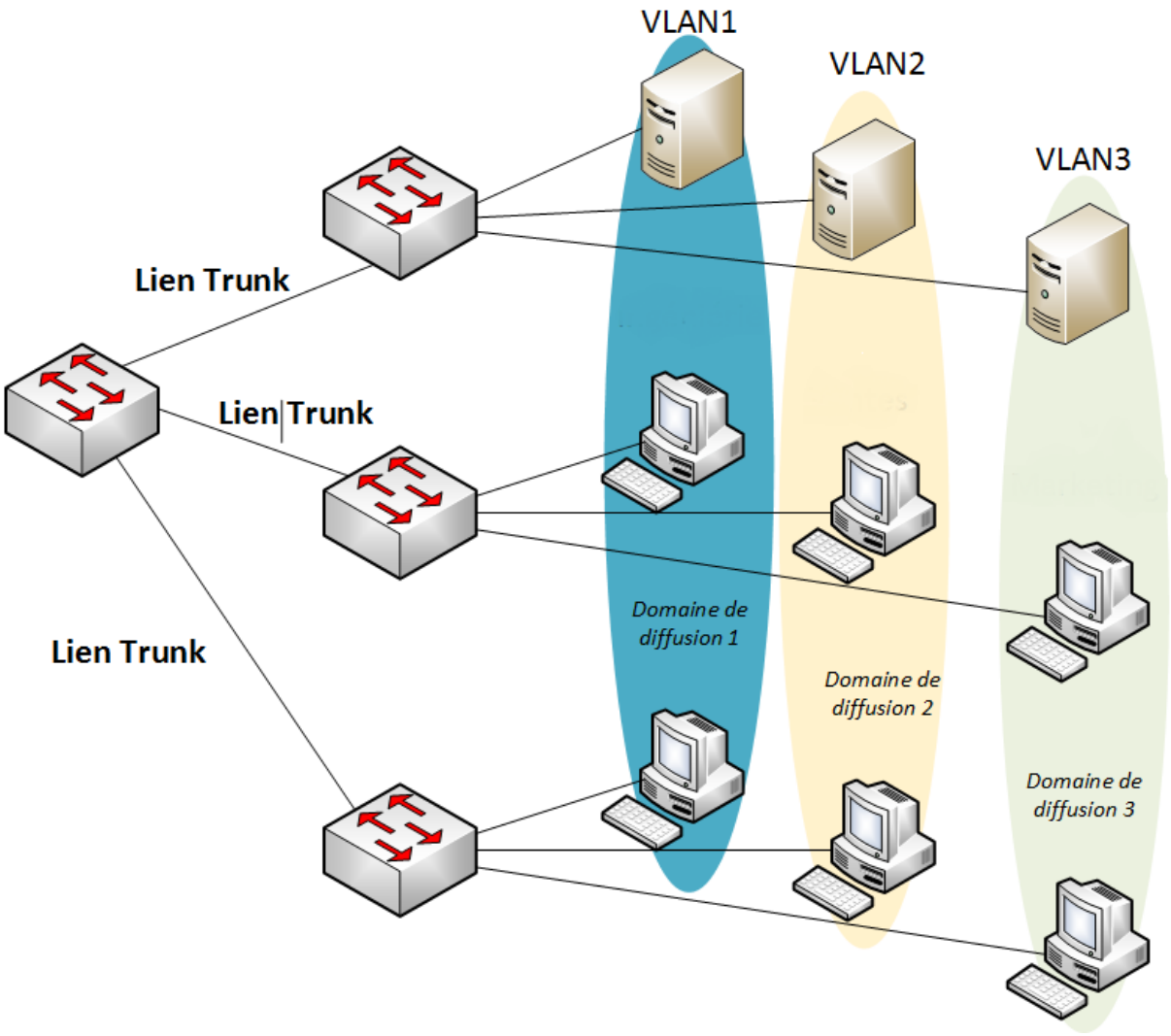

Figure II.5 : Utilisation du Trunk entre des commutateurs.

II.6. Quelques protocoles d'administration et de gestion des VLANs

II.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. Ce protocole est basé sur la norme 802.1q et exploite une architecture client-serveur avec la possibilité d'instancier plusieurs serveurs [16].

II.6.1.1. Fonctionnement du VTP

VTP permet d'ajouter, renommer ou supprimer un ou plusieurs réseaux locaux virtuels sur un seul commutateur (le serveur) qui propagera cette nouvelle configuration à l'ensemble des autres commutateurs du réseau (clients). VTP permet ainsi d'éviter toute incohérence de configuration des VLANs sur l'ensemble d'un réseau local.

Les administrateurs peuvent changer les informations de VLAN sur les commutateurs fonctionnant en mode serveur uniquement. Une fois que les modifications sont appliquées, elles sont distribuées à tout le domaine VTP au travers des liens « trunk » (Cisco ISL ou IEEE 802.1Q). En mode transparent, le Switch reçoit les mises à jour et les transmet à ses voisins sans les prendre en compte. Il peut créer, modifier ou supprimer ses propres VLANs mais ne les transmet pas. Les switchs en mode client appliquent automatiquement les changements reçus du domaine VTP.

VTP permet de gérer les VLANs de la plage **«** normale » (Vlan ID compris entre 1 Et 1005). La création de VLANs dans la plage « étendue » (Vlan ID supérieur à 1005) n'est possible qu'en mode VTP transparent.

Les configurations VTP successives du réseau ont un numéro de révision. Si le numéro de révision reçu par un Switch client est plus grand que celui en cours, la nouvelle configuration est appliquée. Sinon, elle est ignorée.

Quand un nouveau commutateur est ajouté au domaine VTP, le numéro de révision de celui-ci doit être réinitialisé pour éviter les conflits.

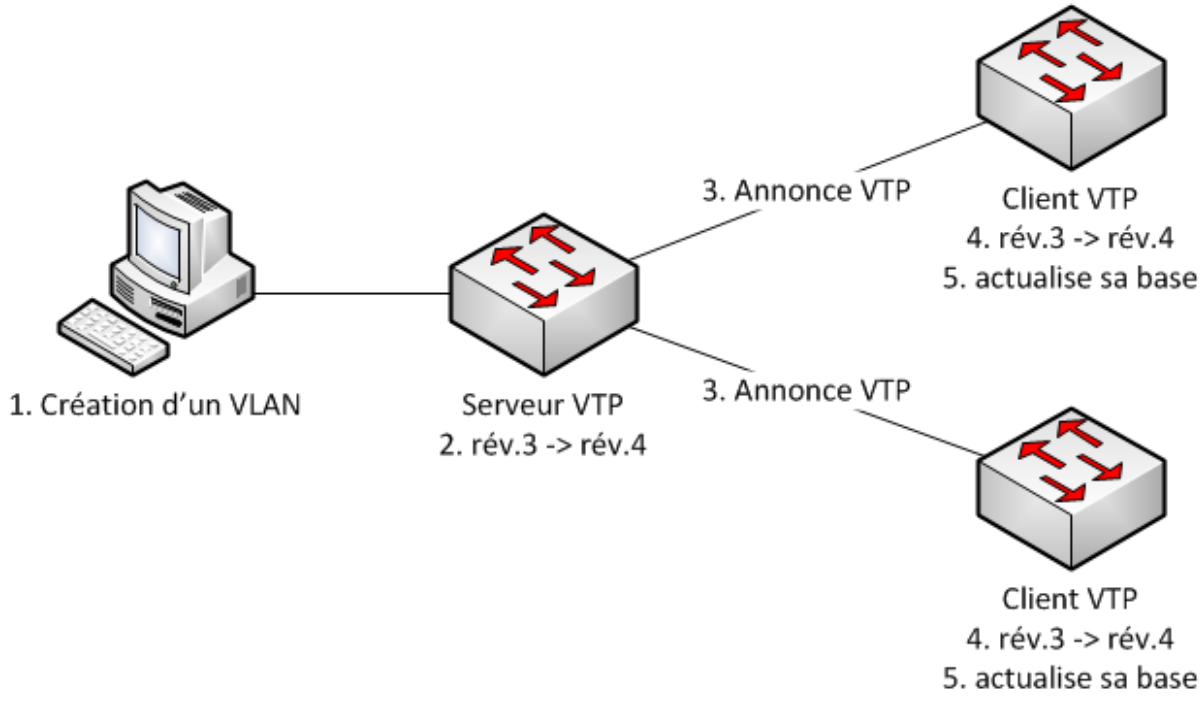

Figure II. 6 : Fonctionnement du VTP.

II.6.1.2. Les modes du VTP

Le protocole VTP développé par Cisco permet de centraliser la gestion de la base des données des équipements Cisco d'un réseau et d'en faciliter l'exploitation. Il est constitué de trois modes :

- **Serveur :** Il s'agit d'un équipement sur lequel il est possible de créer, modifier ou supprimer des VLANs et de les transmettre au domaine VTP.
- **Client :** Il s'agit d'un équipement qui va recevoir les informations des serveurs VTP qui se situent dans le même domaine VTP, les prendre en compte et les retransmettre aux Switchs qui lui sont interconnectés.
- **Transparent :** Le Switch va recevoir les informations des serveurs VTP du même domaine et les retransmettre sans les prendre en compte. Il est possible de créer, modifier ou supprimer des VLANs en local sur ce Switch sans que ceux-ci soient répercutés sur les autres équipements du même domaine.

II.6.2. Protocole Spanning-Tree

Le protocole Spanning-Tree (STP) est un protocole de couche 2 (liaison de données) conçu pour les switchs et les bridges. La spécification de STP est définie dans le document IEEE 802.1d. Sa principale fonction est de s'assurer qu'il n'y a pas de boucles dans un contexte de liaisons redondantes entre des matériels de couche 2. STP détecte et désactive des boucles de réseau et fournit un mécanisme de liens de backup. Il permet de faire en sorte que des matériels compatibles avec le standard ne fournissent qu'un seul chemin entre deux stations d'extrémité [17].

II.6.3. Protocole DHCP

DHCP (Dynamic Host Configuration Protocol). Il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau 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 BOOTP (Bootstrap Protocol) qui est utilisé par exemple lorsque l'on installe une machine à travers un réseau (on peut effectivement installer complètement un ordinateur, et c'est beaucoup plus rapide que de le faire à la main). Cette dernière possibilité est très intéressante pour la maintenance de gros parcs machines. Les versions actuelles des serveurs DHCP fonctionne pour IPv4 [18].

II.7. Les ACLs (Access Control List)

Les listes de contrôle d'accès sont des listes de conditions qui sont appliquées généralement au trafic circulant via une interface de routeur (Figure II.7).

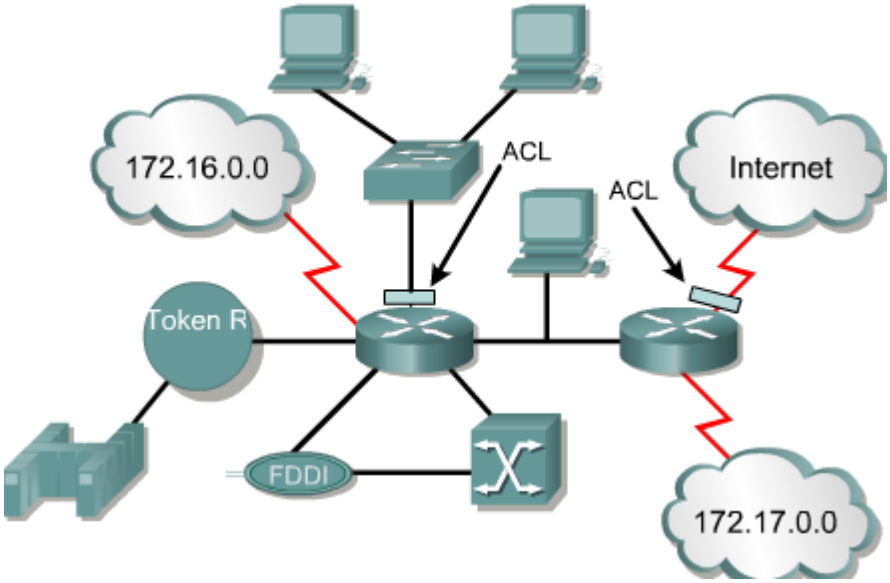

Figure II.7 : Les ACLs [19].

Ces listes indiquent au routeur les types de paquets à accepter ou à rejeter. L'acceptation et le refus peuvent être basés sur des conditions précises. Les ACL permettent de gérer le trafic et de sécuriser l'accès d'un réseau en entrée comme en sortie.

Des listes de contrôle d'accès peuvent être créées pour tous les protocoles routés, tels que les protocoles IP (Internet Protocol) et IPX (Internetwork Packet Exchange). Des listes de contrôle d'accès peuvent également être configurées au niveau du routeur en vue de contrôler l'accès à un réseau ou à un sous-réseau [19].

II.7.1. L'intérêt d'utiliser des ACLs

Voici les principales raisons pour lesquelles il est nécessaire de créer des listes de contrôle d'accès [19] :

- Limiter le trafic réseau et accroître les performances. En limitant le trafic vidéo, par exemple, les listes de contrôle d'accès permettent de réduire considérablement la charge réseau et donc d'augmenter les performances
- Contrôler le flux de trafic. Les ACL peuvent limiter l'arrivée des mises à jour de routage. Si aucune mise à jour n'est requise en raison des conditions du réseau, la bande passante est préservée

- Fournir un niveau de sécurité d'accès réseau de base. Les listes de contrôle d'accès permettent à un hôte d'accéder à une section du réseau tout en empêchant un autre hôte d'avoir accès à la même section
- Déterminer le type de trafic qui sera acheminé ou bloqué au niveau des interfaces de routeur. Il est possible d'autoriser l'acheminement des messages électroniques et de bloquer tout le trafic via Telnet.
- Autoriser un administrateur à contrôler les zones auxquelles un client peut accéder sur un réseau.
- Filtrer certains hôtes afin de leur accorder ou de leur refuser l'accès à une section de réseau. Accorder ou refuser aux utilisateurs la permission d'accéder à certains types de fichiers, tels que FTP ou HTTP.

II.7.2. Les types des listes contrôles d'accès

Il existe trois types d'ACL que voici [19] :

- **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.
- **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. Cela donne une plus grande souplesse pour décrire ce que vérifie la liste de contrôle d'accès. L'accès d'un paquet peut être autorisé ou refusé selon son emplacement d'origine et sa destination, mais aussi selon son type de protocole et les adresses de ses ports.
- **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 :

Dans ce chapitre, nous avons défini en premier lieu le réseau local virtuel. Puis, nous avons cité les différents avantages des VLANs, leurs différents types. Ensuite, nous avons présenté les méthodes d'implémentation des VLANs. Enfin, nous avons cité quelques protocoles d'administration et de gestion des VLANs ainsi que les listes de contrôle d'accès.

CHAPITRE III

PRÉSENTATION DE L'ORGANISME D'ACCUEIL

CHAPITRE III

PRESENTATION DE L'ORGANISME D'ACCUEIL

Introduction

Avant d'entamer notre étude, il convient de commencer par la présentation de l'entreprise et la détermination de notre position au sein du système d'information. On doit cependant donner un aperçu des améliorations finales de la démarche qu'on va mener, et montrer les objectifs à attendre par notre travail.

III.1. Historique et présentation de l'entreprise « ifri »

III.1.1. Historique

La SARL IBRAHIM et fils «IFRI» est une société à caractère industriel, évoluant dans le secteur agro-alimentaire.

Á l'origine, c'était la « **Limonaderie IBRAHIM »** qui existait en **1986**, celle-là a été créé sur les fond propres de Mr **IBRAHIM LAID**, son gérant, dix(10) ans plus tard c'est-à-dire en **1996**, elle fut transformée en **SNC** (société à nom collectif), puis elle s'est fait un statut de **SARL** (société à responsabilités limitées) composée de plusieurs associés.

La SARL IBRAHIM et fils «IFRI», à caractère familial (Les gérants sont IBRAHIM LAID et ses 5 fils), inaugure un premier atelier d'embouteillage d'eau minérale en bouteilles en polyéthylène et téréphtalate (PET), le 20 juillet 1996. Elle fût la première entreprise privée dans le secteur des eaux minérales. A cette date, plus de 7.5 millions de litres d'eau minérale sont commercialisés à l'échelle nationale. La production franchira le cap des 504 millions de L (litres) dans toute la gamme des produits « ifri » en 2011.

Avec près de 30% de parts de marché des eaux embouteillées, cette marque est leader dans les eaux minérales.

III.1.2. Situation géographique

Le complexe de production d'eau minérale naturelle de la SARL IBRAHIM et FILS-ifri est situé dans la commune d'Ighzer Amokrane – Daira d'Ifri Ouzellaguen –Wilaya de Bejaia. Il est localisé au sud-ouest de l'agglomération d'Ighzer Amokrane, soit à 400m au sud de la RN.26.

III.1.3. Identification de la SARL Ibrahim & fils - ifri

L'identification de la Sarl Ibrahim & fils se présente sous la forme de la fiche technique ci-dessous :

Raison sociale	Sarl IBRAHIM et Fils–Ifri
Sigle (Abréviation utilisée)	IFRI
Statut de l'entreprise	Privé
Forme juridique	Société à responsabilité limitée
Année de création	1996
N° R C	98 B 5162810-00 / 06 N° I F : 099806018261598
Capital	1 293 000 000 .00DA
Adresse	Z I Ahrik, Ighzer Amokrane, Ifri-Ouzellaguen 06010 Béjaia
Téléphone	(213) 34 35 12 66 (213) 34 35 10 21
Fax	(213) 34 35 12 32 (213) 34 35 17 59
Email	ifri@ifri-dz.com
Site web	www.ifri-dz.com
Gérant	Mr IBRAHIM Kaci
Effectifs	1030
Secteur d'activité	Agroalimentaire
Type de produits ou services	Production d'Eau Minérale & Boissons diverses.

Tableau III. 1 : Fiche technique de la SARL IBRAHIM et FILS « ifri ».

III.1.4. Les filiales de la SARL Ibrahim & fils -ifri

La SARL IBRAHIM et fils dispose de trois filiales très importantes, pour l'aboutissement des objectifs de l'entreprise mère; deux de ces filiales, sont considérées comme, un important fournisseur pour l'une et un moyen incontournable, d'acheminer et de distribuer à temps, pour l'autre, nous citons les filiales dans le tableau III.2 qui suit :

Filiale	**Activité**	**Adresse**
Général Plast	Production de préformes en PET et bouchons en PEHD.	Zone industrielle Taharacht Akbou Bejaia-Algérie.
Sarl Huileries Ouzellaguen	Activité agricole, transformation (trituration) d'olives et mise en bouteille d'huile d'olive extra vierge	Zone industrielle AHRIK Ighzer Amokrane ifri Ouzellaguen Bejaia.
Sarl Bejaïa Logistique	Composée d'une armada de plus de 200 semi remorque pour le transport sur toutes distances et manutention.	Zone industrielle Taharacht Akbou Bejaia-Algérie.

Tableau III.2 : Les filiales de la SARL IBRAHIM et FILS « ifri ».

III.2. Organigramme de l'entreprise

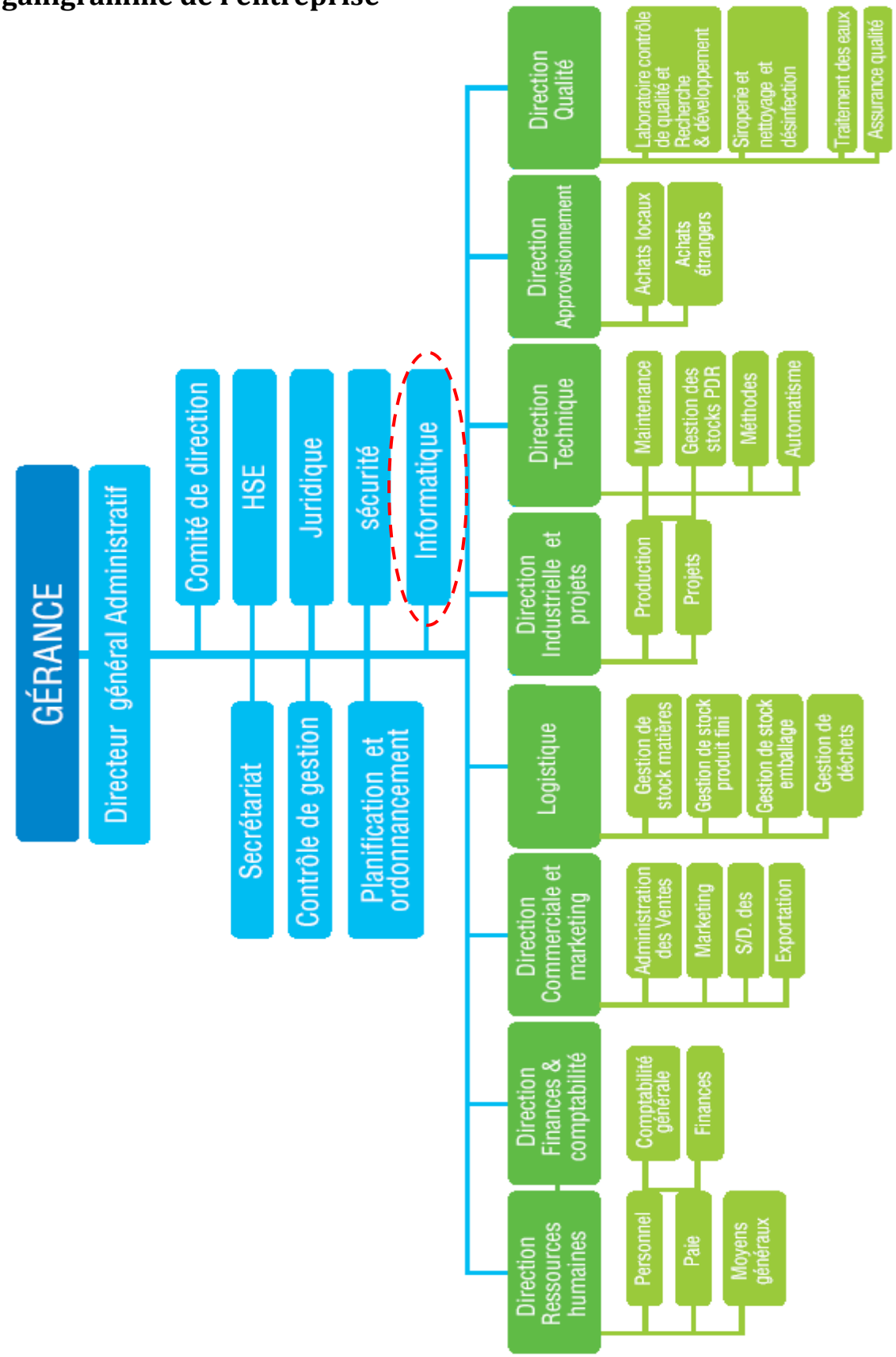

Figure III.1 : Organigramme de l'entreprise « ifri ».

III.3. Le service informatique

Il est composé de quatre (04) éléments, un responsable informatique, un ingénieur applicatif et deux (02) informaticiens.
Les prérogatives du service sont:

- Développement et réalisation des projets informatiques.
- Administration du réseau.
- Gestion du parc informatique.
- Maintenance du système informatique.
- Introduction de nouvelles technologies.
- Formation du personnel aux techniques informatiques.
- Sauvegarde et archivage des données de l'entreprise.

III.4. Ressources matérielles et logicielles existantes

III.4.1. Ressources matérielles

L'entreprise IFRI dispose d'un parc informatique très vaste, l'ensemble du matériel se trouvant au siège du site central est recensé comme suit :

Description de l'Equipment	Quantité	Observation
Serveur IBM	04	Réf: X3550
Serveur HP Pro Liant	01	Réf: DL380
Serveur Dell	01	Réf:
Routeur CISCO Série 1900	01	Modèle : 1941
Micro-ordinateur de Bureau	146	Dell & HP Compaq
Micro-ordinateur Portable	45	Différents Marques
Imprimantes	101	Réseaux et USB
Photocopieur	05	Réseaux en grand model
Switch	41	HP Procuvre & Autres
Point d'accès	12	DLINK, SYSLINK, CISCO …
Terminaux	10	Scan Code à bar
Standard téléphonique ALCATEL Lucent	01	Alcatel

Tableau III. 3 : Résumé du matériel informatique sur le site central.

Pour une description plus détaillée, le tableau suivant résume les éléments matériels les plus essentiels notamment ce qui peuvent être touchés par notre étude.

Equipement	Caractéristiques	Observation
Serveur IBMx3550	→ Plateforme Windows server 2008 R2. → Processeurs intel Xeon 4 cœur(s). → 8GoRAM. → 700 Go HDD	→ Serveur DHCP → Serveur DNS. → Contrôleur de domaine « **ifri-dz.local** ». → Serveur de fichiers.
ServeurIBMx3550	→ Plateforme Windows server 2008 R2. → ProcesseursintelXeon4c œur(s). → 16 Go RAM. → 500 Go HDD	→ Application métier Sage Commerciale, Comptabilité &Immobilisations → Sauvegarde locale des bases.
Serveur IBMx3550	→ Plateforme Windows server 2008 R2. → Processeurs Intel Xeon 4 cœurs. → 8 Go RAM. → 900 Go HDD	→ VMware Hypervisor 4.1 → Images de tests
Serveur IBMx3550	→ Plateforme Windows server 2008 R2. → Processeurs intel Xeon 4 cœur(s). → 16 Go RAM. → 500 Go HDD	→ VMware Hypervisor 4.1: → Image système «Windows 2003 R2», pour sage paie. → Image système « Windows 2003 R2», pour la messagerie interne.
Serveur HPProLiantDL380 G6	→ 02 Processeurs. → 24 Go RAM. → HDD 1To (Raid 0-1)	→ VMware Hypervisor 4.1 → En attente de migration
Firewall Pfsense	→ Versions 1.2 → 04 Interfaces réseaux	→ Passerelle par default. → Segment WAN → Segment LAN → Segment DMZ → Segment LAN Privé
Routeur Cisco 1921	→ Ligne Spécialisée (LS) Fibre Optique. → Débit:08Mbits/s	
13Bornes WIFI	→ DLink → Syslink → Tplink	→ 02 Gérance & DFC. → 01 Commerciale. → 01 Administration. → 01 Administration Industrielle. → 08 dans les villas des propriétaires.

Tableau III.4 : Caractéristiques de l'équipement informatique sur le site central de « ifri ».

III.4.2. Ressources logicielles

Comme ressources logiciels on peut citer :

- Les systèmes exploitations: (Windows 2008 server R2, Windows 2003 server R2, Windows XP professionnel sp3 et Windows 7 professionnel sp1).
- Antivirus Kaspersky Lab version entreprise.
- Le pack Ms Office2007 et 2010.

III.5. Etude et critique de l'existant

III.5.1. Architecture existante

L'architecture LAN existante du site principal de la SARL « ifri » est illustré dans la figure III.2 :

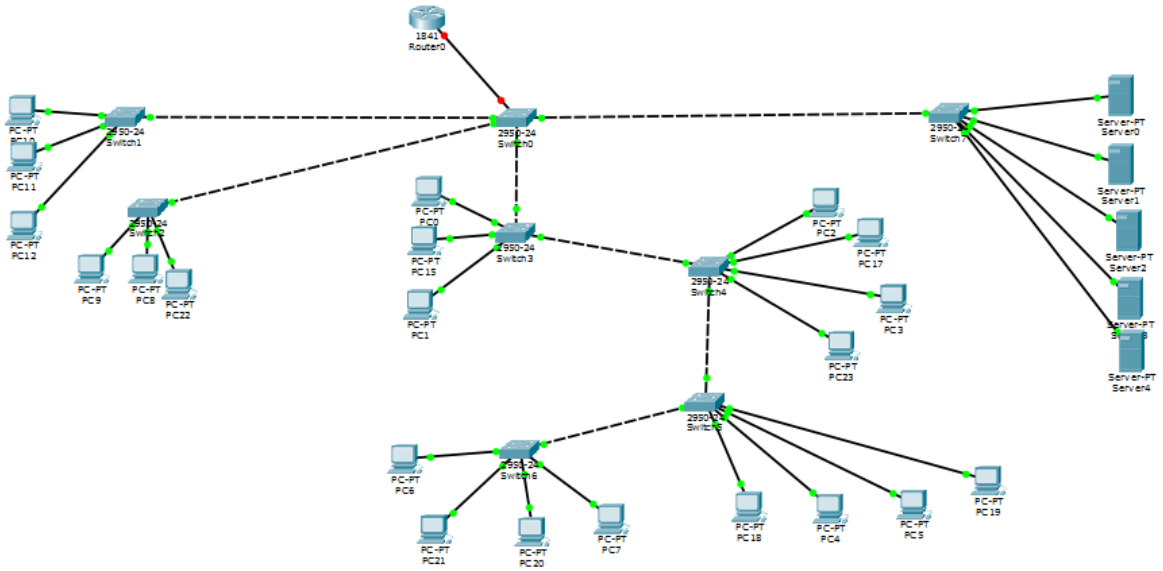

Figure III.2 : Architecture existante.

III.5.2. Critique de l'existant

L'étude du réseau de l'entreprise nous a permis de déterminer un nombre important de contraintes pouvant réduire ses performances, voir sa dégradation, nous avons :

- L'absence de segmentation du réseau en sous-réseau favorise l'action des utilisateurs pirates et les collisions importantes dans le réseau.
- L'absence de la redondance des équipements et liaisons.
- Le réseau est mal organisé, en effet, on peut trouver jusqu'à 5 Switchs d'accès en série.
- L'absence des Switchs de distribution dans le réseau et la présence unique des Switchs d'accès.
- Un volume accru du trafic généré par chaque utilisateur.
- Les application toujours plus complexes et fichiers plus volumineu**x.**
- Le trafic web et flux de messagerie important.

Tous ces phénomènes entrainent la dégradation du réseau et sont facteurs d'insécurité. Ainsi quelle solution pouvons-nous apporter pour pallier ces insuffisances ? L'étude de notre thème consistera donc à faire des propositions concrètes par rapport aux problèmes ci-dessus énumérés.

III.6. Problématique

De nombreuses insuffisances ont été découvertes lors de l'étude du réseau de la Sarl -ifri, qui nous a permis également de définir un nombre important de contraintes pouvant réduire ses performances voir le dégrader. Ainsi on note :

Comment organiser le réseau local afin de pallier aux problèmes liés à la croissance de l'environnement réseau ? Et comment pouvons-nous réduire les domaines de Broadcast et lier aux problèmes affectant ses performances en termes d'optimisation de la bande passante et d'amélioration de la sécurité ?

III.7. Solutions proposées

L'objectif de notre projet est de proposer des solutions afin de renforcer la politique de sécurité du réseau local et une meilleure gestion de ce dernier, pour cela :

Nous devons proposer une nouvelle architecture, organiser notre réseau local d'une bonne manière et adopter un bon modèle de segmentation VLANs pour une bonne organisation qui permettra une optimisation du réseau en termes d'efficacité et de performance, En effet, cette solution est la meilleure et l'adéquate, en vue des avantages qu'elle offre.

Il nous faudra également insérer des listes de contrôles d'accès dans le routeur afin d'offrir une couche de sécurité supplémentaire. En effet, les ACLs sont particulièrement adaptés pour autoriser ou refuser le trafic entrant et sortant de manière sélective.

III.8 Spécification des besoins

Après l'étude critique de l'existant et afin de résoudre au mieux les différents préoccupations manifestées par le responsable informatique de la Sarl –ifri, plusieurs besoins ont été relevés, à savoir :

- Modifier l'architecture existante et mettre en œuvre une nouvelle architecture.
- Mettre en place un autre commutateur de distribution de secours en cas d'une panne le réseau reste en bon fonctionnement.
- Ajouter un commutateur de niveau 3 pour une meilleure gestion des VLANs.
- Mettre en place des points d'accès Wifi accessible que par la direction de commerce et finance, la direction générale et le service informatique.
- Segmenter le réseau câblé en plusieurs VLANs.
- Mettre en place des listes de contrôles d'accès.

Conclusion :

À travers ce chapitre, nous avons présenté l'organisme d'accueil ainsi que le service informatique de l'entreprise dans lequel nous avons effectué notre stage, cela nous a permis d'énumérer le matériel existant et de faire une étude critique sur l'architecture existante cela nous a conduit à mettre en avant une problématique bien précise ce qui nous a conduit à la proposition d'une solution de segmentation du réseau local en VLANs.

CHAPITRE IV

CONCEPTION ET SIMULATION

CHAPITRE IV

CONCEPTION ET SIMULATION

Partie I : Conception de l'architecture

Introduction

Après avoir bien étudié les solutions proposées du coté théorique, vient le tour de la conception de l'architecture du modèle type. Cette partie consiste à organiser le réseau LAN sur les différents plans (nommage, adressage et routage) et déployer les protocoles nécessaires.

IV.1.1. Présentation générale du modèle type

Notre modèle type se compose d'un routeur, un modem-routeur et un Switch-cœur, avec des Switchs d'accès.

Pour assurer la disponibilité et la continuité de fonctions, le routeur est lié avec le Switch- cœur et ce dernier avec tous les Switch d'accès.

Nous allons également mettre en place un serveur DHCP pour une affectation dynamique d'adresses IP, ainsi que des points d'accès Wifi.

IV.1.2. Présentation des équipements

Les équipements réseau utilisés sont présentés dans le tableau suivant:

Équipements de modèle type	Nombre	Type et marque de Switch
Routeur	01	Cisco ISR 1841
Switch Cœur	01	Cisco Catalyst 3560
Switch Distribution	02	Cisco Catalyst 2950
Switch d'Accès	05	Cisco Catalyst 2950

Tableau IV. 1 : Liste des équipements utilisés.

IV.1.3. Nomination des équipements

Le plan de nommage consiste à attribuer des noms bien particuliers pour chaque équipement afin de faciliter la conception de l'architecture, l'administration et la gestion du réseau local. Le tableau ci-dessous indique les noms des différents équipements :

Couche Cœur	Couche Distribution	Couche Accès	Serveur	Point D'accès	PCs
Routeur	SW-Dis1 SW-Dis2	SW-Acces-A SW-Acces-B SW-Acces-C SW-Acces-D SW-Serveurs	SRV-DHCP SRV-Paie SRV-Applicatif SRV-Fichiers SRV-Connexion	Acc-Pt-DG Acc-Pt-DFC Acc-Pt-IT	DIRECTEUR SECRETARIAT DIRECTEUR-RH CHEF-IT ING-IT Laptop0 Laptop1 Laptop2 PC0,PC1,…,PC19

Tableau IV.2 : Nomination des équipements du réseau local.

IV.1.4 Nomination des VLANs

Les différents VLANs à implimenter seront nommés comme suit :

Nom de VLAN	ID VLAN	Adresse de sous réseau	Masque de sous réseau
DG	VLAN 10	10.10.10.0	255.255.255.0
DFC	VLAN 20	10.10.20.0	255.255.255.0
DRH	VLAN 30	10.10.30.0	255.255.255.0
DAppro	VLAN 40	10.10.40.0	255.255.255.0
Commerciale	VLAN 50	10.10.50.0	255.255.255.0
Admin-Ind	VLAN 60	10.10.60.0	255.255.255.0
Logistique	VLAN 70	10.10.70.0	255.255.255.0
Qualite	VLAN 80	10.10.80.0	255.255.255.0
DHCP	VLAN 90	10.10.90.0	255.255.255.0
IT	VLAN 100	10.10.100.0	255.255.255.0
Paie	VLAN110	10.10.110.0	255.255.255.0
Connex	VLAN120	10.10.120.0	255.255.255.0

Tableau IV. 3 : Nomination des VLANs.

IV.1.5. Désignations des interfaces :

Chaque équipement s'interconnecte à un autre équipement via une interface précise. Le tableau IV.4 désignera la liste des interfaces qui participeront à l'interconnexion des différents équipements :

Equipement 1	Equipement 2	Interface Equipement 1	Interface Equipement 2
SW-Cœur	Routeur	Fa0/22	Fa0/0
	SW-Dis1	Fa0/23	
	SW-Dis2	Fa0/24	
	SW-Serveurs	Fa0/21	
SW-Dis1	SW-Acces-A	Fa0/21	
	SW-Acces-B	Fa0/22	
	SW-Acces-C	Fa0/23	
	SW-Acces-D	Fa0/20	
	SW-Cœur	Fa0/24	
SW-Dis2	SW-Acces-A	Fa0/21	
	SW-Acces-B	Fa0/22	
	SW-Acces-C	Fa0/23	
	SW-Acces-D	Fa0/20	
	SW-Cœur	Fa0/24	

SW-Acces-A	SW-Dis1	Fa0/24	
	SW-Dis2	Fa0/23	
	Acc-Pt-DG	Fa0/7	Port 0
	Acc-Pt-DFC	Fa0/10	Port 0
	DIRECTEUR	Fa0/3	
	SECRETARIAT	Fa0/2	
	DIRECTEUR-RH	Fa0/9	
	PC0	Fa0/5	
	PC1	Fa0/6	
	PC2	Fa0/1	
	PC3	Fa0/8	
SW-Acces-B	SW-Dis1	Fa0/24	
	SW-Dis2	Fa0/23	
	PC4	Fa0/1	
	PC5	Fa0/2	
	PC6	Fa0/3	
	PC7	Fa0/4	
	PC8	Fa0/5	
	PC9	Fa0/6	
SW-Acces-C	SW-Dis1	Fa0/24	
	SW-Dis2	Fa0/23	
	PC10	Fa0/1	
	PC11	Fa0/2	
	PC12	Fa0/3	
	PC13	Fa0/4	
	PC14	Fa0/5	
	PC15	Fa0/6	
SW-Acces-D	SW-Dis1	Fa0/23	
	SW-Dis2	Fa0/24	
	Acc-Pt-IT	Fa0/6	Port 0
	PC16	Fa0/1	
	PC17	Fa0/2	
	PC18	Fa0/3	
	PC19	Fa0/7	
	Chef-IT	Fa0/5	
	ING-IT	Fa0/4	
SW-Serveurs	SW-Cœur	Fa0/24	
	SRV-DHCP	Fa0/2	
	SRV-Fichiers	Fa0/3	
	SRV-Applicatif	Fa0/4	
	SRV-Paie	Fa0/5	
	SRV-Connexion	Fa0/6	

Tableau IV. 4 : Liste des interfaces.

IV.1.6. Protocole VTP

Le protocole VTP (VLAN Trunking Protocol) est un protocole de la couche 2 propriétaire à Cisco, conçu pour pallier aux problèmes opérationnels au sein des réseaux commutés comportant des VLANs.

VTP règle le problème de la configuration manuelle des VLANs. En effet, si le réseau à une taille considérable, la déclaration de tous les VLANs crées dans tous les commutateurs sera vraiment très difficile à réaliser, et cela est pareil lors de l'ajout d'un nouveau VLAN ou lors de la modification. Donc, la mise à jour des VLANs d'une façon manuelle est très difficile. Le protocole VTP, autorise les changements centralisés (ajout, suppression et modification) qui seront communiqués par les VTP-SEVER à tous les autres commutateurs VTP-CLIENT du réseau ou VTP-TRASPARENT. VTP permet ainsi d'éviter toute incohérence de configuration des VLANs.

Dans notre cas, c'est le switch coeur (SW-Coeur) qui est configuré comme serveur VTP (SERVER-VTP), par contre tout le reste des commutateurs seront considérés comme client VTP (CLIENT-VTP), donc, toutes les modifications seront transmises à partir du SERVER-VTP vers tous les CLIENT-VTP.

Le tableau IV.5 désigne le SERVER-VTP et les CLIENT-VTP :

Equipement	Nom Domaine	Mode
SW-Cœur	ifri	SERVER
SW-Dis1	ifri	CLIENT
SW-Dis2	ifri	CLIENT
SW-Serveurs	ifri	CLIENT
SW-Acces-A	ifri	CLIENT
SW-Acces-B	ifri	CLIENT
SW-Acces-C	ifri	CLIENT
SW-Acces-D	ifri	CLIENT

Tableau IV.5 : Désignation VTP.

Partie II : Simulation

IV.2.1.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, 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 découvrir le fonctionnement des différents éléments constituant un réseau informatique [20].

La Figure IV.1 est une image montrant l'interface principale du simulateur Cisco Packet Tracer :

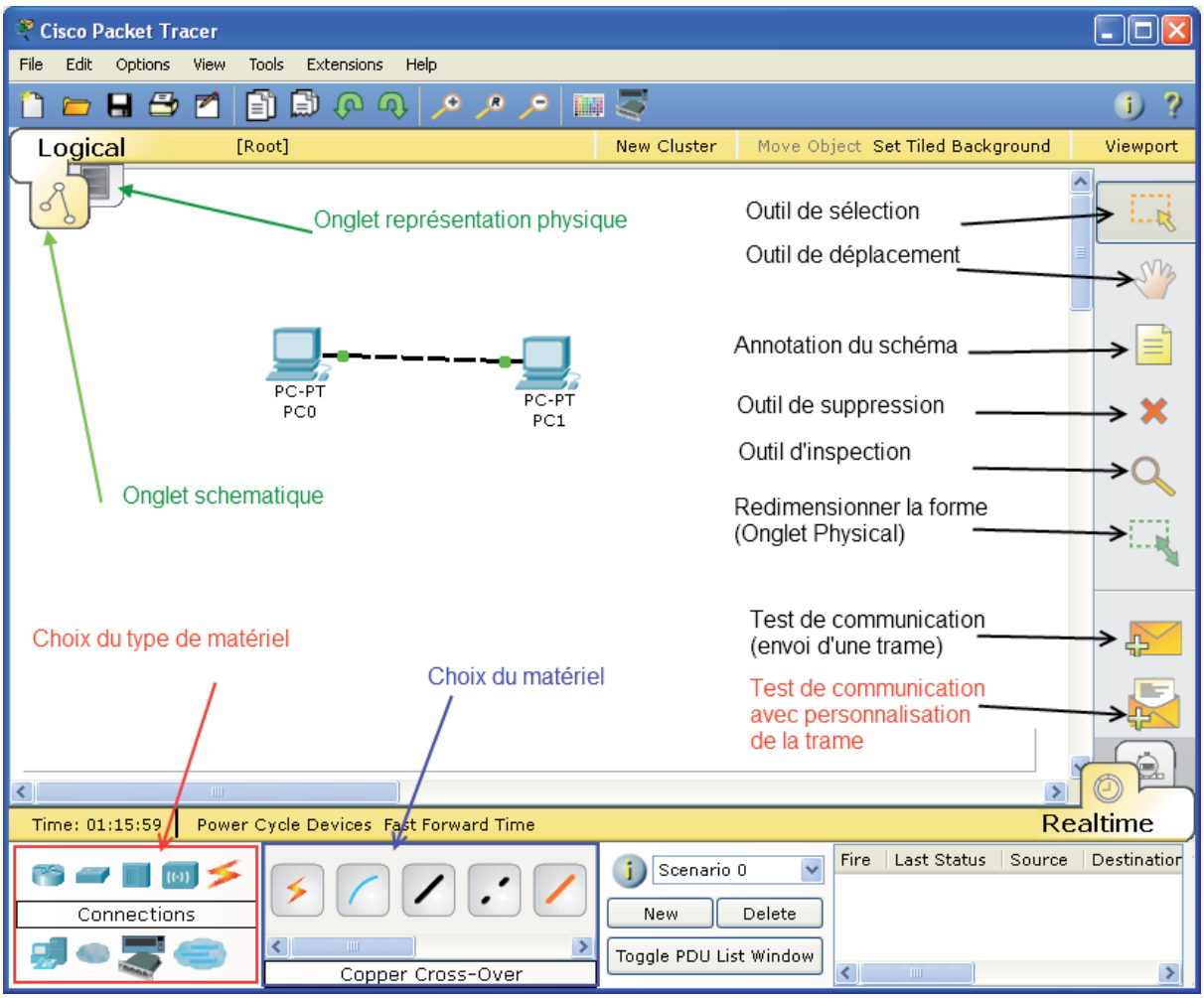

Figure IV. 1 : L'interface de simulateur « Cisco Packet Tracer » [21].

IV.2.2. 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 langage de commandes, c'est-à-dire qu'à partir des commandes introduites par l'utilisateur du logiciel, que la configuration est faite [20].

La Figure IV.2 est l'interface CLI du Packet Tracer:

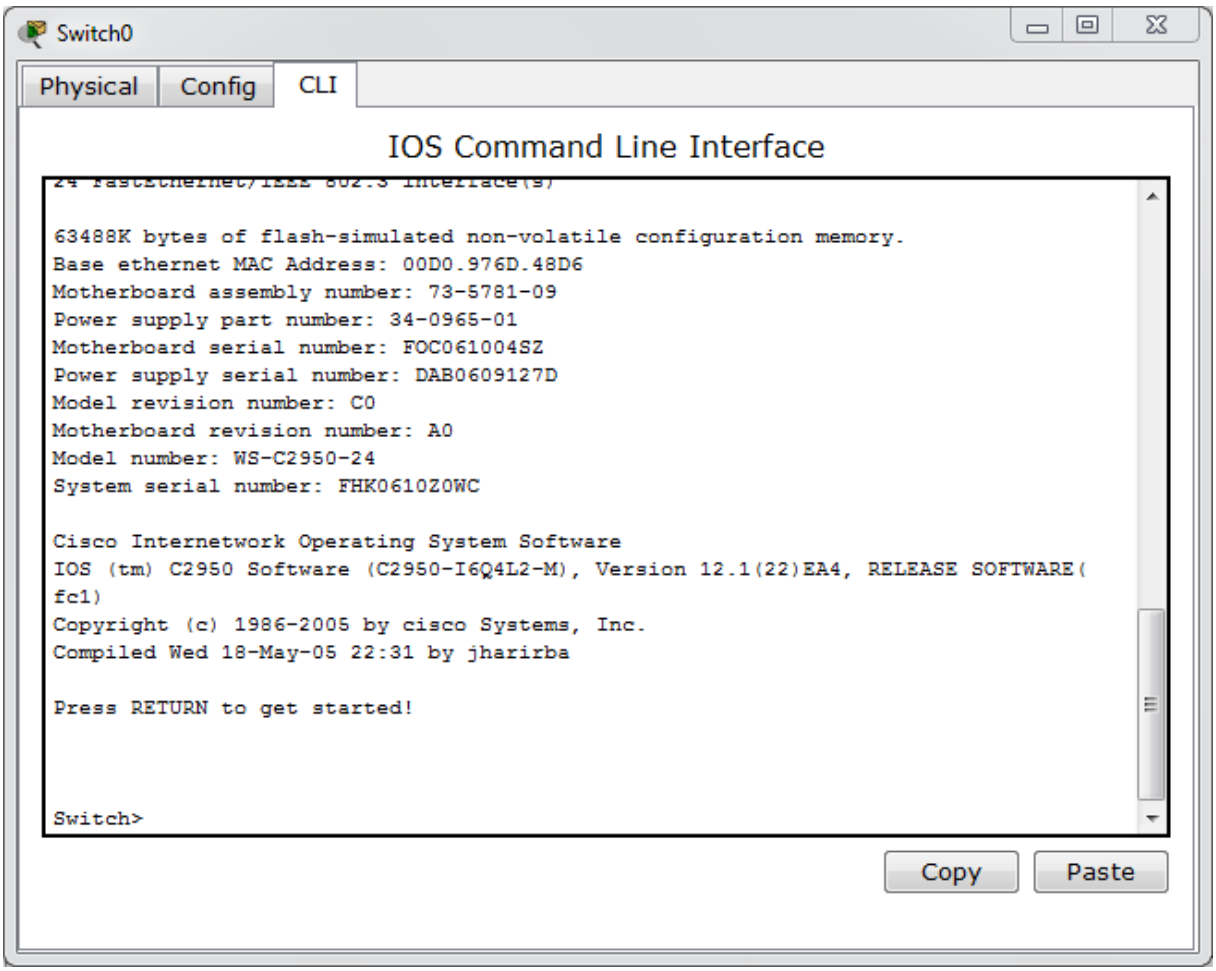

Figure IV. 2 : Interface CLI.

IV.2.3. Les différents VLANs utilisés

Les VLANs à implémenter sont :

ID_VLAN	Nom_VLAN
DG	VLAN 10
DFC	VLAN 20
DRH	VLAN 30
DAppro	VLAN 40
Commerciale	VLAN 50
Admin-Industrielle	VLAN 60
Logistique	VLAN 70
Qualite	VLAN 80
DHCP	VLAN 90
IT	VLAN 100
Paie	VLAN 110
Connexion	VLAN 120

Figure IV.3 : La liste des VLANs.

IV.2.4. Architecture de mise en œuvre

L'architecture à réaliser et à mettre en œuvre sera celle illustrée sur la figure IV.4 :

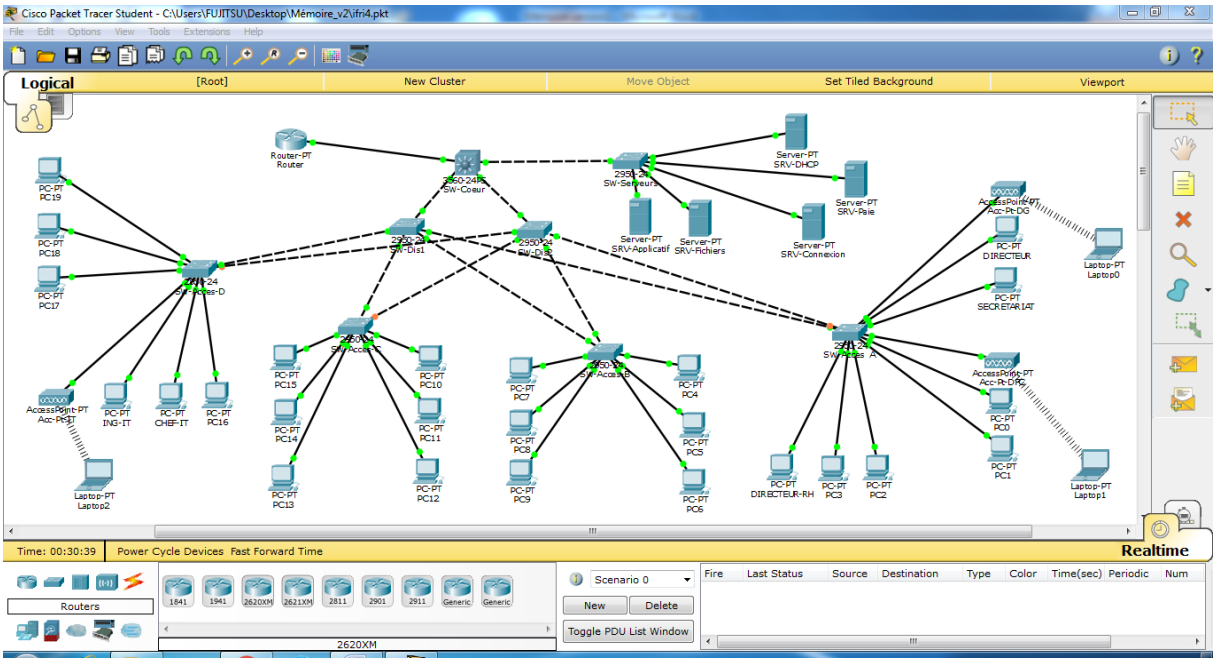

Figure IV.4 : Architecture à réaliser.

Pour la réalisation de cette architecture nous allons lancer les étapes de configuration suivante :

IV.2.5. Configuration des équipements

Une série de configuration des équipements constituants le réseau local sera réalisée en montrant un exemple de chaque configuration.

Et pour cela, nous allons suivre les étapes de configuration suivante :

- Configuration des commutateurs.
- Configuration du routeur.
- Configuration des serveurs et PCs.
- Configuration des points d'accès.
- Tests de validation des configurations.

IV.2.5.1. Configuration des commutateurs

Cette configuration contiendra un ensemble de points à configurer, en commençant d'abord, par une petite configuration des noms de chaque commutateur, ensuite configurer les différents VLANs existants, ainsi la configuration des interfaces du commutateur, en tenant compte bien sur, de l'ensemble des protocoles à implémenter, tel que VTP, Spanning-Tree et DHCP.

a. Configuration du Hostname

Cette étape consiste à donner un nom significatif à l'ensemble des équipements constituant le LAN. Par exemple, la nomination du Switch cœur.

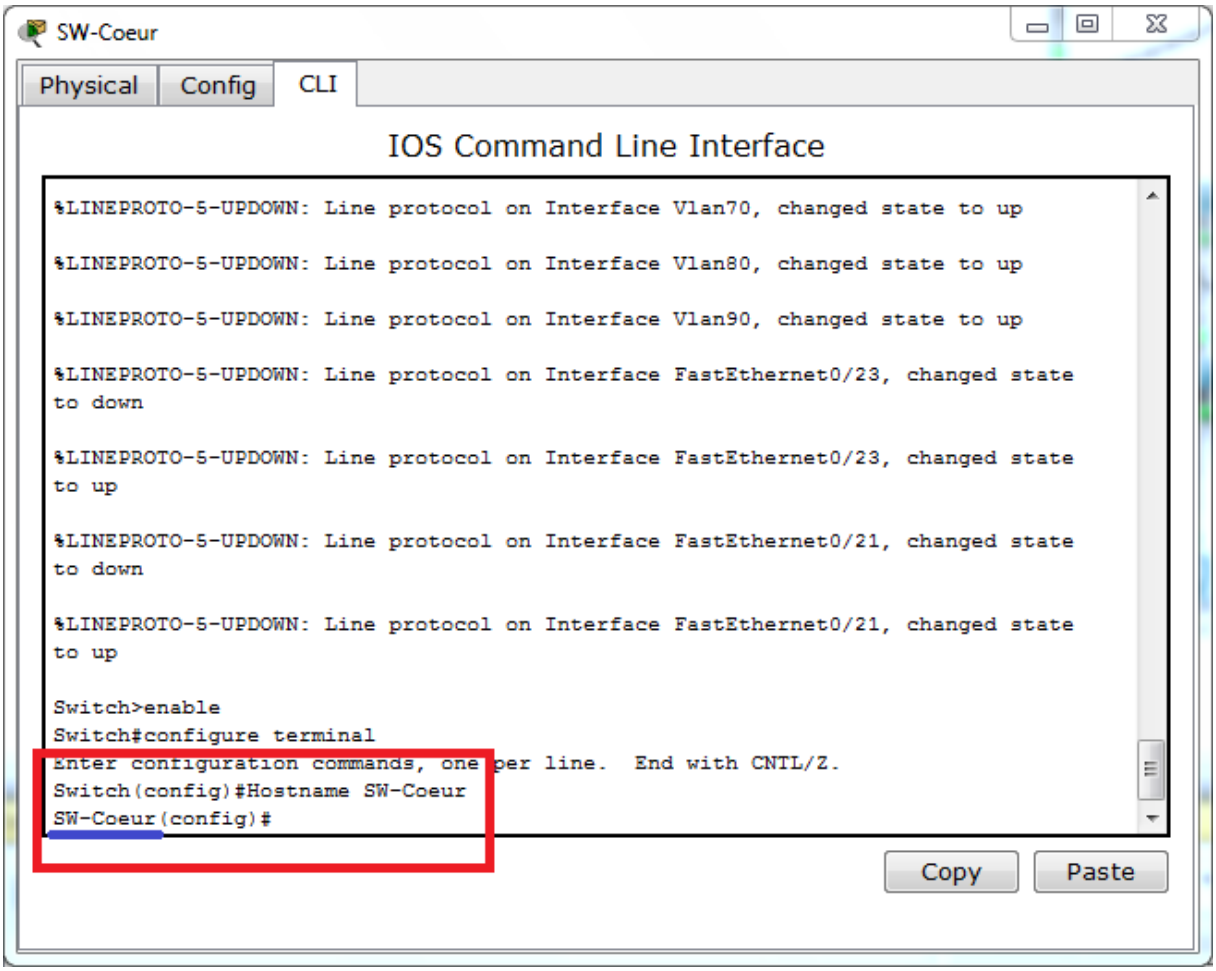

Figure IV. 5 : Nomination du Switch cœur.

b. Configuration des mots de passe

- **Sécuriser l'accès à la ligne de console**

Nous avons choisi « ifriconsole » comme mot de passe d'accès à la console, cet exemple montre les commandes de mise en place du mot de passe sur le SW-cœur.
La même chose sera faite pour tous les autres les commutateurs

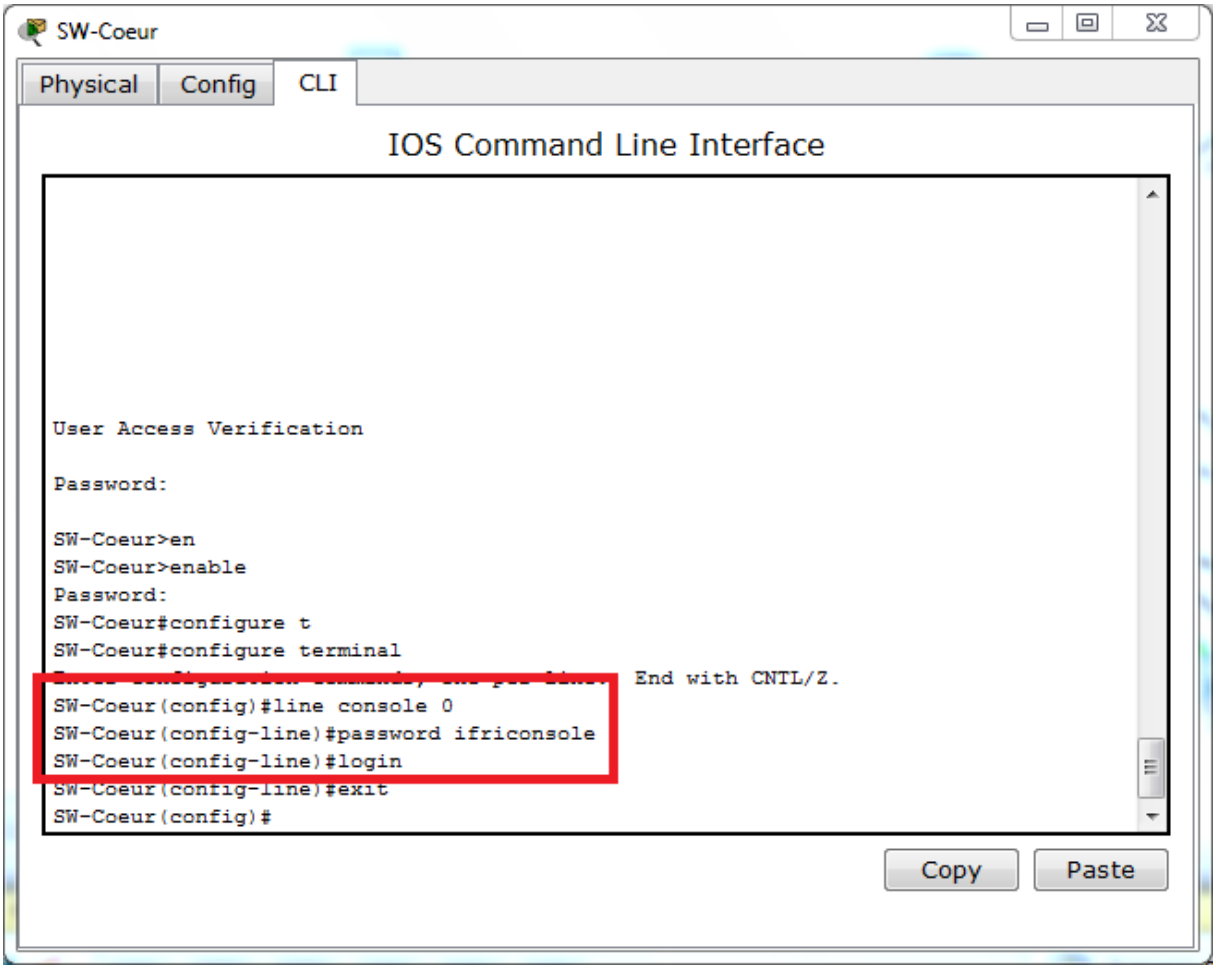

Figure IV.6 : Mot de passe console au SW-Cœur.

- **Sécuriser l'accès au mode privilégié**

Nous avons choisi le mot de passe « ifrisecret » pour sécuriser l'accès au mode privilégié.

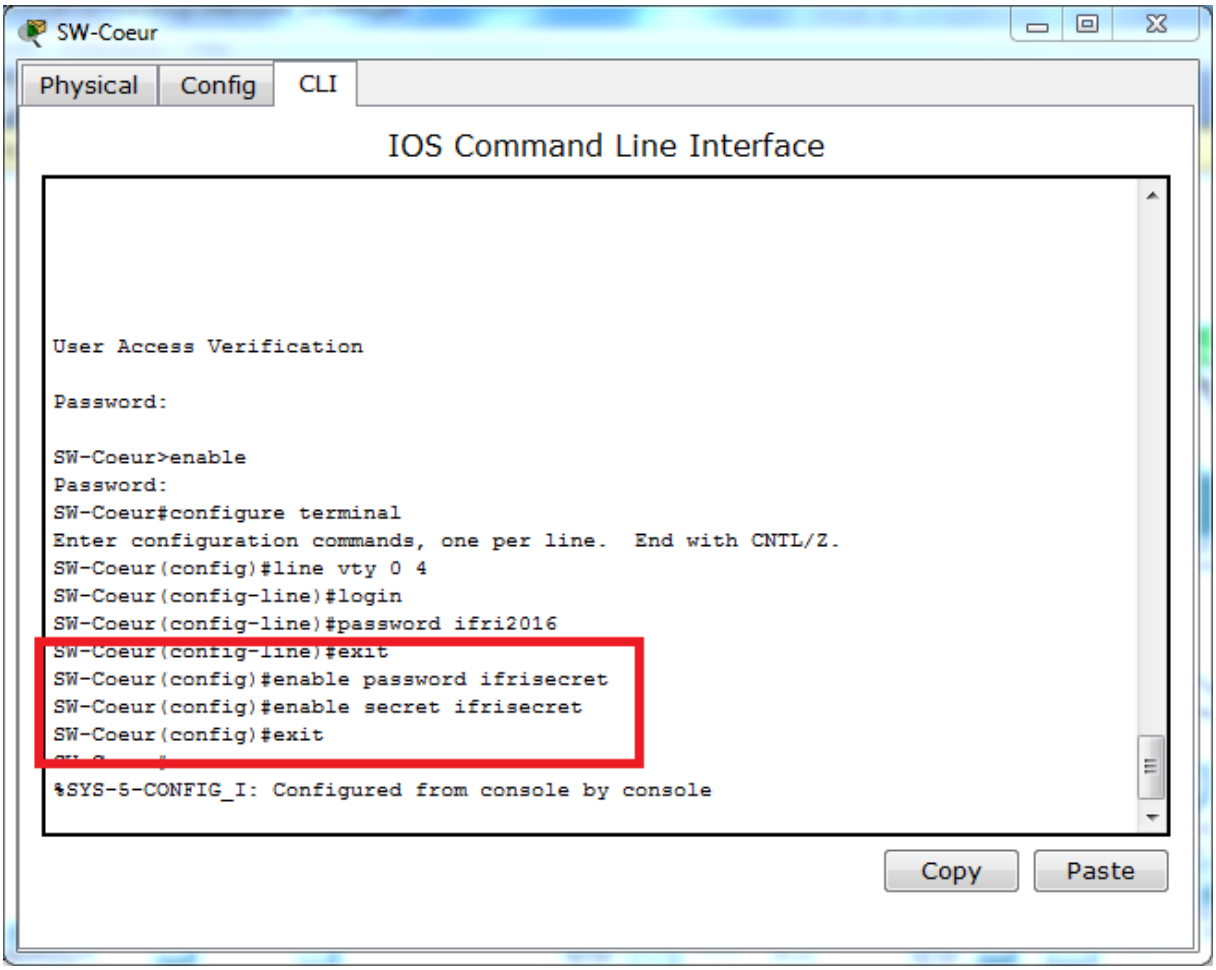

Figure IV.7 : Mot de passe pour le mode privilégié au SW-Cœur.

c. Création des VLANs

La création des VLANs est faite au niveau du Switch cœur dans le réseau local.

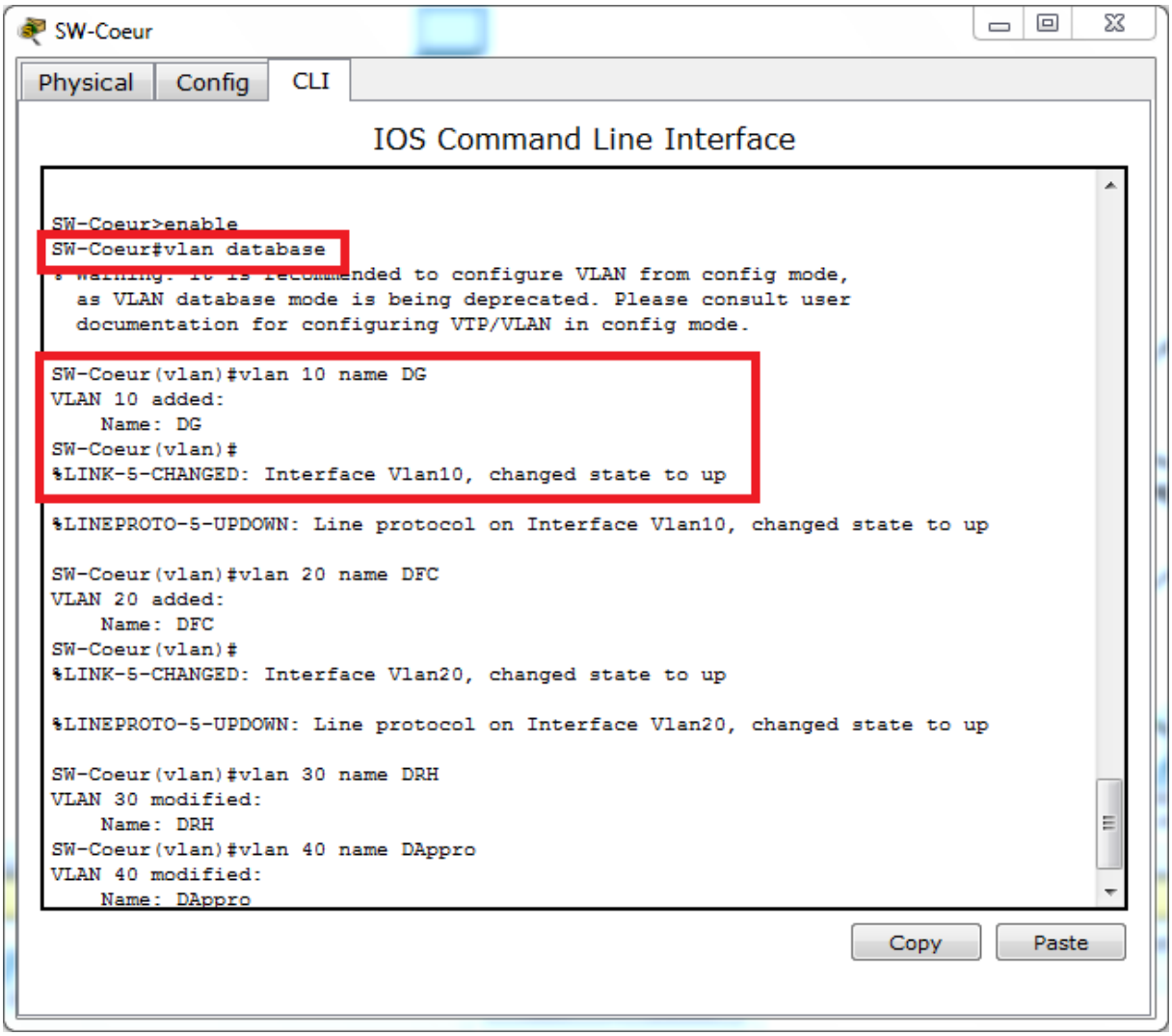

Figure IV. 8 : Création des VLANs.

d. Configuration du protocole VTP

Le Switch cœur du LAN de la SARL -ifri, sera configuré comme un Server-VTP. Donc, c'est lui qui gère l'administration de l'ensemble des VLANs. Un nom de domaine est attribué, dans le cas présent c'est « ifri » en plus d'un mot de passe du domaine qui est « ifri2016 ».

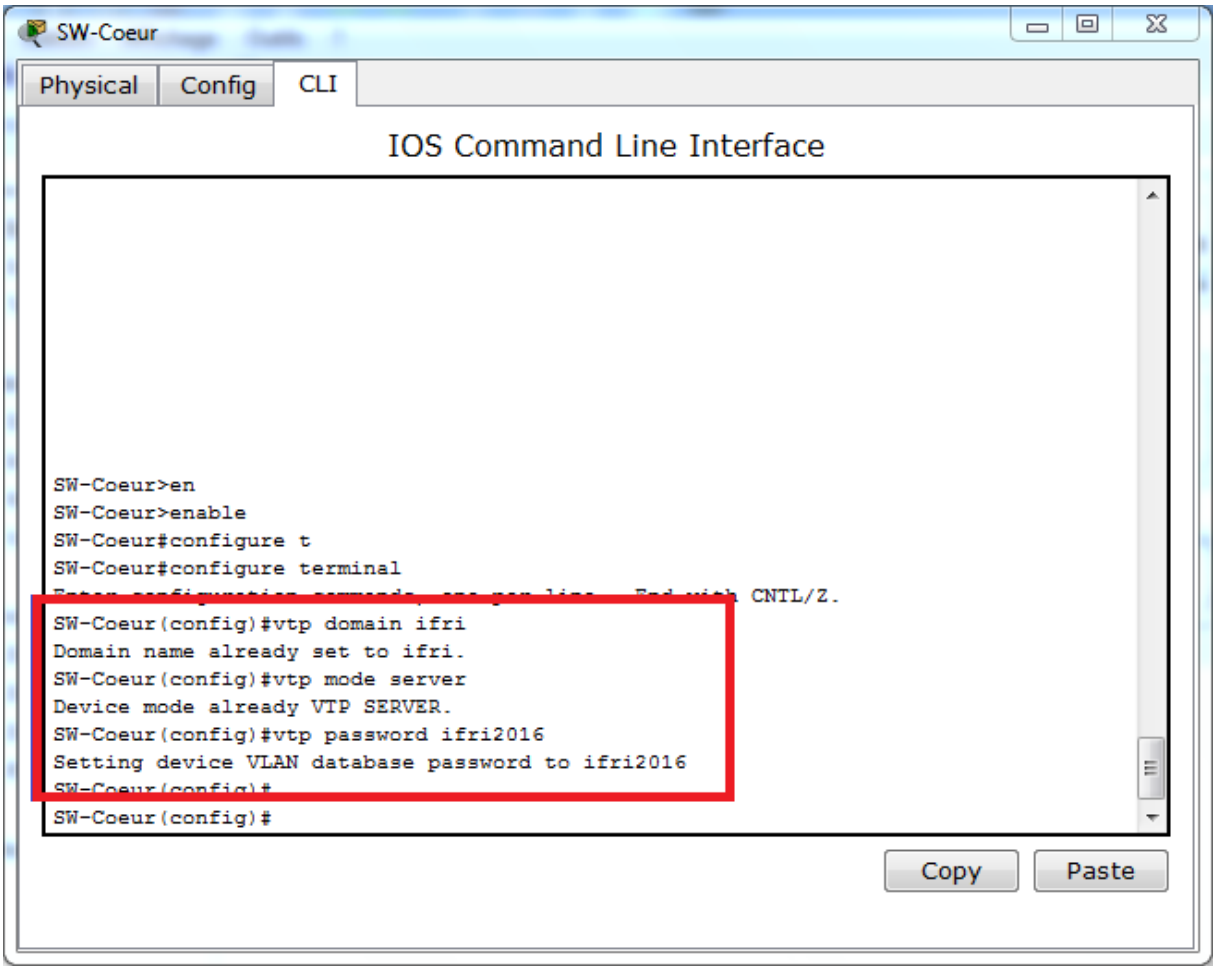

Figure IV.9 : Configuration du VTP-Server.

Par ailleurs, la configuration des Client-VTP sera au niveau de tous les commutateurs de Distribution et d'Accès du LAN.

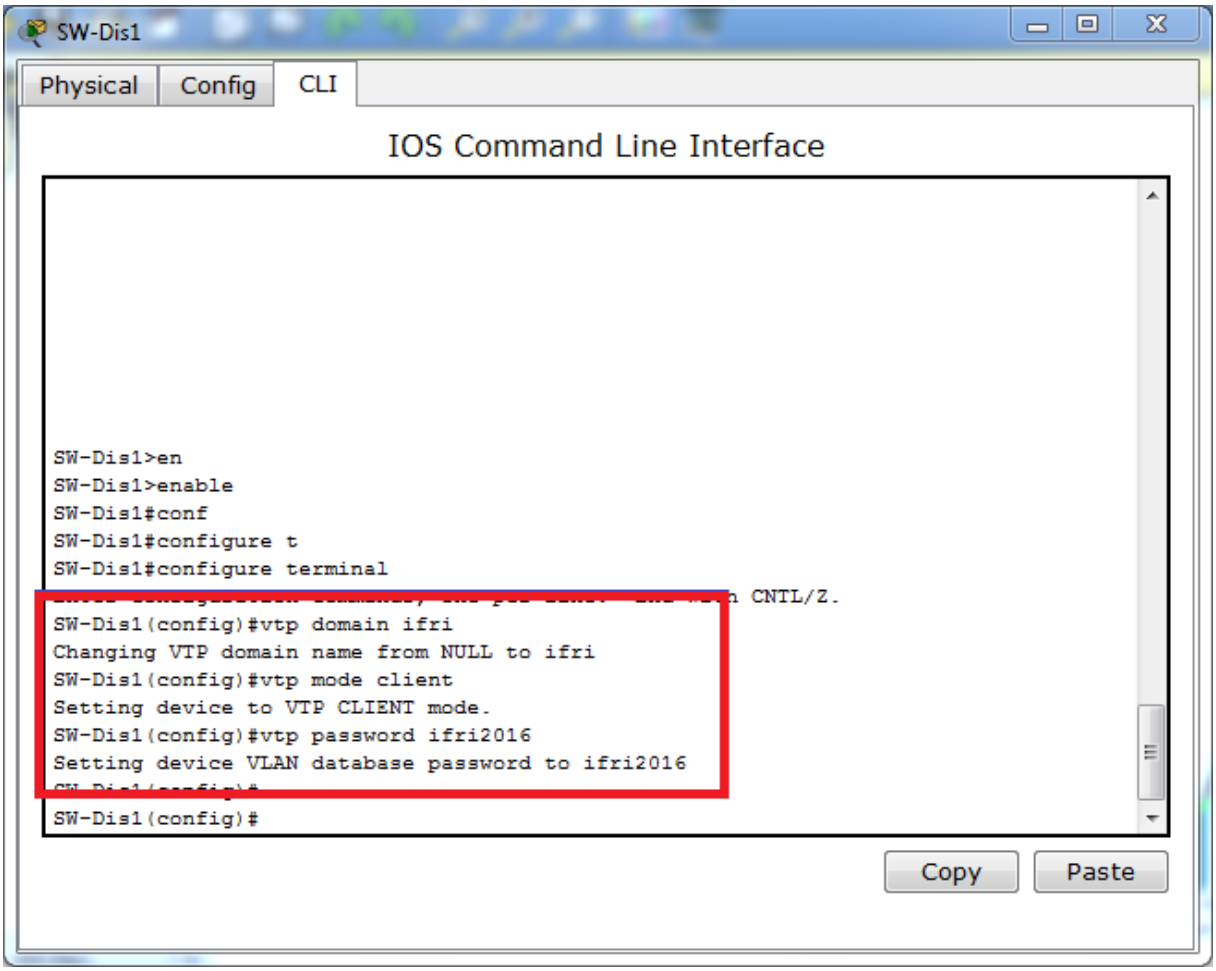

Figure IV. 10 : Configuration du VTP-Client.

Une fois que les VTP-Clients sont configurés, la configuration des VLANs effectuée sur le Switch cœur (VTP-Server) sera propagée à l'ensemble des autres commutateurs du réseau (clients), En effet, l'ensemble des VLANs vont être créés automatiquement.

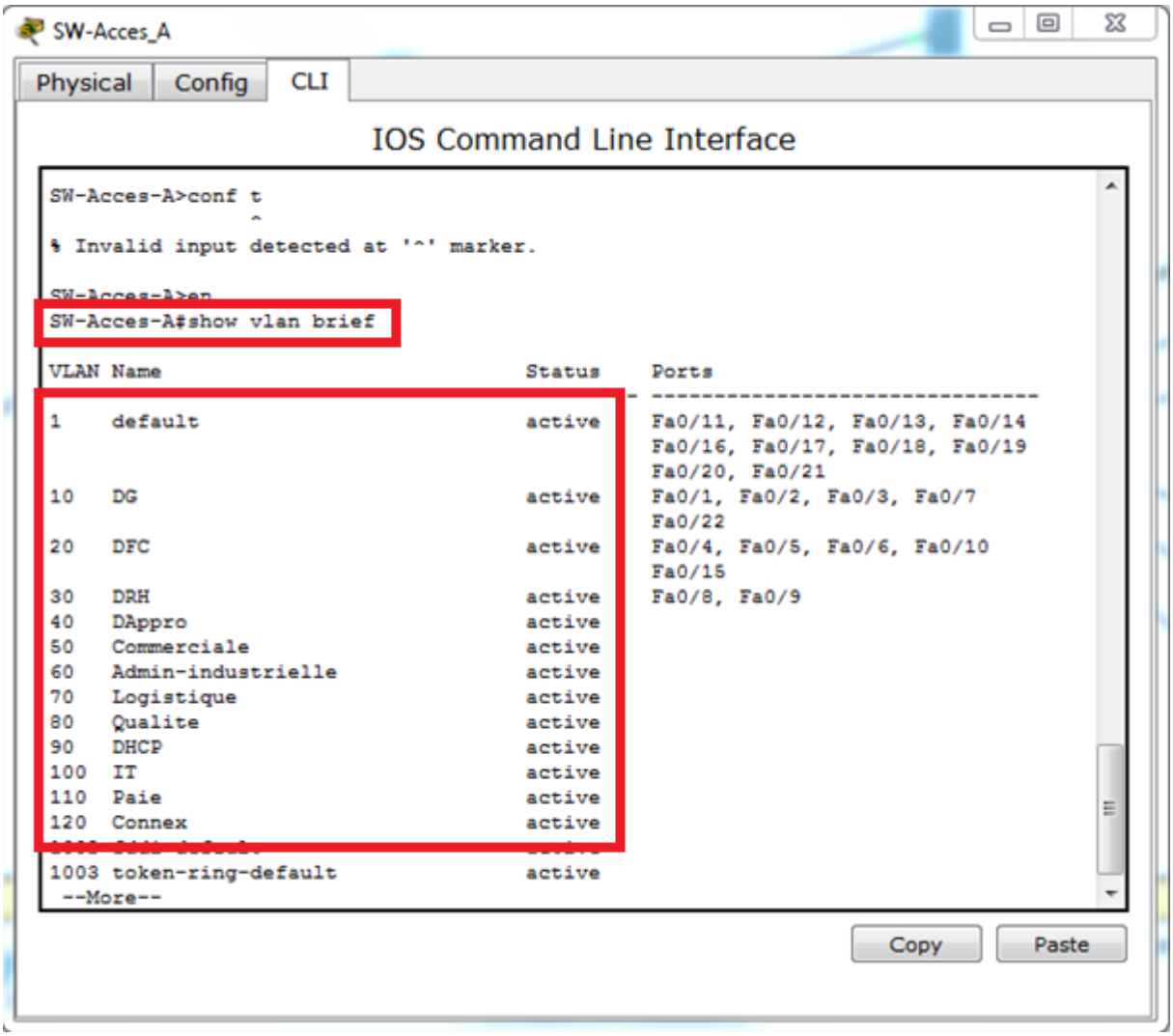

Figure IV. 11 : Les VLANs crées après la configuration du VTP-Client.

e. Configuration des VLANs

Dans cette partie de configuration, nous allons attribuer les adresses IP de passerelle pour chaque VLAN au niveau du Switch cœur, ainsi que l'adresse du serveur DHCP comme illustré dans la figure IV.12 :

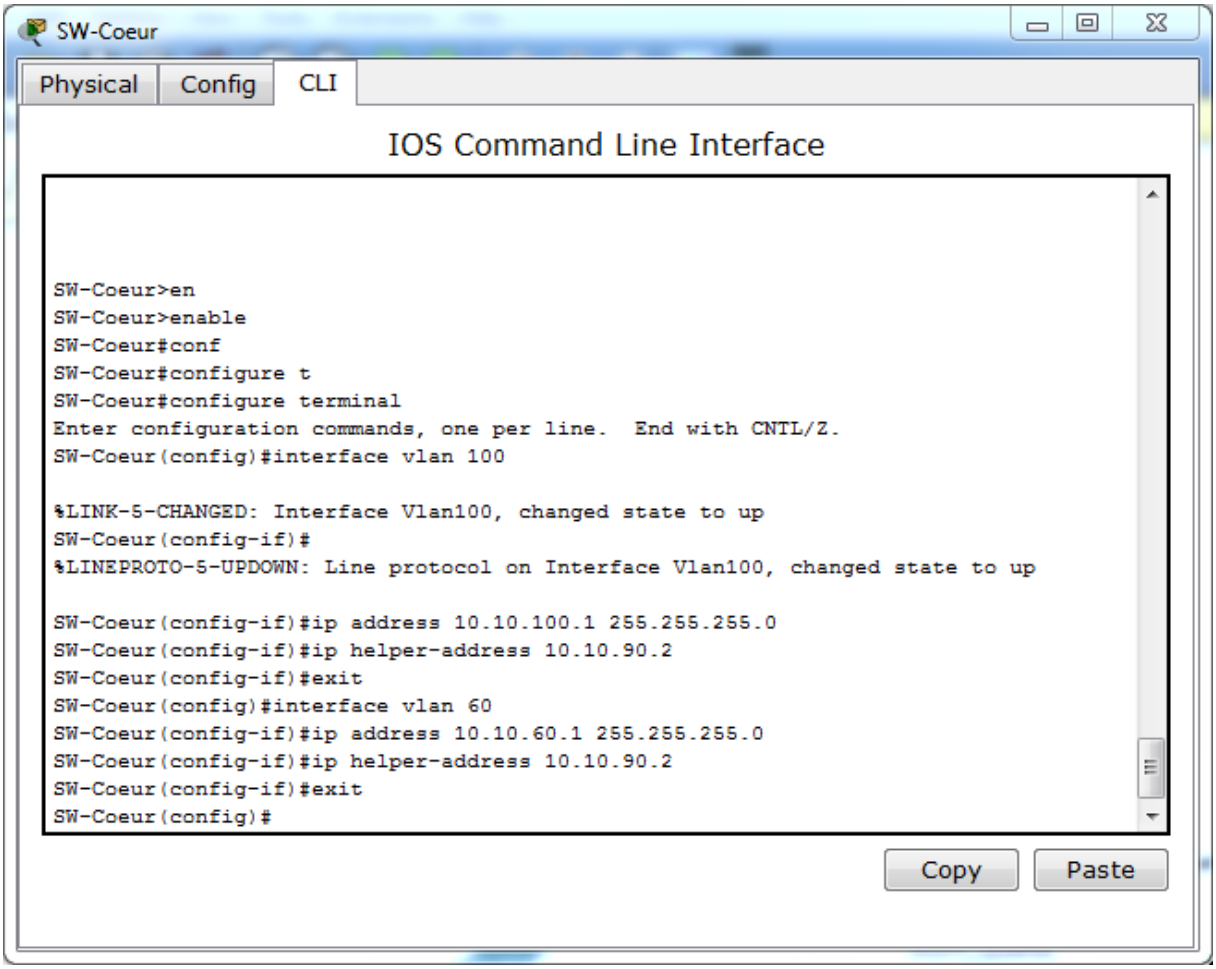

Figure IV. 12 : Attribution des adresses IP pour chaque VLAN au niveau du Switch cœur.

f. Configuration des interfaces

- **Configuration des liens Trunk**

Les interfaces des équipements d'interconnexion à configurer en mode Trunk, sont toutes les interfaces existantes entre le Switch cœur et l'ensemble des commutateurs Accès et commutateurs Distribution, ainsi celle du Switch cœur avec le routeur.

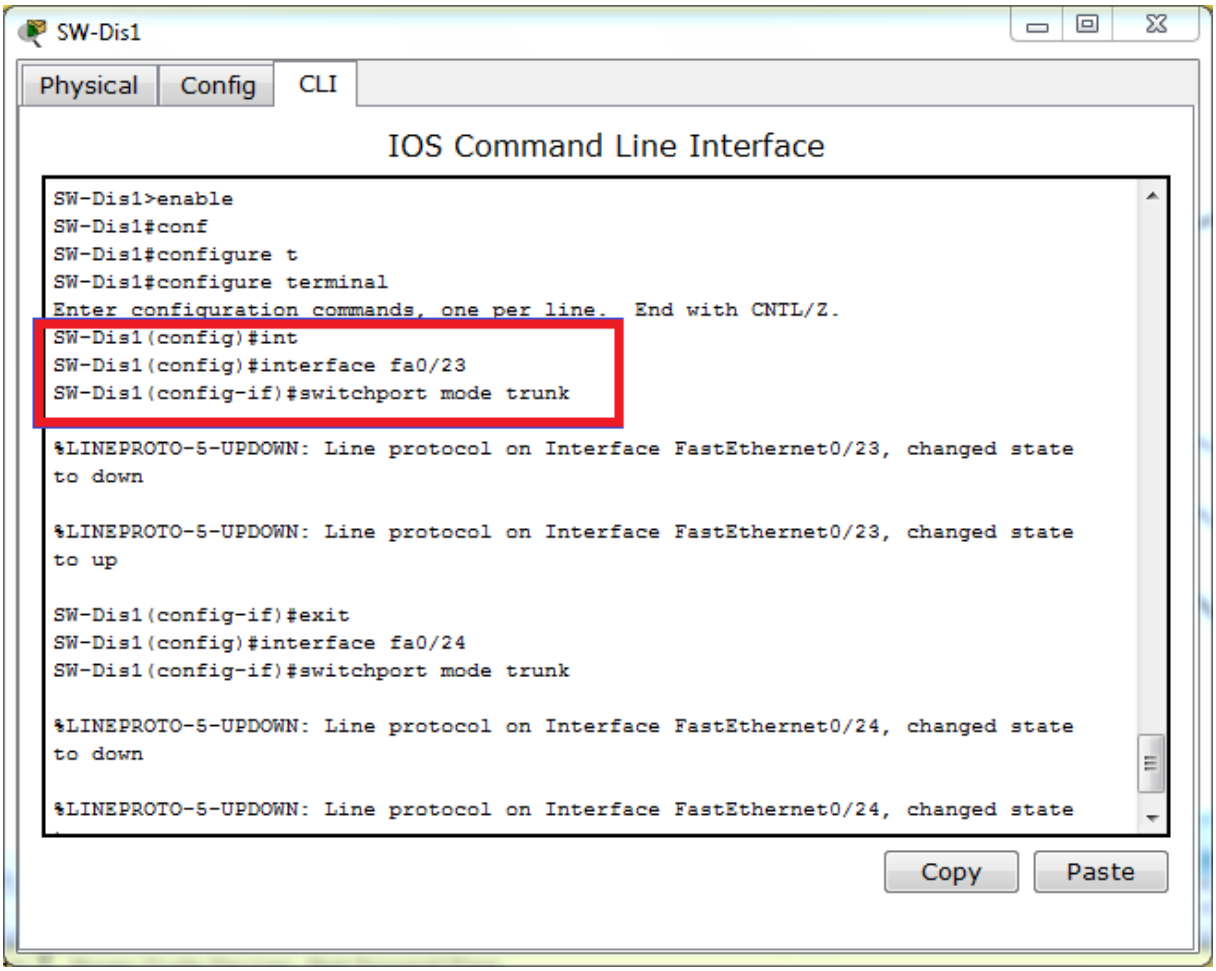

Figure IV.13 : Configuration des liens Trunk.

- **Attribution des ports des commutateurs aux VLANS**

C'est au niveau de chaque commutateur Accès, que les ports vont être assignés aux différents VLANs existants. En effet, chaque port d'un commutateur appartiendra à un VLAN donné.

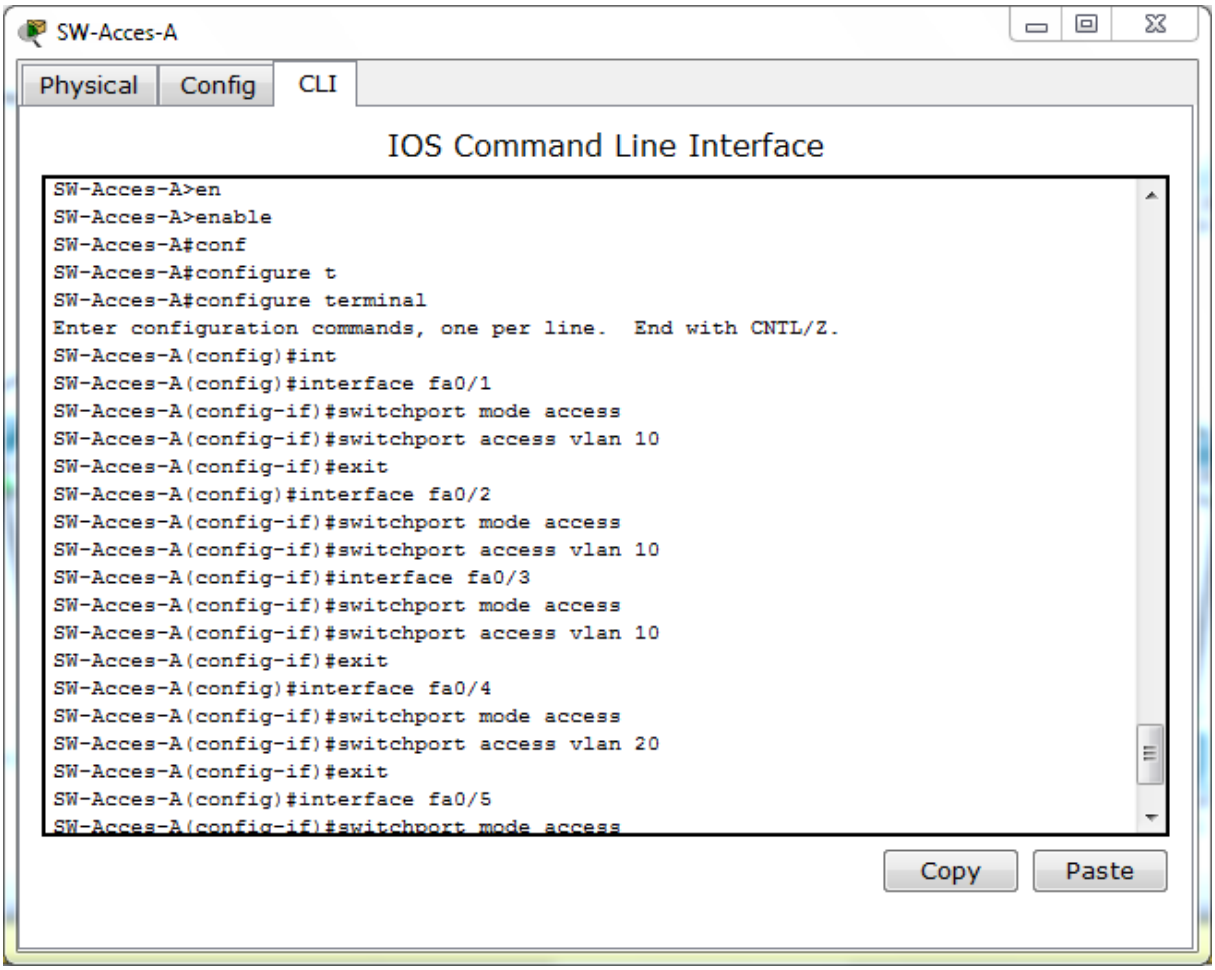

Figure IV. 14 : Attribution des ports aux VLANs.

g. Configuration de Spanning-Tree

Maintenant nous allons configurer le protocole Spanning-Tree pour définir le Switch cœur en tant que Switch racine.

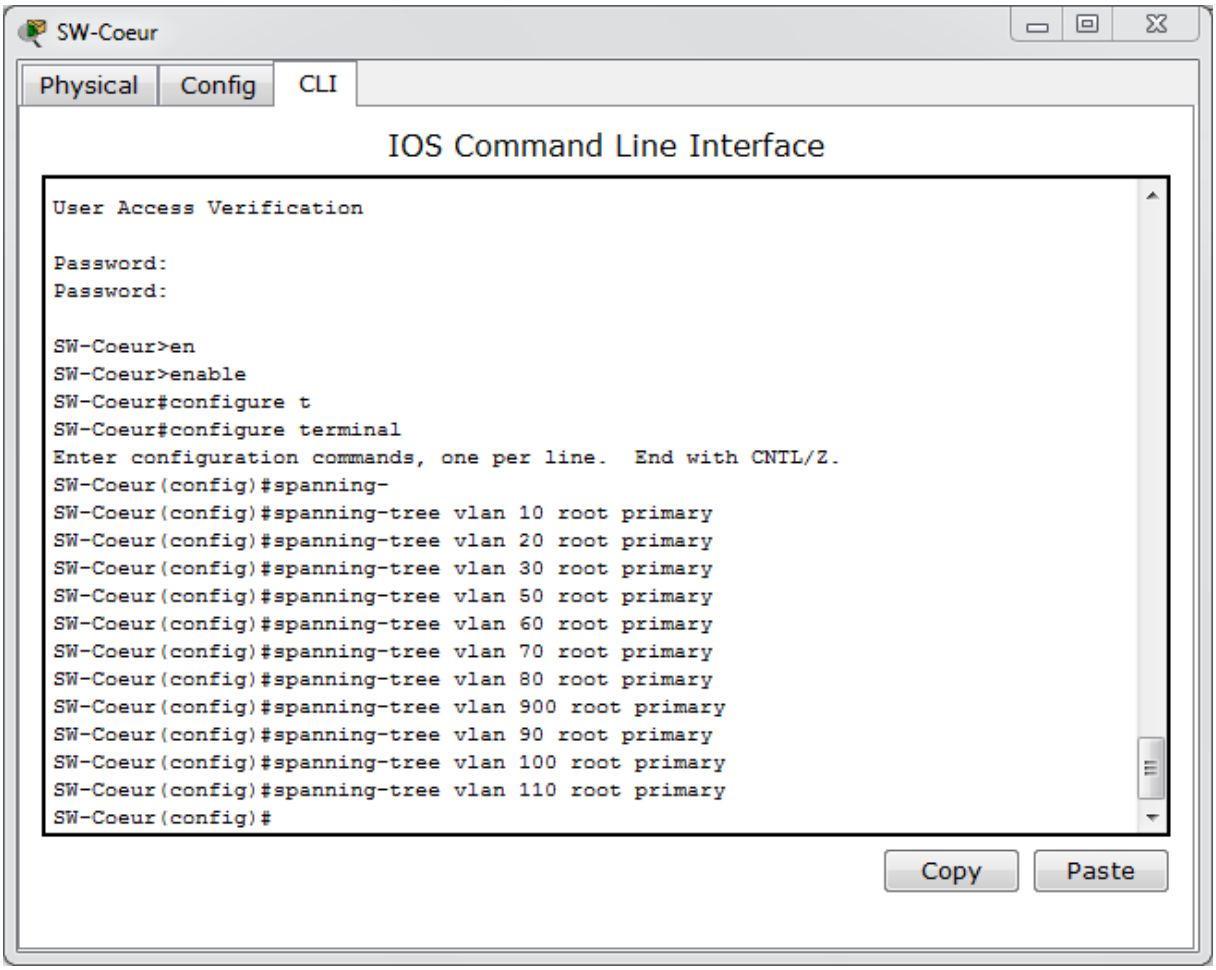

Figure IV. 15 : Configuration de Spanning-Tree.

h. Insertion des ACLs

Nous allons maintenant utiliser les listes des contrôles d'accès afin de limiter la communication entre certains VLANs, nous avons pris comme exemple le VLAN 110 qui est le serveur paie (SRV-Paie) auquel nous avons autorisé la communication qu'avec le VLAN 30 (DRH) et le VLAN 100 (IT), et bloqué la communication avec les autres VLANs comme le démontre la figure IV.16 :

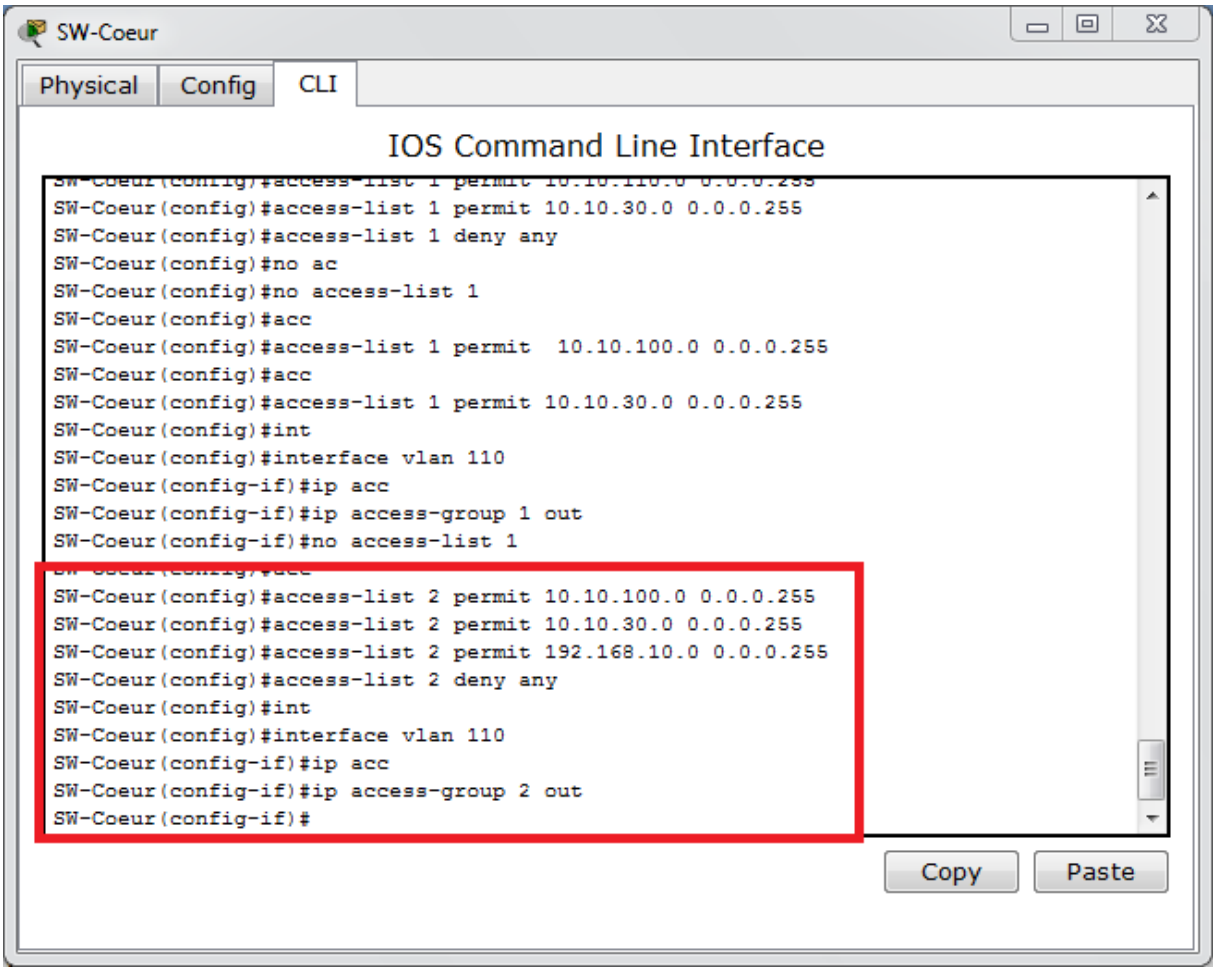

Figure IV. 16 : Configuration des ACLs au niveau du Switch cœur.

i. Configuration de routage :

- **Configuration de routage RIP**

Nous allons à présent configurer le routage RIP au niveau du Switch cœur, pour cela nous allons commencer par attribuer une adresse IP à l'interface FastEthernet0/1 laquelle est directement liée au routeur.

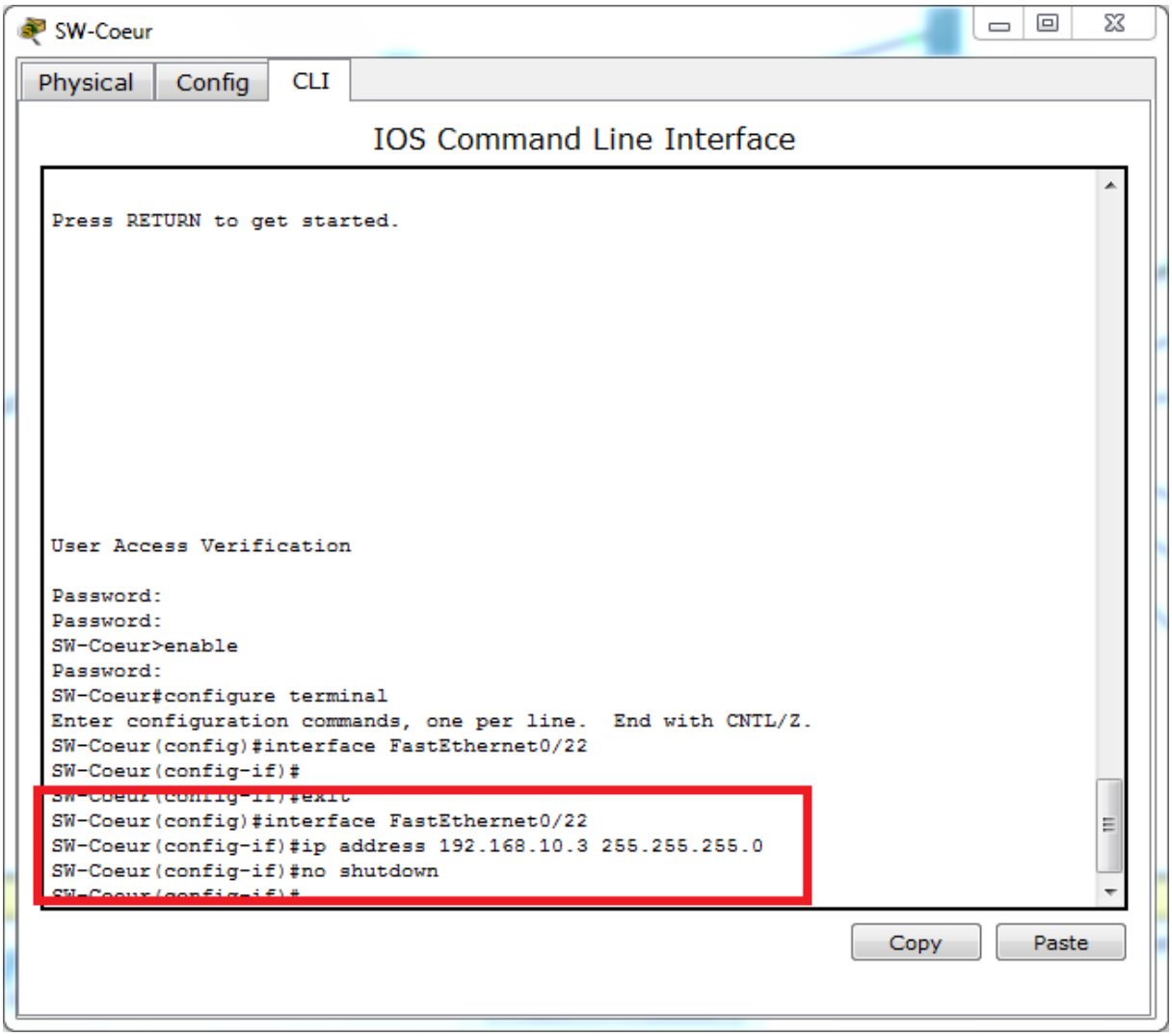

Figure IV.17 : Attribution d'adresse IP à l'interface liée au routeur.

Ensuite, Le routage qui consiste à déclarer au niveau du Switch cœur, les réseaux qui lui y sont directement connectés, comme le montre la figure IV.18 :

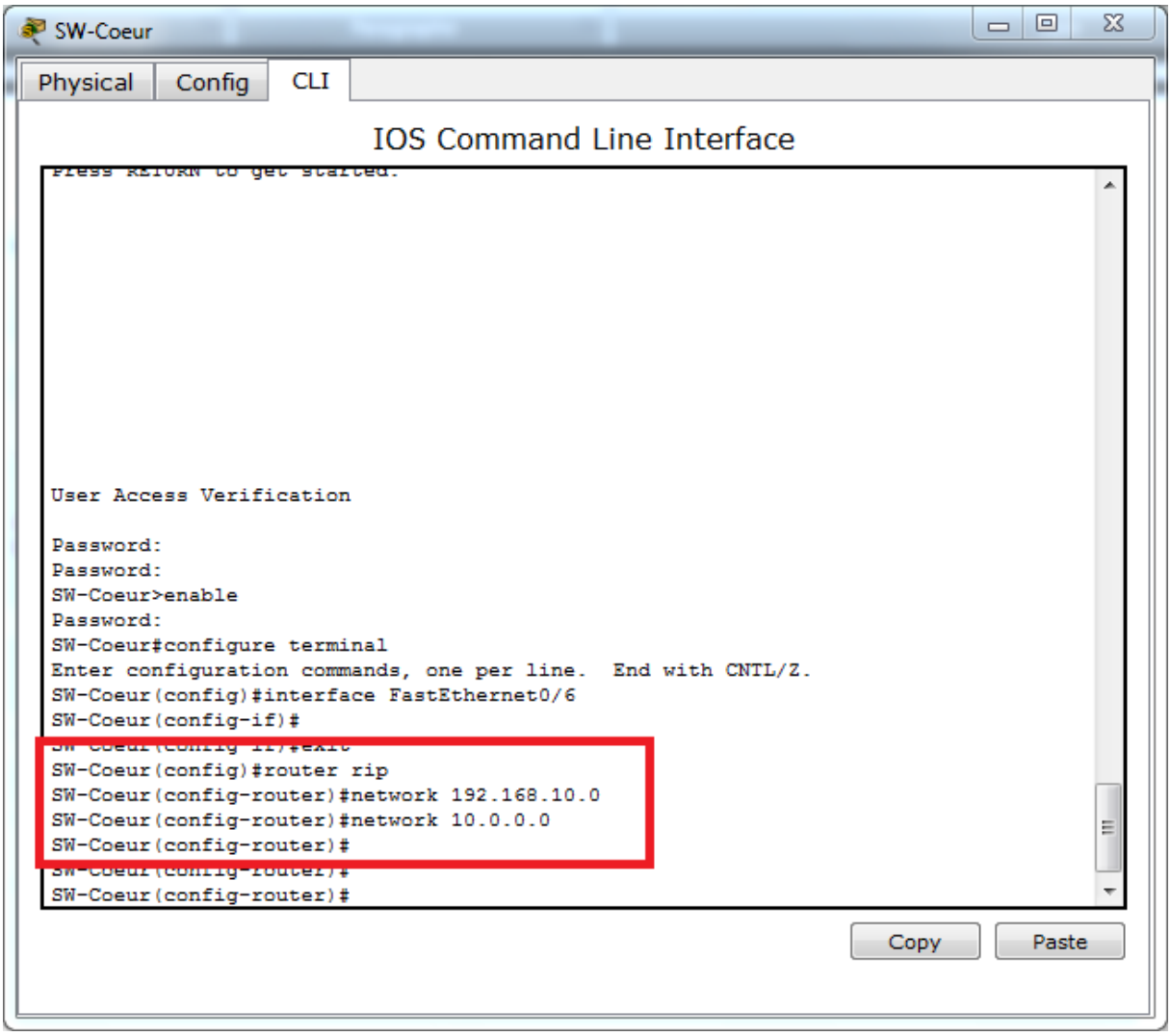

Figure IV. 18 : Routage RIP sur le SW-Cœur.

- **Configuration de routage inter-VLANs**

Nous allons maintenant configurer le routage inter-VLAN avec la commande «ip routing » sur le Switch cœur.

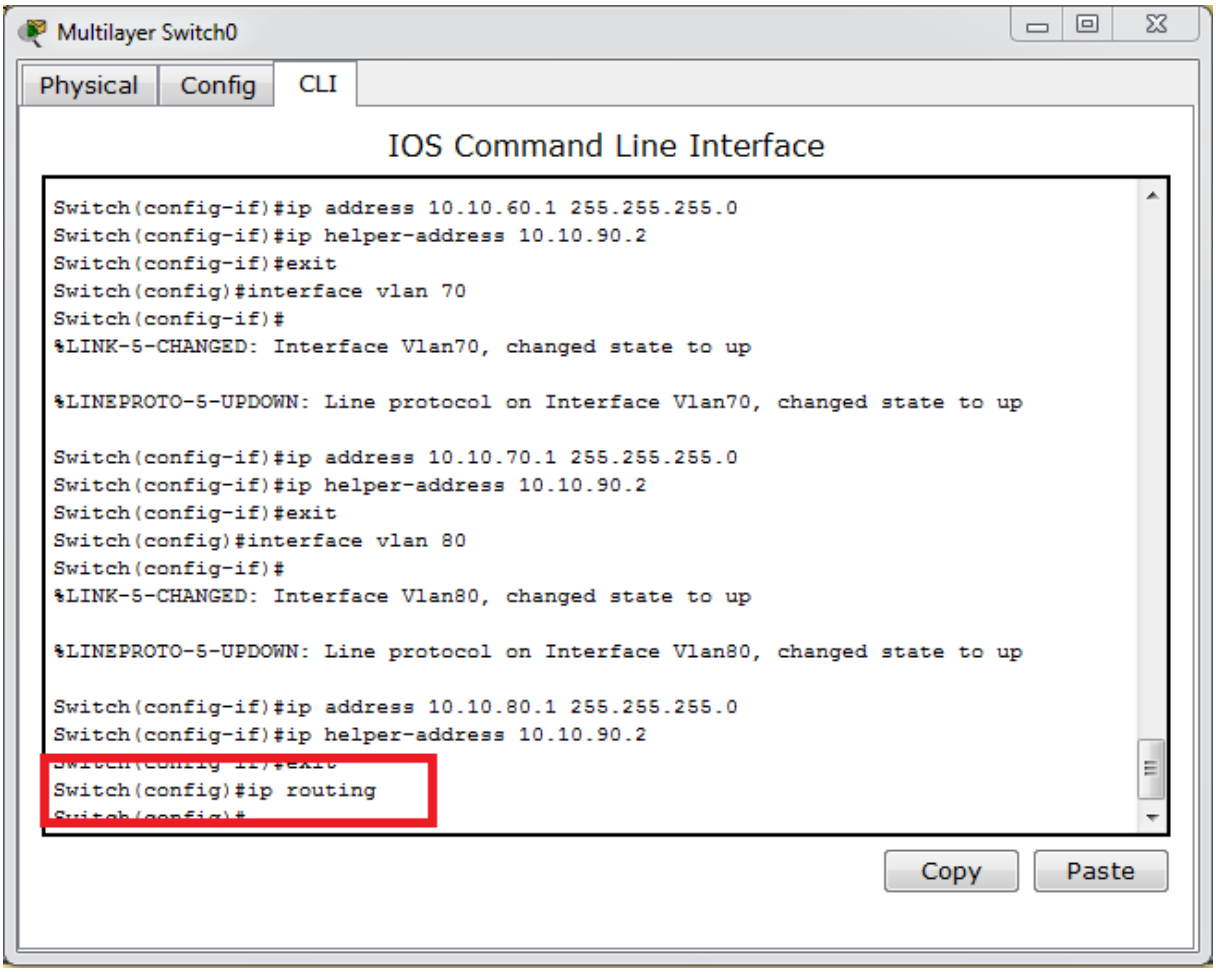

Figure IV.19 : Configuration du routage inter-VLANs.

IV.2.5.2. Configuration du routeur

a. Configuration de l'interface du routeur

Dans cette étape nous allons attribuer les adresses IP à l'interface du routeur qui est directement liée avec le Switch cœur, et l'activer par la suite, comme l'illustre la Figure IV.20.

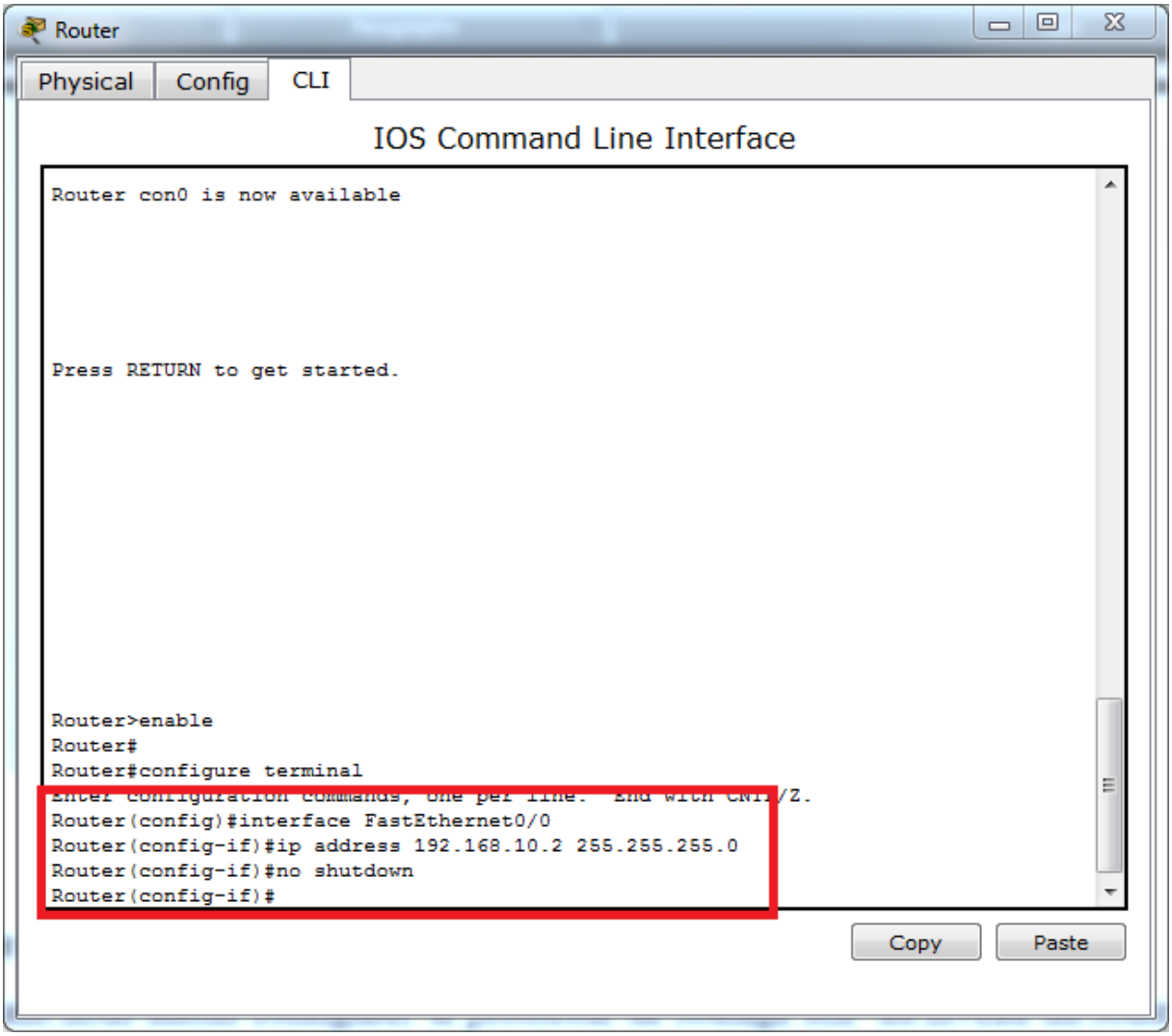

Figure IV.20 : Attribution des adresses IP aux interfaces du routeur.

b. Configuration du routage RIP

Comme nous l'avons fait sur le Switch cœur, nous allons configurer le protocole de routage RIP au niveau du routeur, tel que la figure IV.21 le montre :

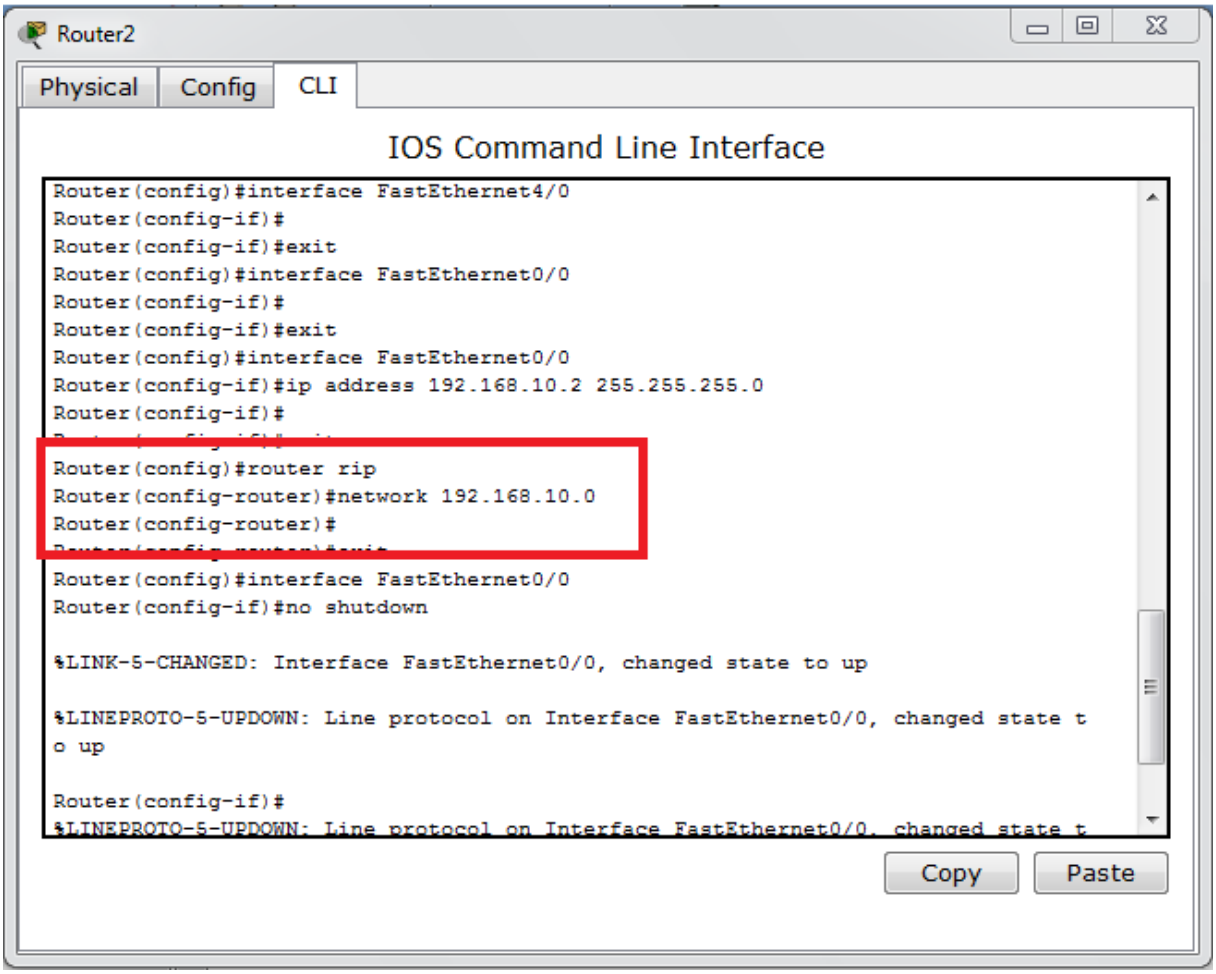

Figure IV.21 : Configuration de routage RIP au niveau du routeur.

IV.2.5.3. Configuration des serveurs et PCs

a. Configuration de DHCP

Pour configurer le serveur DHCP, nous devons tout d'abord créer des pools d'adresses qui comporteront les noms des VLAN tout en introduisant les Gateway (Passerelles) et le nombre maximum d'utilisateurs.

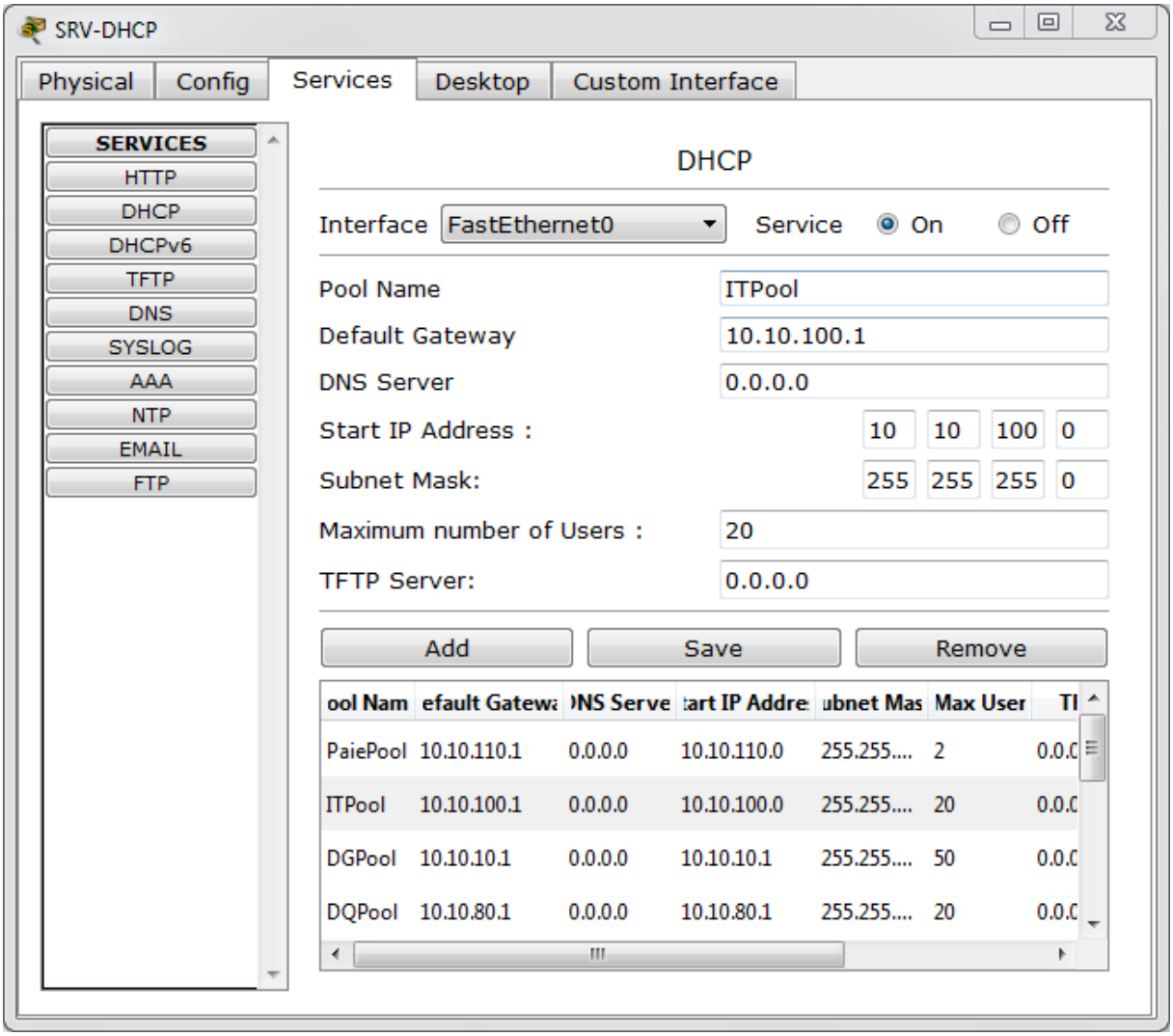

Figure IV.22 : Création des Pools d'adresses.

Ensuite, nous allons attribuer une adresse IP statique au serveur DHCP.

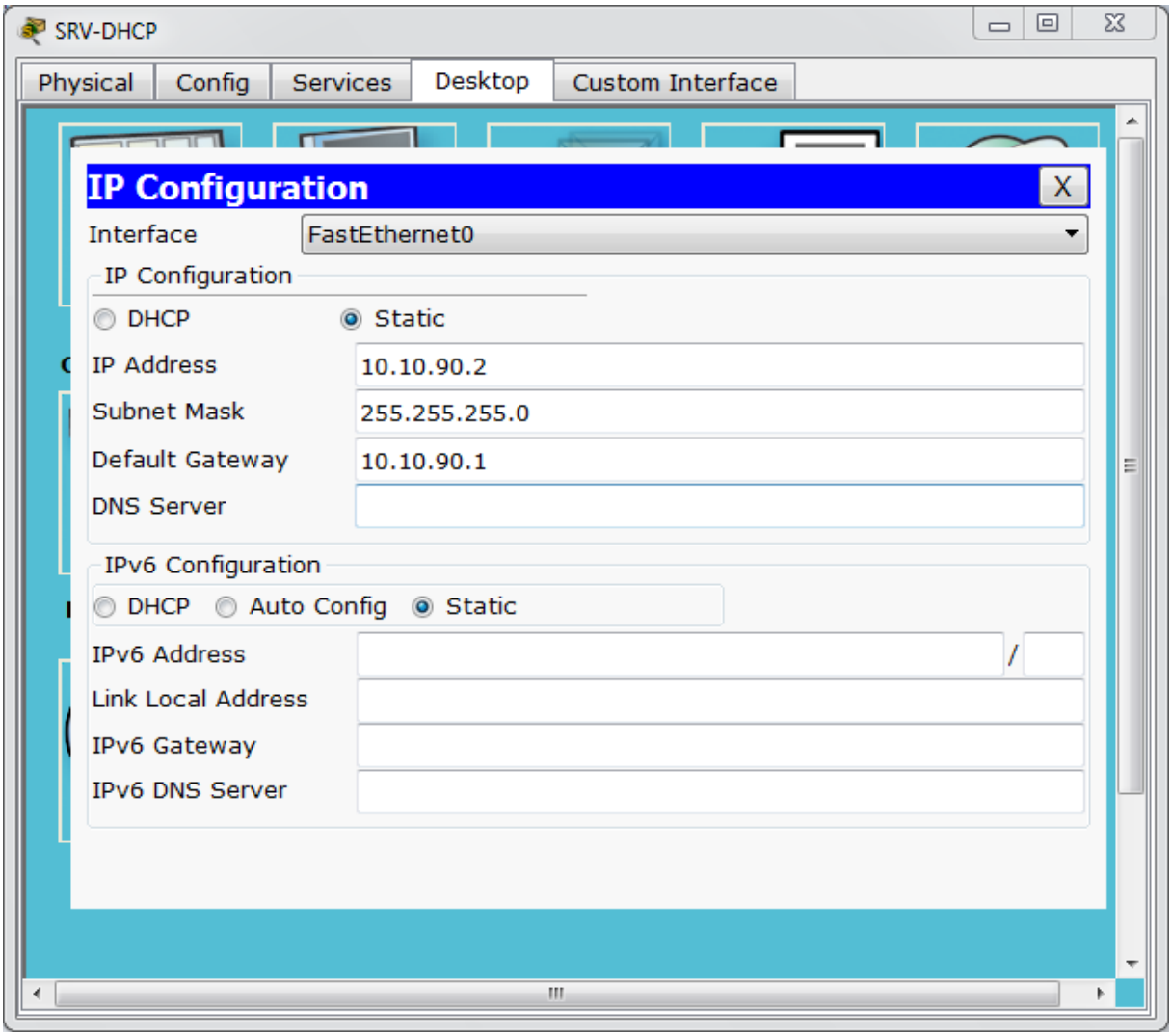

Figure IV. 23 : Attribution d'une adresse IP au serveur DHCP.

b. Configuration des PCs

La configuration des PCs passe par l'attribution d'une adresse IP dynamiquement par le serveur DHCP comme le montre la figure IV.24.

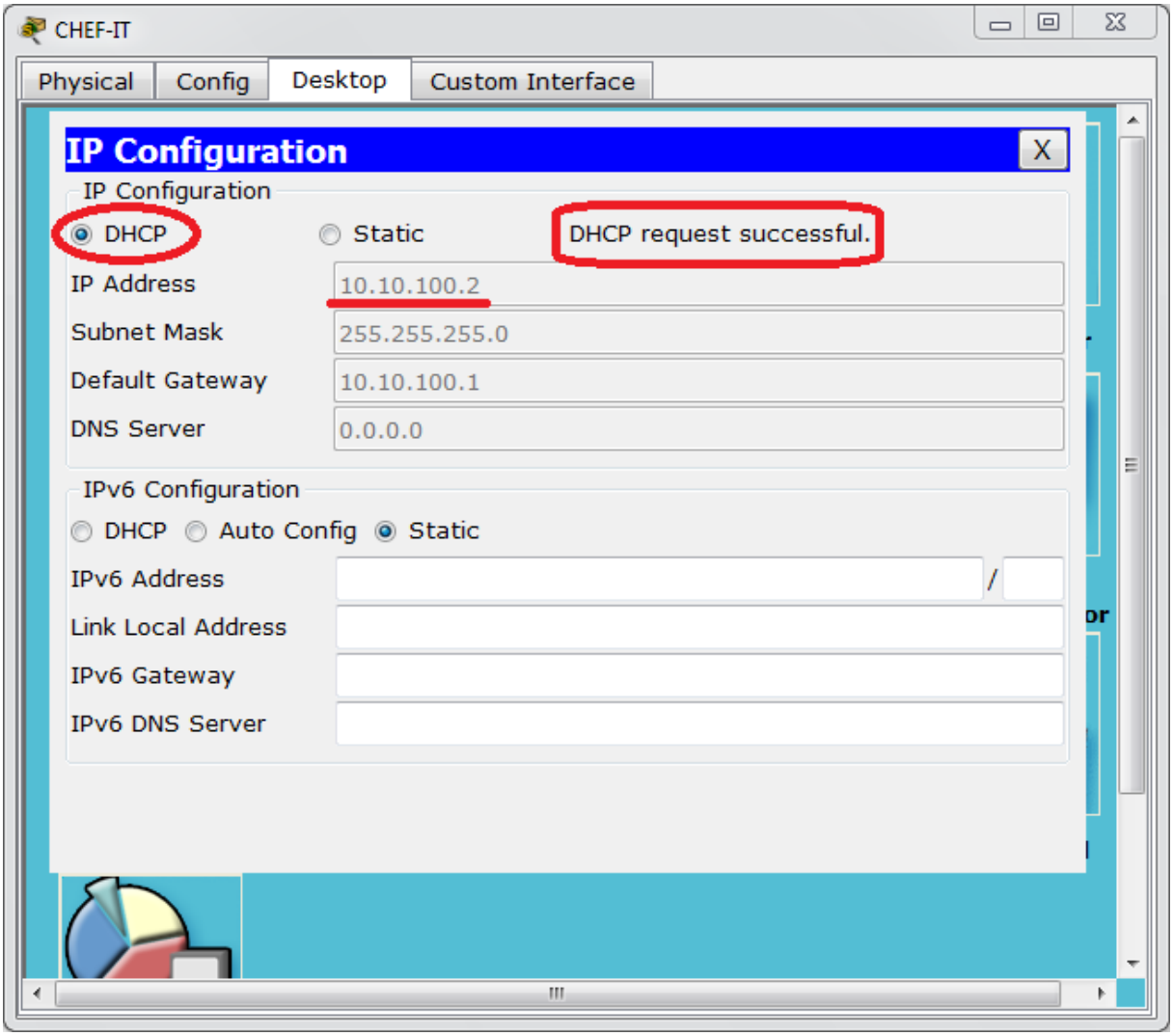

Figure IV. 24 : Attribution d'une adresse IP par le serveur DHCP.

IV.2.5.4. Configuration des points d'accès Wifi

Pour la configuration des points d'accès Wifi, nous prendront pour exemple un point d'accès wifi (figure IV.25) situé à la direction de finances et de commerce.

a. Configuration des points d'accès

Nous allons commencer par la configuration de point d'accès (Acc-Pt-DFC).

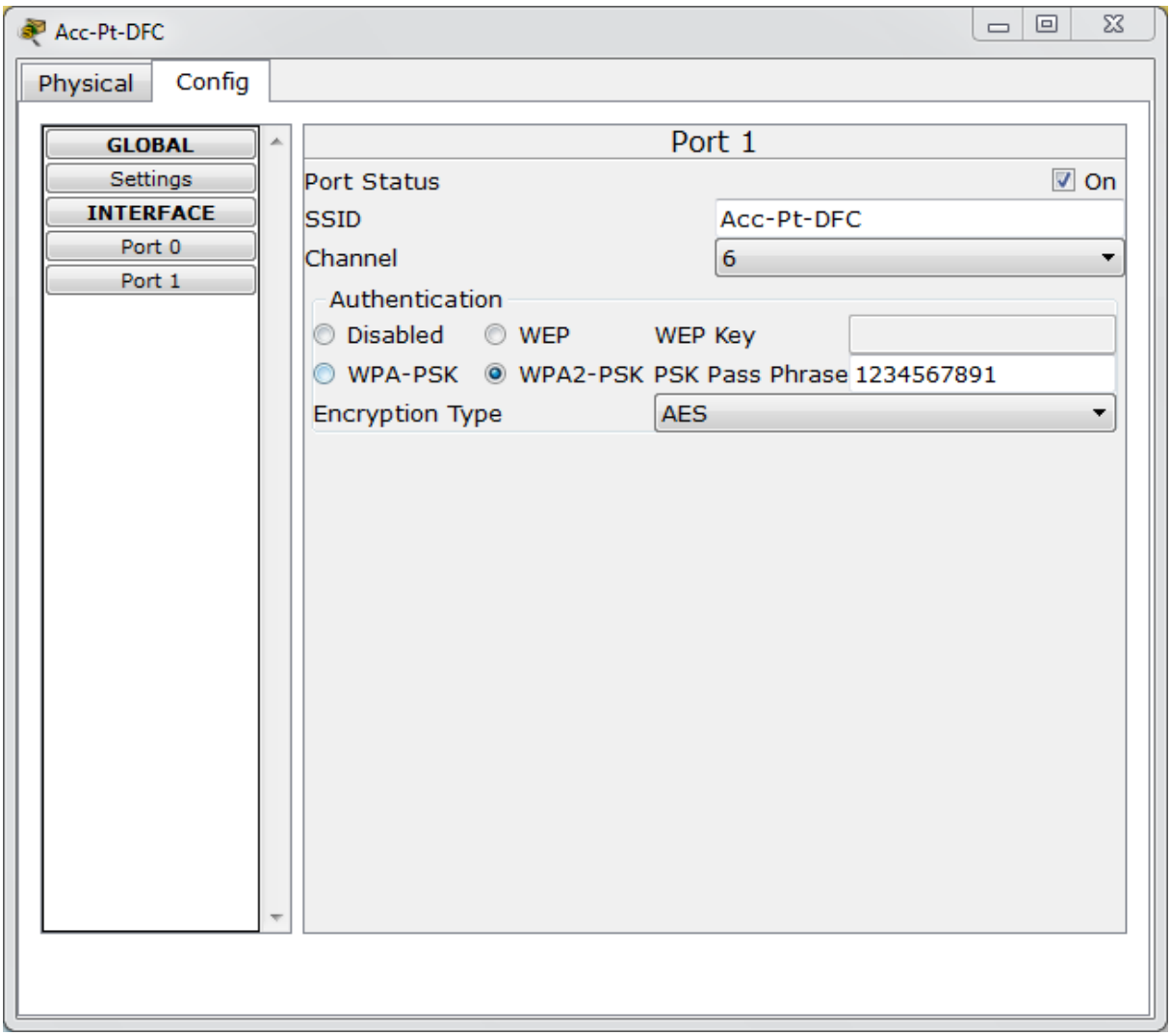

Figure IV.25 : Configuration du point d'accès (Acc-Pt-DFC).

b. Configuration des Laptops

Nous allons maintenant introduire la même clé wifi au niveau du Laptop (figure IV.26), afin que ce dernier puisse se connecter au point d'accès Wifi (figure IV.27)

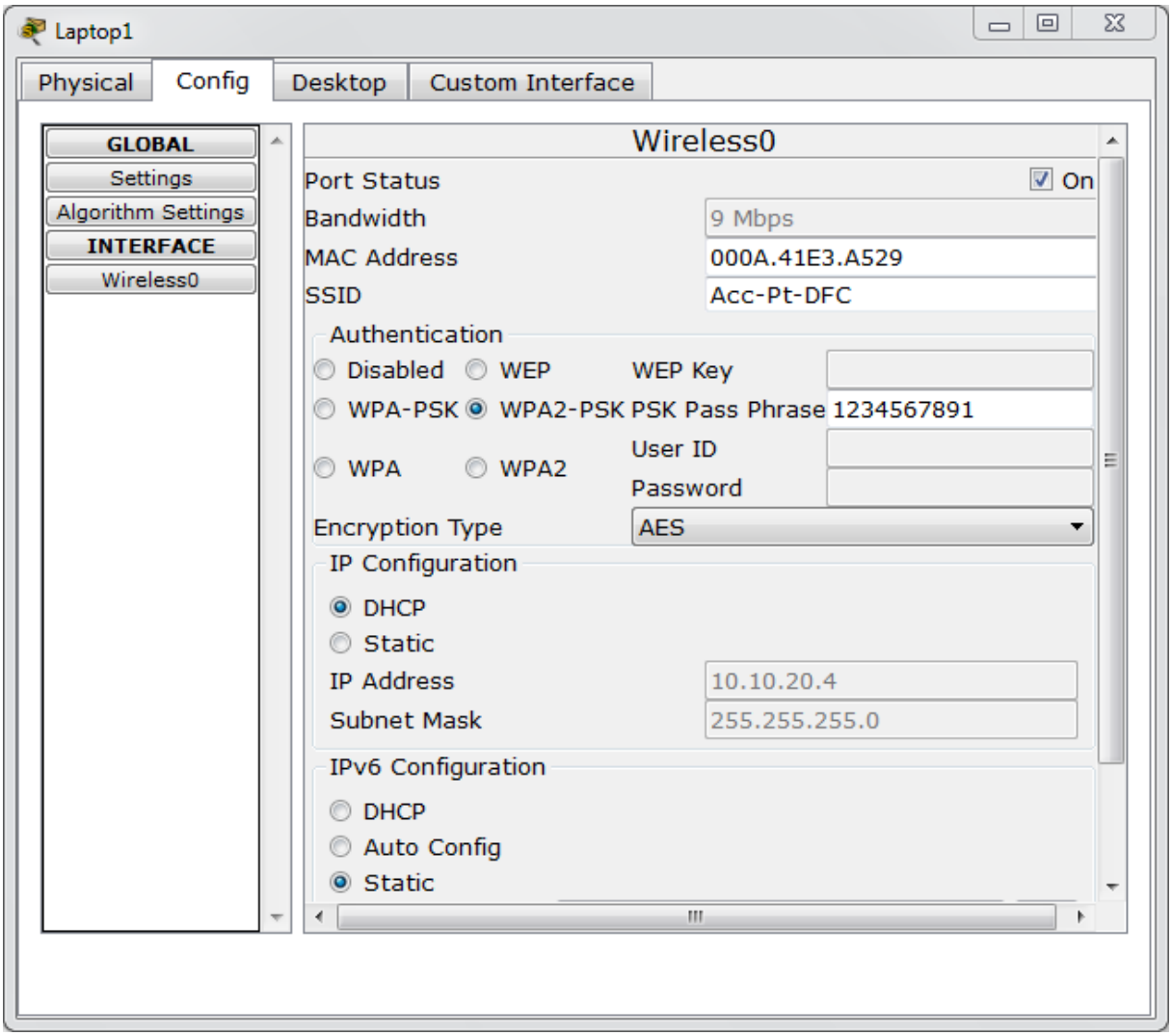

Figure IV.26 : Configuration du Wifi sur le Laptop.

Après l'introduction du mot passe correct, le Laptop est connecté.

Figure IV.27 : La connexion au point d'accès wifi est établie.

IV.2.5.5. Tests de validation des configurations

Dans cette partie, l'ensemble des tests de validation consiste à vérifier l'accessibilité de l'ensemble des équipements, en utilisant la commande « Ping » qui teste la réponse d'un équipement sur le réseau. Donc, si un équipement veut communiquer avec à un autre, le Ping, permet d'envoyer des paquets au destinataire. Si l'équipement récepteur reçoit ces paquets, donc, communication réussie. Sinon, cas échoué.

a. Test intra-VLANs

A ce stade, nous allons vérifier la communication entre les équipements situés dans le même VLAN. Prenant un exemple entre le PC DIRECTEUR (10.10.10.3) et le PC SECRETARIAT (10.10.10.2).

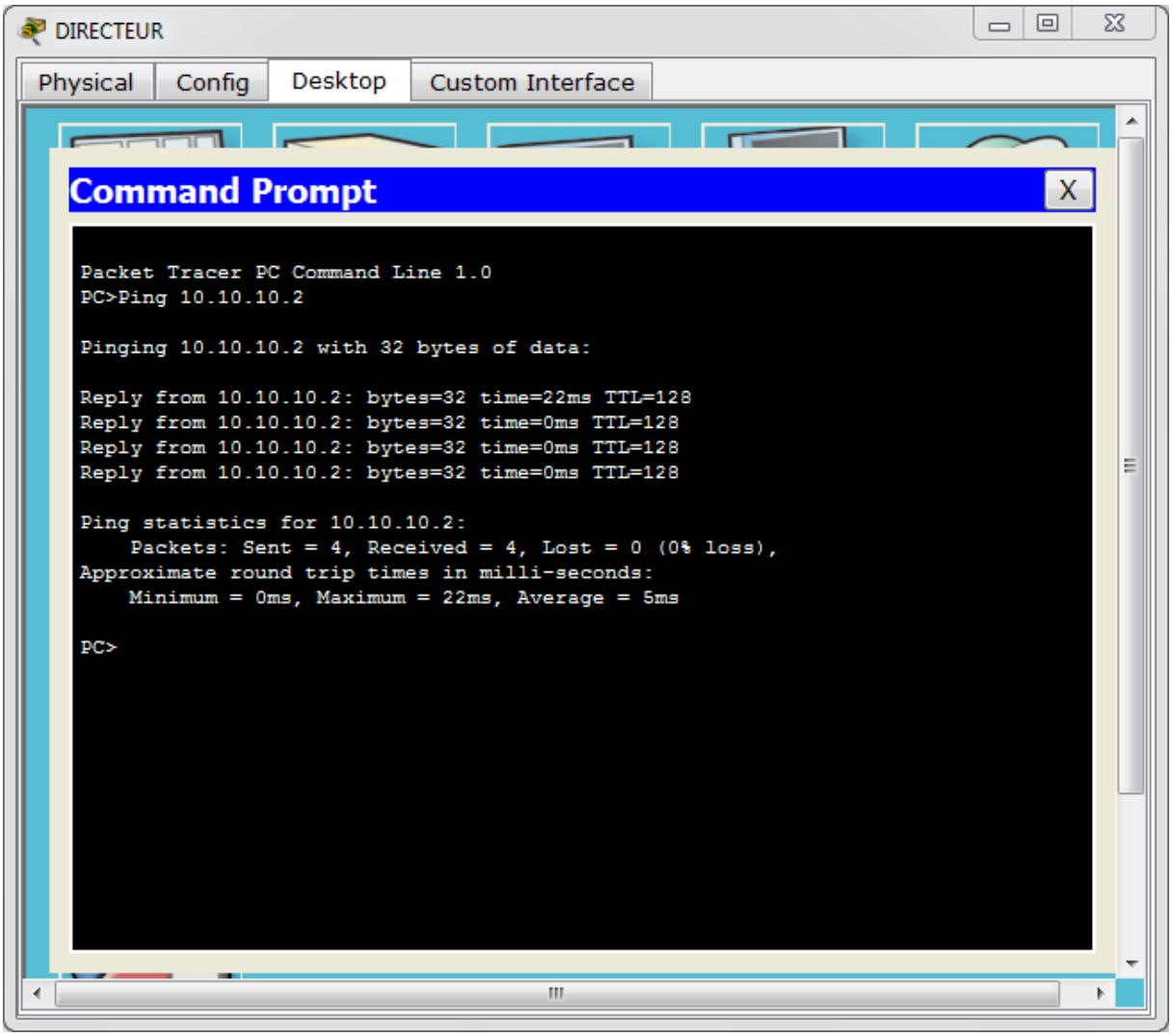

Figure IV.28 : Ping réussi entre le pc DIRECTEUR et le PC SECRETARIAT.

b. Test inter-VLANs

Maintenant vérifier la communication entre les équipements situés dans des VLANs différents. Nous prenons comme exemple le réussi entre PC CHEF-IT (VLAN 100) et PC DIRECTEUR-RH (VLAN 30).

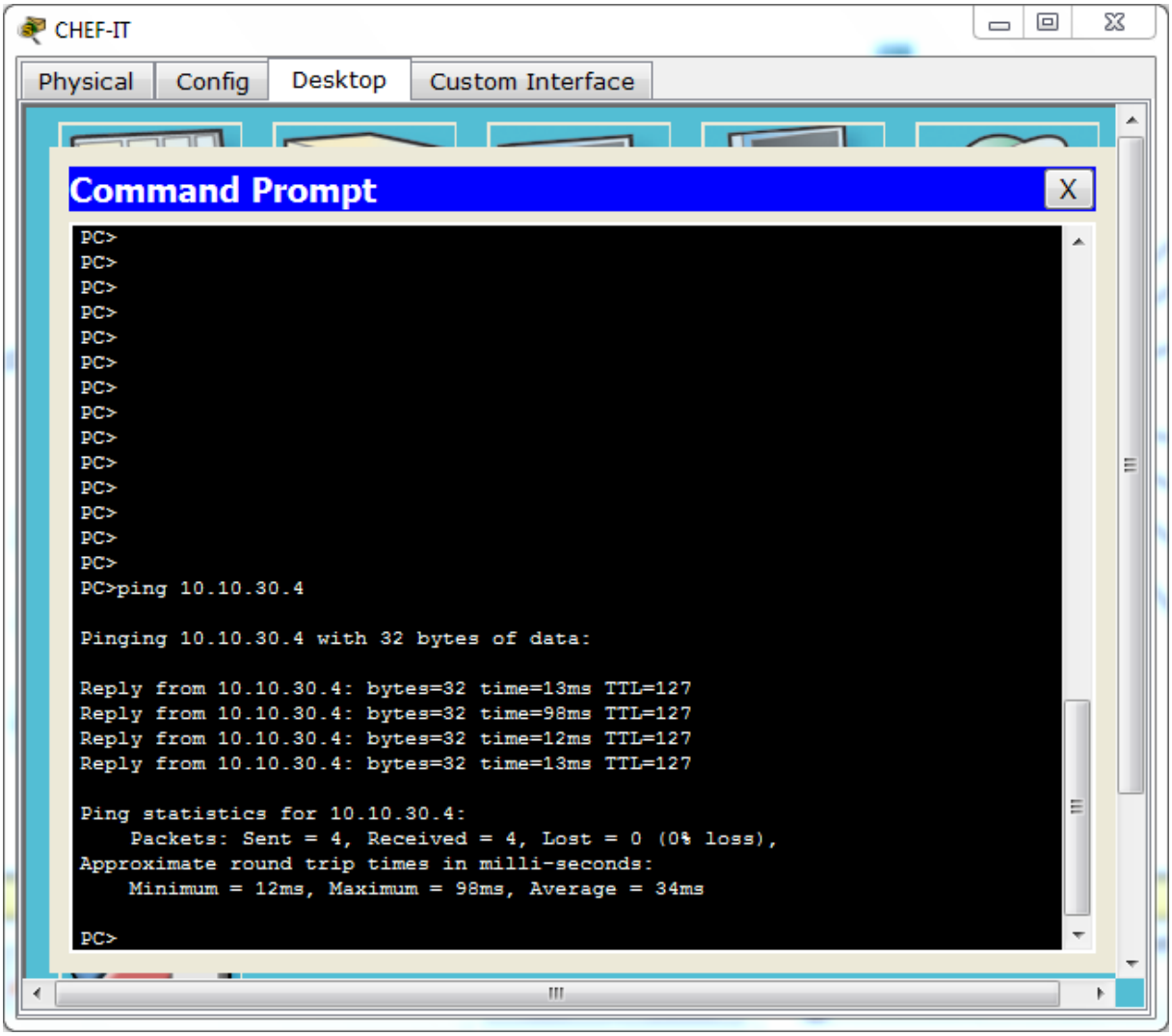

Figure IV. 29 : Test réussi entre PC CHEF-IT (VLAN100) et PC DIRECTEUR-RH (VLAN30).

c. Test des ACLs

Nous allons maintenant illustrer deux exemples pour vérifier l'accessibilité, dans le premier, nous ferons un test de communication entre le pc DIRECTEUR-RH (10.10.30.2) du VLAN 10 (DRH) et le serveur SRV-Paie (10.10.110.2) (Figure IV.30) appartenant à un autre VLAN, sachant que le directeur doit pouvoir accéder au serveur.

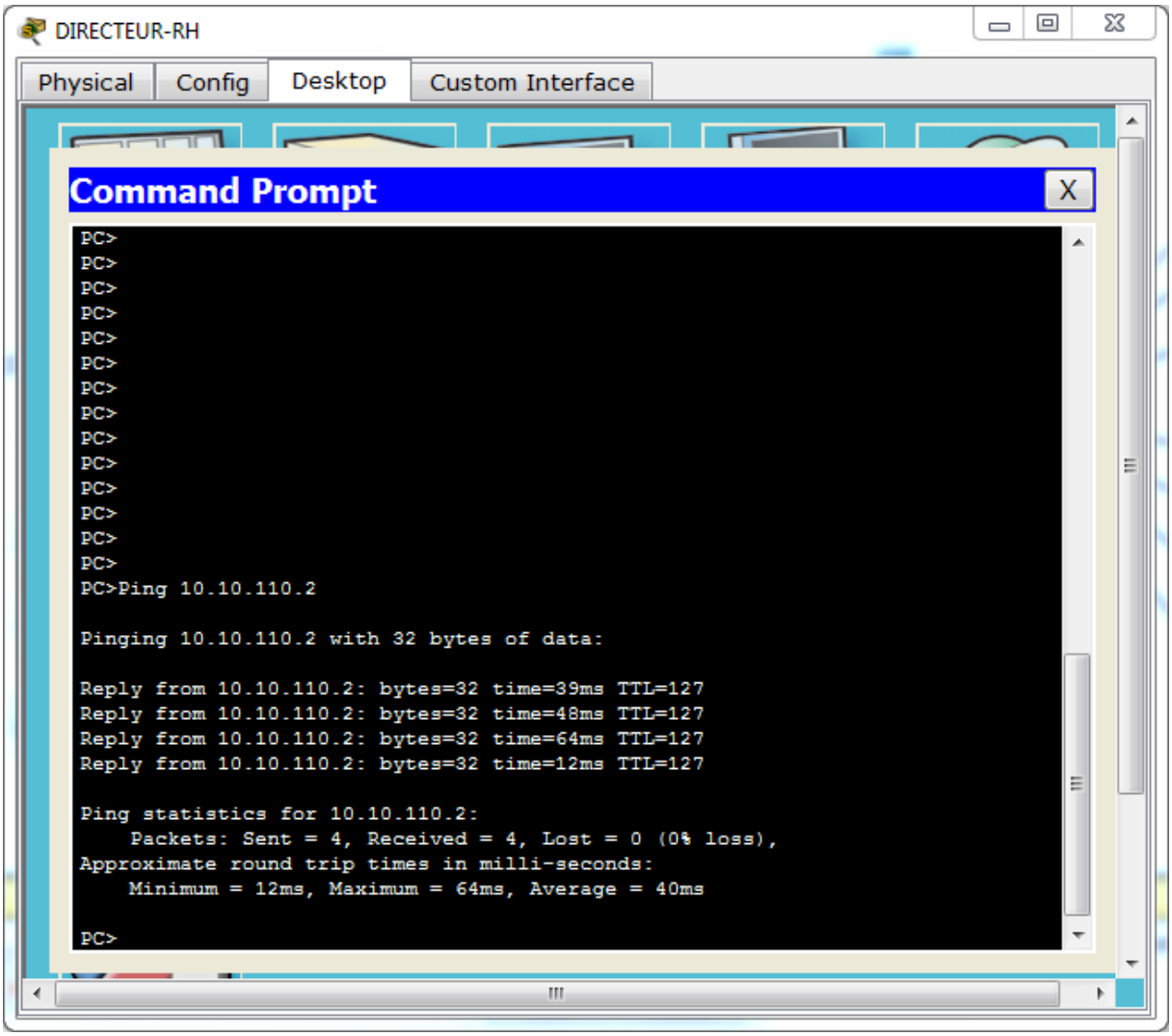

Figure IV.30 : Ping réussi entre le pc DIRECTEUR-RH (VLAN 30) et le SRV-Paie.

Par contre dans le 2éme exemple, nous allons démontrer que le PC8 (10.10.40.3) du VLAN40 (DAppro) ne peut pas communiquer avec le serveur SRV-Paie (10.10.110.2) (Figure machin), car nous avons limité l'accès au serveur grâce à des ACL préalablement implémentées au niveau du Switch cœur.

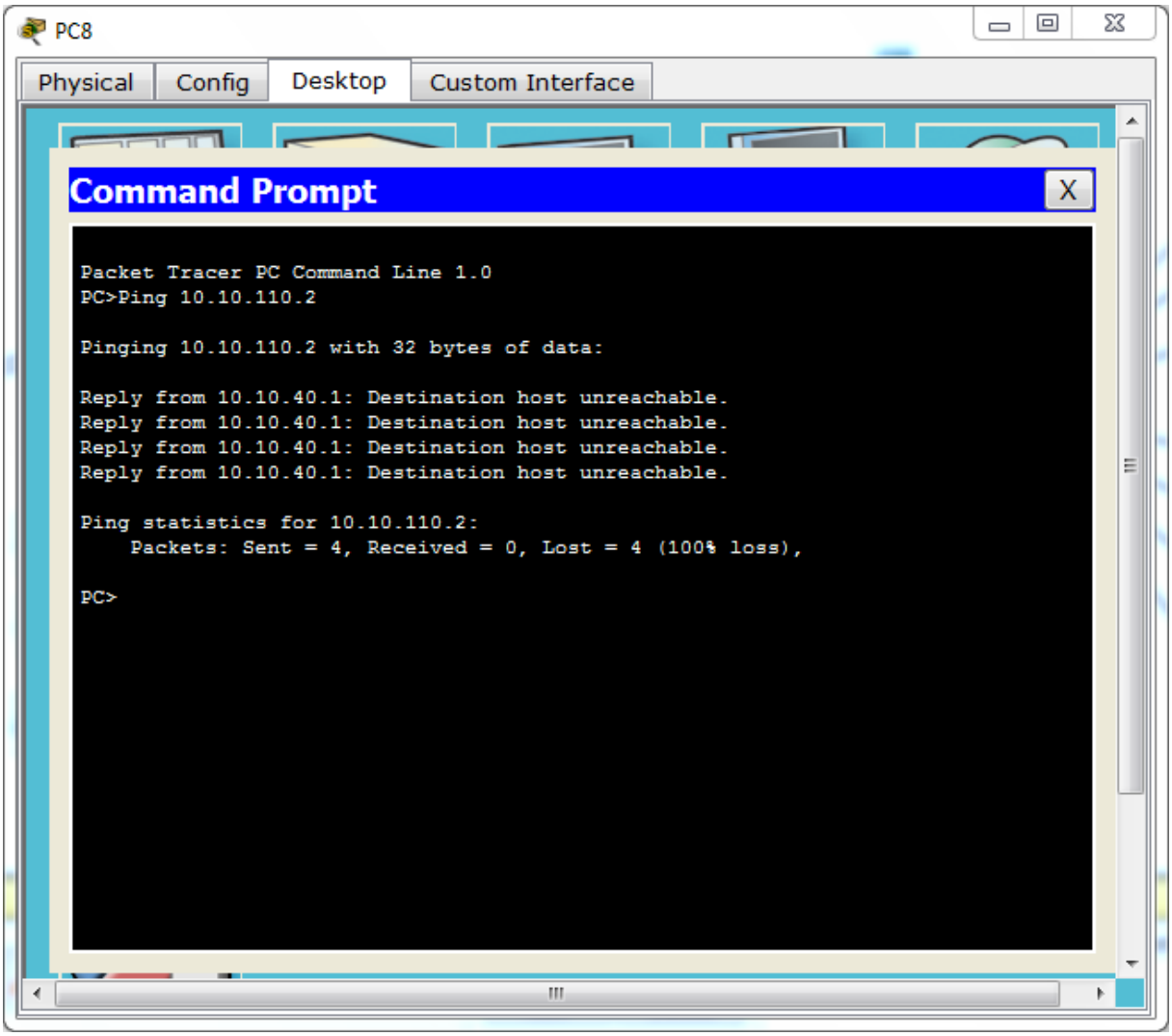

Figure IV.31 : Ping échoué entre le PC8 et le SRV-Paie.

Conclusion

À travers la première partie de ce chapitre, nous avons présenté la conception de l'architecture du réseau local où nous avons désigné, nommé les différents équipements, les interfaces et les différents VLANs que nous allons implémenter dans la phase de réalisation. La deuxième partie est dédiée à la réalisation de notre projet où nous avons commencé par la présentation du simulateur « Cisco Packet Tracer » ainsi que l'ensemble des configurations réalisées au niveau de notre architecture pour sa mise en marche en configurant, les commutateurs et en créant les VLANs, ensuite, nous sommes passé à la configuration du routeur, puis à la configuration des points d'accès Wifi, et enfin nous avons effectué un ensemble de tests de validation et de vérification afin de prouver l'efficacité des solutions.

CONCLUSION GÉNÉRALE

Conclusion Générale

L'étude du réseau local de la SARL « ifri », nous a permis de mettre en place des VLANs dans une nouvelle architecture que nous avons proposée pour son site principal.

Dans notre travail, nous avons abordé les généralités sur les réseaux locaux virtuels notamment, leurs différents types et leurs utilités, ainsi quelques protocoles d'administration et de gestion en l'occurrence VTP, STP et DHCP qu'on a implémenté sur notre architecture réseau.

La réalisation de ce travail est faite comme suite :

- Définition du contexte du projet et critique de l'architecture existante.
- Proposition d'une nouvelle architecture réseau adaptée à la topologie physique actuelle de l'organisme d'accueil
- Création des VLANs avec l'implémentation des protocoles VTP, STP et DHCP.

En effet, nous avons constaté l'intérêt majeur que joue les VLANs, ainsi les protocoles VTP, STP et DHCP dans l'amélioration de la qualité de transmission d'information et plus de souplesse dans l'administration d'un réseau local. Pour un réseau informatique d'une entreprise comme celle de la SARL « ifri », cela va lui permettre une augmentation considérable des performances du réseau.

Ce travail a fait l'objet d'une expérience intéressante, et a eu énormément d'apport sur nos connaissances et nos compétences en terme de configuration dans un environnement Cisco. De Plus, nous avons enrichi nos connaissances déjà acquises dans la segmentation des réseaux locaux d'entreprises en VLANs.

Enfin, pour augmenter la disponibilité et la fiabilité du réseau, Il est nécessaire, pour l'entreprise de prendre en compte notre proposition.

BIBLIOGRAPHIE

[1] Journal officiel, "Liste des termes, expressions et définitions du vocabulaire de l'informatique", octobre 1998.

[2] R. CIREDDU, Cours sur la topologie des réseaux, lycée La Martinière Monplaisir, consulté le 28 Mai 2016.
Source <http://robert.cireddu.free.fr/SIN/La%20topologie%20des%20reseaux.pdf >

[3] M. SALMANI, Cours Réseaux d'entreprise, lycée technique Moulay Youssef, année 2010/2011, consulté le 28 Mai 2016.
Source < http://chari.123.ma/doc_1/salmani/Communiquer/Reseaux%20dentreprise.pdf >

[4] A. TANGUY, Topologie réseaux : Le modèle hiérarchique en 3 couches, 3 Aout 2011, consulté le 28 Mai 2016.
Source < http://bibabox.fr/topologie-reseau-le-modele-hierarchique-en-3-couches/>

[5] W. BAPTISTE, Introduction au réseau, consulté le 29 Mai 2016.
Source <http://baptiste-wicht.developpez.com/tutoriel/reseau/introduction/developpez.com>

[6] Cours réseau, Modèle OSI, USTHB, consulté le 01 Juin 2016.
Source < http://usthb.orgfree.com/info/5eminfo/cours/Coursreseau/ModeleOSI.doc >

[7] < http://cisco.goffinet.org/s1/modele-tcp-ip-et-protocoles > consulté le 01 Juin 2016.

[8] < http://www.commentcamarche.net/contents/reseaux-internet-5 > consulté le 01 Juin 2016.

[9] T. LAMMEL, CCNA CISCO certified network associate study guide 6éme edition, 2007.

[10] : Agence Wallonne des Télécommunications, Les VLAN Ethernet, consulté le 03 Juin 2016.
Source < http://www.awt.be/contenu/tel/fic/t00,015.pdf >

[11] E. LECLERCQ et M. SAVONNET, Réseaux virtuels (VLAN), Université de Bourgogne, 8 avril 2011, consulté le 04 juin 2016.
Source < http://ufrsciencestech.u-bourgogne.fr/licence3/SystemesEtReseaux2/SupportsCours/ch10.pdf >

[12] R. SANCHEZ, Les réseaux locaux virtuels, CERTA, janvier 2006, consulté le 06 Juin 2016.
Source < http://www.reseaucerta.org/docs/didactique/VLAN.pdf >

[13] G. VALET, Notions fondamentales sur les réseaux, lycée Diderot - Paris 17, Janvier 2011, consulté le 06 Juin 2016.
Source < http://docplayer.fr/12272170-Les-lans-virtuels-vlans.html >

[14] P. LATU, Introduction au routage inter-VLAN, consulté le 07 Juin 2016.
Source < https://www.inetdoc.net/pdf/inter-vlan-routing.pdf >

[15] F. NOLOT, Cours Les Virtual LAN, Université de Reims Champagne – Ardenne, consulté le 07 Juin 2016.
Source < http://www.nolot.eu/Download/Cours/rezo/AdminRS-Cours2-VLAN.pdf >

[16] E. NOBILET, Procédure VLAN Trunking Protocol, consulté le 12 Juin 2016.
Source
<http://nobileteric.weebly.com/uploads/2/9/6/6/29668301/proc%C3%A9dure_vtp.pdf>

[17] A. AUBERT, Apprentissage et suppression de boucles, Télécom Saint-Etienne, consulté le 12 Juin 2016.
Source <
https://mootse.telecom-st-etienne.fr/pluginfile.php/13048/mod_resource/content/1/STP.pdf>

[18] R. DROMS et T. LEMON, The DHCP Handbook. Macmillan Technical Publishing, 1999, consulté le 14 Juin 2016.
Source < http://www.dhcp-handbook.com/>

[19] < http://www.linux-france.org > consulté le 15 Juin 2016.

[20] Simulation du fonctionnement d'un réseau informatique, Académie de LYON, consulté le 16 Juin 2016.
Source < http://sen.arbezcarme.free.fr/_atelier/3.3-Rotation-3-ToutEnBois/3.3.6-Simulation-du-fonctionnement-d-un-reseau-informatique/TP%20Cisco%20Packet%20Tracer.pdf >

[21] Packet Tracer, Manuel de prise en main, consulté le 16 Juin 2016.
Source <http://www.siloged.fr/cours/docs/manuels/doc_packettracer.pdf>

RÉSUMÉ

La flexibilité d'un réseau local est un paramètre très important auquel toute organisation doit faire face compte tenu de son évolution. A cet effet, afin de gérer au mieux l'extensibilité de son réseau et apporter plus d'agilité dans sa gestion, plusieurs techniques et concepts sont apparus tel que les VLANs.

Dans notre projet, nous nous sommes intéressés à l'étude du réseau local de l'entreprise « ifri » et à la configuration des VLANs en utilisant le logiciel Cisco Packet Tracer. Nous avons commencé par la présentation des aspects théoriques relatifs aux réseaux informatiques et les VLANs, la présentation du cadre de référence spécialement le réseau local de « ifri », et nous avons fini par la mise en œuvre comportant la simulation du réseau local basé sur les VLANs.

Mot clés : Réseau local, VLAN, Simulation, Packet Tracer.

ABSTRACT

The flexibility of a local area network is a very important parameter which any organization has to face considering its evolution. For that purpose, to manage at best the extensibility of its network and bring more suppleness in its management, several techniques and concepts appeared such as VLANs.

In our project, we are interested in the study of the local network of the "ifri" company and configurate VLANs solution using Cisco Packet Tracer software. We began with the presentation of the theoretical aspects relative to the data networks and the VLANs, the presentation of the reference frame specially the local area network of " ifri ", and we finished by the implementation containing the simulation of the local area network based on the VLANs.

Keywords: LAN, VLAN, Simulation, Packet Tracer.