République Algérienne Démocratique et publique
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira De Bejaia.
Faculté des Sciences Exactes
Département Informatique

Mémoire de fin de Cycle

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

Option : Administration et Sécurité des Réseaux Informatique

Thème

Proposition d'une configuration sécurisée d'un Réseau Local

Cas D'étude : Entreprise NAFTAL.

Réalisé par :

- Mr BOUBALOU Saïd
- Melle YOUSFI Meriem

Devant le jury composé de :

Président : Mr K.AMROUNE	M.C.B, Université A/Mira de Bejaia
Examinateur: Mr R.OUZEGANE	M.A.A, Université A/Mira de Bejaia
Examinateur: Mr N.REGAB	M.A.A, Université A/Mira de Bejaia
Encadreur : Mm K.GHIDOUCHE	M.A.B, Université A/Mira de Bejaia

Promotion 2015-2016

Remerciements

Nous remercions d'abord notre Dieu de nous avoir accordé le courage et la patience pour mener à bout ce travail.

Nous remercions notre Encadreur M^{me} GHIDOUCHE Kahina d'avoir accepté de diriger ce travail, et pour ses précieux conseils et encouragements, sans lesquels cette étude n'aurait pas vu le jour. Merci pour votre confiance, votre disponibilité même depuis l'étranger et le temps que vous avez bien voulu consentir à l'aboutissement de ce mémoire.

Nous remercions de même notre encadreur de stage M^{r} TALAELBIR pour son encadrement pendant celui-ci.

Nos remerciements s'adressent également aux membres du jury M^{r} AMROUNE , M^{r} OUZEGANE Redouane et M^{r} REGAB Nadim qui nous ont honorés en acceptant d'examiner notre travail et surtout d'y avoir aporter un jugement critique et objectif a ce travail.

Nous tenons à remercier tous les enseignants qui ont assurés notre formation Durant notre cycle universitaire. Ainsi, que tout le personnel du département informatique.

Dédicaces

A la femme de ma vie, que dieu, le tout puissant, te préserver et t'accorder santé, longue vie et bonheur, à ma mère.

A l'homme qui sait toujours sacrifiés pour me voir réussir, à mon exemple eternel, à mon père.

A ma chère petite sœur, à qui je souhaite toute la réussite du monde ainsi que tout le bonheur.

A celle qui a su me redonner le sourire, à celle qui a fait de moi une personne meilleure, à Sabrina.

A celle qui a partagé tout cela avec moi, à ma très chère binôme, à mon amie Meriem

A ma deuxième famille avec laquelle je partage toute ma vie, à l'association LAHNA SMILE.

A mes chers amis, Fayçal, Kamel, Mohamed, Idir, Djilalli, Adel, Amine, Karim, Hafidh, Dyhia, , Ryma, Nesrine, Imene, Nissa, katia, Sara, Mimi, Siham, Mouna, à tous mes amis, merci pour tout.

Said

Dédicaces

A ma force qui m'inspire chaque jour, que la puissance divine le protège et lui procure santé, à mon père.

A *mon eternel soutien, mon absolu idéal, que dieu puisse lui accorder longue vie, à ma mère.*

A *mes piliers ceux qui ne cessent de m'encourager, de me chérir, à mes frères et mes sœurs.*

A *ma meilleure amie qui n'a jamais existé, qui m'a soutenu et qui a toujours été là pour moi, à toi chère Katia.*

A *mon binôme pour le frère agréable qu'il était et qu'il restera pour moi, à mon ami Saïd.*

A *toute ma famille, la fierté d'être l'une des leurs,*

A *ma deuxième famille celle que j'ai vu naitre, à l'association Lahna smile.*

A *mes amis(e).*

Meriem

Tables des matières

Tables des matières

Tables des matières

Tables des matières

Liste des figures

Liste des tableaux

Liste des abréviations

AAA : Authentification Autorisation Acouting

ACL : Access control list

ARP : Adresse Resolution Protocol

DZM : DeMilitarized Zone

FTP : File Transfert Protocol

ICMP : Internet Control Message Protocol

IDS : Système de détection d'intrusion

IGMP: Internet Group Management Protocol

IP: Internet Protocol

IPSec: Internet Protocol Security

LAN: Local Area Network

L2TP: Layers 2 Tunneling protocol

L2F: Layer 2 Forwarding

MAN: Métropolitain Area Network

OSI: Open System Interconnection

Liste des abréviations

PPTP: Point-to-point Tunneling Protocol

RARP: Reverse Address Resolution Protocol

STP: Shielded Twisted Pair

SMTP: Simple Mail Transport Protocol

TELNET: Telecommunication Network

TCP: Transmission Control Protocol

UTP: Unshielded Twisted Pair

VPN: Virtual Private Network

WAN: Wide Area Network

Introduction générale

L'humanité a longtemps imaginé un monde où nous contrôlons tout, un univers sans frontières ni limites où tout est possible, c'est de ces besoins qu'est née l'informatique, cette science qui met en œuvre des ensembles complexes de machines appelés Automate, Calculateurs, Ordinateurs, et systèmes informatiques.

L'évolution de la technologie ne s'est pas arrêtée la, en effet un moyen **e** relier ces équipements informatique fut élaborée, c'est ce qu'on appelle les réseaux informatiques. L'utilisation croissante de ces derniers dans les entreprises et leur interconnexion à internet on fait émerger aujourd'hui de nouvelles préoccupations sécuritaires.

La majorité des entreprises ne peuvent plus ignorer désormais d'intégrer la sécurité informatique de leurs réseaux dans leur cahier de charges, si elles ne veulent pas risquer de voir leurs outils de travail perturbés par une attaque ciblées ou non, généralisée, véhiculée par le réseau mondial ou par leur propres réseaux locaux. Pour ne pas perdre d'information névralgique, une stratégie de défense sécuritaire en conséquence s'impose. Et vue la diversité des attaques évolutives dans le temps, il faut constamment rechercher de nouvelles solution pour sécuriser le réseau.

La sécurité des réseaux est devenue un élément-clé de la continuité des systèmes informatique de l'entreprise quelque soit son activité. L'entreprise NAFTAL de BEJAIA ne déroge pas à cette règle. Avec le nombre d'utilisateur qui ne cesse d'accroitre les risques sécuritaire augmentent considérablement et le réseau local se fragilise vis-à-vis d'éventuelles attaques internes et/ou externes. Tout cela nous pousse à travailler sur **Proposition d'une configuration sécurisé du réseau local de NAFTAL.**

Le premier chapitre s'intitule **« Généralités sur les réseaux »** où nous présentons quelques principes de base des réseaux informatique.

Le deuxième chapitre titré « **Généralités sur la sécurité informatique »** sera consacré à la présentation des différentes techniques de sécurité utilisées et plus particulièrement celle des réseaux locaux.

Le troisième chapitre nommé **« Présentation de l'organisme d'accueil »** aura pour objectif de mieux comprendre l'organisme et sa structure hiérarchique, nous allons donc évoquer les différentes problématiques rencontrés et la solution que nous pensons la plus adéquate.

Introduction générale

Le quatrième et dernier chapitre nous allons enfin passer à la **« Réalisation »**. Ce dernier est décomposé en deux partie, dans la première nous introduirons les outils et logiciels ayant servi à l'élaboration du projet, tout en expliquant les configurations, nous passerons ensuite à la deuxième partie qui sera consacrée à l'implémentation des solutions présentées précédemment.

La conclusion Générale résumera les points forts accomplis dans ce travail, tout en spécifiant quelques perspectives futures pour mener à bien ce travail.

CHAPITRE I

GENERALITES SUR LES RESEAUX

Introduction

Les réseaux sont nés du besoin de transporter une information d'une personne à une autre. Pendant longtemps, cette communication s'est faite directement par l'homme, comme dans le réseau postal, ou par des moyens sonores ou visuels. Il y a un peu plus d'un siècle, la première révolution des réseaux consisté à automatiser le transport des données.

Aujourd'hui, on peut dire qu'un réseau est un ensemble d'équipement et de liaisons de télécommunication autorisant le transport d'une information. L'objectif de ce chapitre est de présenter les concepts de base liés aux réseaux informatiques.

I.1 Définition d'un réseau informatique

Un réseau informatique est un réseau dont chaque nœud est un système informatique autonome, reliés par un support matériel et logiciel, et qui ont ainsi la possibilité de communiquer entre eux directement ou indirectement. En pratique deux ordinateurs suffisent pour constituer un réseau informatique.

Les services offerts par un réseau informatique peuvent être de nature très diverses et multiples, mais généralement prennent l'une des formes suivantes : Échange des informations, Partage et centralisation des ressources matérielles et/ou logicielles.

I.2 Objectifs des réseaux

La nécessité de communication et de partage des informations en temps réel, imposent aujourd'hui aux entreprises ainsi qu'aux individus la mise en réseau de leurs équipements informatiques en vue d'améliorer leurs rendements.

I.2.1 Apports pour les entreprises

Les réseaux permettent aux entreprises de :

- Partager des ressources (imprimantes, disque dur, processeur, etc.)
- Réduire les coûts.
- Augmenter la fiabilité : dupliquer les données et le traitement sur plusieurs machines. Si une machine tombe en panne une autre prendra la relève.
- Fournir un puissant média de communication (e-mail, conférence virtuelle, etc.).

I.2.2 Apports pour les individus

Les réseaux permettent aux individus :

- L'accès facile et rapide à des informations pertinentes : Informations de type financier
- L'accès au système de type Toile (Web) : recherche des informations de tout genre (sciences, art, cuisine, sport, etc.).
- La communication entre les individus : Vidéoconférence, courrier électronique, groupes d'intérêts (newsgroup) etc.
- L'envoie de textes, de sons et d'images.
- L'accès aux jeux interactifs : toutes sortes de jeux (jeux d'échec, de combats, etc.).

I.3 Les types de réseaux

Les différents types de réseau informatique peuvent être classifiés selon leurs étendues, on distingue les réseaux suivant :

I.3.1 Le réseau local

S'étendant sur quelques dizaines à quelques centaines de mètres, le Local Area Network (LAN), en français Réseau local d'entreprise (RLE), sont utilisés principalement pour relier les ordinateurs personnels ou les stations de travail que l'on trouve dans les

entreprises à des ressources partagées avec les quelles ils échangent des informations. Le débit peut aller de quelque Mb/s à 100 Mb/s.

Les LANs étant de taille restreinte, le délais de transmission est borné et connu, ce qui permet, par exemple, de simplifier la gestion du réseau.

Voici quelques caractéristiques des réseaux locaux :

-La simplicité de sa configuration.

-Les adresses sont attribuées aux équipements dès leurs installations. Ceux-ci peuvent être insérés ou retirés, ou encore être inactifs sur le réseau, pour autant perturber son fonctionnement.

-Le coût de câblage intervient pour une part non négligeable dans l'installation du réseau.

I.3.2 Le réseau métropolitain

Le réseau Métropolitain Area Network (MAN) est également nommé réseau fédérateur. Il assure des communications sur des plus longues distances, interconnectant souvent plusieurs réseaux LAN, Il peut servir à interconnecter, par une liaison privée ou non, différents bâtiments distants de quelques dizaines de kilomètre.

I.3.3 Le réseau étendu

Les étendues de réseaux les plus conséquentes sont classées en Wide Area Network (WAN). Constitué de réseaux de type LAN, voire MAN, les réseaux étendus sont capables de transmettre les informations sur de milliers de kilomètres à travers le monde entier. Le WAN le plus célèbre est le réseau public internet dont le nom provient de cette qualité : Inter Networking ou interconnexion de réseaux.

I.4 Topologies des réseaux

Il existe deux types de topologie dans les réseaux, le premier est la topologie da câblage ou topologie physique. Le second est la topologie d'accès ou topologie logique.

I.4.1 Topologie physique

La topologie d'un réseau décrit la façon dont sont interconnectés les nœuds et les terminaux des utilisateurs. On distingue trois topologies, l'étoile, le bus et l'anneau, qui peuvent être combinées pour obtenir des topologies hybrides :

- **L'étoile :** Dans cette architecture (Figure1), qui fut la première créée, chaque station, est reliée à un nœud central. La convergence entre les télécommunications et l'informatique a favorisé cette topologie, qui a l'avantage de s'adapter à de nombreux cas de figure reconfigurable, une étoile pouvant jouer le rôle d'un bus ou d'un anneau.

  Du fait de sa centralisation, la structure en étoile peut toutefois présenter une certaine fragilité. De plus, elle manque de souplesse, puisqu'il faut une liaison supplémentaire pour toute station rajoutée et que les extensions du réseau sont limitées par la capacité du nœud central.

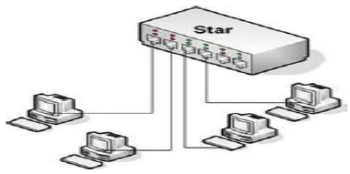

Figure I.1 : La topologie en étoile.

- **Le bus** : Dans cette architecture, les stations sont raccordées à une liaison physique commune. La figure 2 représente une topologie en bus, avec un câble sur lequel se connectent de nombreuses machines (stations de travail, imprimante, etc.).

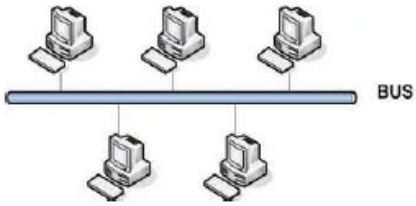

Figure I.2 : La topologie en bus.

- **L'anneau :** Dans cette configuration, le support relie toutes les stations, de manière à former un circuit en boucle, comme illustré à la figure 3. L'information circule dans une direction, le long du support de transmission. Il est cependant possible de réaliser un réseau bidirectionnel en utilisant deux anneaux, les transmissions s'effectuent dans les deux sens.

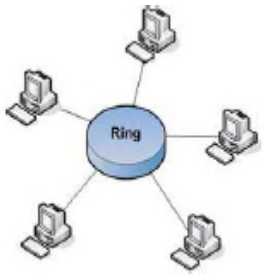

Figure I.3 : La topologie en anneau.

I.4.2 Topologie logique

Elle correspond à la manière de faire circuler le signal parmi les composantes physiques. Par opposition à la topologie logique, représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token Ring et FDDI.

- **Topologie Ethernet :** Ethernet est aujourd'hui l'une des technologies le plus utilisées en local. Il repose sur une topologie physique de type bus linéaire, c'est-à-dire tous les ordinateurs sont reliés à un seul support de transmission. Dans un réseau Ethernet, la communication se fait à l'aide d'un protocole appelé CSMA/CD (Courrier Sense Multiple Access With collision Detection).

- **Le Token Ring :** Token Ring repose sur une topologie en anneau (ring**)**. Il utilise la méthode d'accès par jeton (token). Dans cette technologie, seul le poste ayant le jeton a le droit de transmettre. Si un poste veut émettre, il doit attendre jusqu'à a ce qu'il ait le jeton. Dans un réseau Token Ring, Chaque nœud du réseau comprend un MAU (Multi station Access Unit) qui peut recevoir les connexions des postes. Le signal qui circule est régénéré par chaque MAU.

  Mettre en place un réseau Token Ring coûte cher, et la panne d'une station MAU provoque le disfonctionnement du réseau.
- **Le FDDI :** La technologie LANFDDI (Fibre Distributed Data Interface) est une technologie d'accès réseau utilisant des câbles fibres optiques. Le FDDI est constitué de deux anneaux : un anneau primaire et un anneau secondaire, L'anneau secondaire sert à rattraper les erreurs de l'anneau primaire.

  Le FDDI utilise un anneau à jeton qui sert à détecter et à corriger les erreurs. Ce qui fait que si une station MAU tombe en panne, le réseau continuera de fonctionner.
- **L'ATM :** L'ATM (asynchronous Transfer Mode, c'est-à-dire mode de transfert asynchrone) est une technologie très récente qu'Ethernet, Token et FDDI, Il s'agit d'un protocole de niveau 2, qui a pour objectif de segmenter les données en cellules de taille unique.

  L'en-tête de chaque cellule comprend des informations qui permettent à la cellule d'emprunter son chemin. Les cellules ATM sont envoyées de manière asynchrone, en fonction des données à transmettre, mais sont insérées dans le flux de données synchrones d'un protocole de niveau inférieur pour leur transport.

I.5 Architecture des réseaux

I.5.1 Architecture du réseau poste à poste

Dans le cas où tous les postes ont un rôle identique et sont à la fois clients pour des ressources et serveurs pour d'autres, on parle de réseau d'égale à égale, de paire à paire ou encore de poste à poste.

Dans le réseau poste à poste, chaque utilisateur administre son propre poste. D'autre part, tous les utilisateurs peuvent partager leur ressource comme ils le souhaitent.

I.5.2 Architecture d'un réseau client/serveur

De nombreuse applications fonctionnent selon client/ serveur, cela signifie que des machines clientes (des machines faisant partie du réseau) contactent un serveur, une machine généralement très puissante en terme de capacité d'entrée - sortie, qui leur fournit des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion.

I.6 Les constituants matériels d'un réseau informatique

Les éléments matériels qui permettent d'interconnecter les ordinateurs dans un réseau, sont les suivants :

I.6.1 La carte réseau

C'est une interface qui permet de connecter un ordinateur au support de transmission utilisé par le réseau. Chaque carte réseau possède une adresse exclusive. Elle sert à identifier la carte réseau lorsque les informations sont envoyées ou reçues au sein du réseau. Une fois installée dans un ordinateur, la carte réseau permet à ce dernier de faire partie d'un réseau.

I.6.2 Transceiver

Il permet d'assurer la transmission des signaux circulant sur le support physique, aussi bien à l'émission qu'à la réception.

I.6.3 Les équipement de transmission

Les équipements de transmission sont des supports (canaux physique) d'interconnexion, qui relient les ordinateurs entre eux pour construire un réseau. Ils sont généralement filaires, de plus en plus non filaires.

Avant d'opter pour un type de support de transmission, afin de créer ou d'étendre un réseau, il convient de prendre en considération un certains nombre de facteurs qui sont :

- **Le coût :** le coût du support de transmission influe grandement sur le coût total d'un réseau.
- **L'extensibilité :** il est important qu'un réseau puisse être agrandi pour admettre de nouveau utilisateurs et matériels.
- **La détérioration du signal :** Plus le signal parcourt une distance importante, plus il devient faible, car chaque support permet de transmettre des signaux sur une certaine distance.
- **Support physique d'interconnexion :** C'est le support permettant de relier les ordinateurs entre eux. Les principaux supports physiques utilisés dans les réseaux locaux sont les suivants :

  - Le câble coaxial : c'est un câble électrique (cuivre) blindé coaxial ex : câbles TV. Malgré de bonnes qualités intrinsèques (faible sensibilité aux perturbations électromagnétiques), les câbles coaxiaux sont de moins en moins utilisés et laissent de plus en plus la main aux paires torsadées.

  - La paire torsadée : Les câbles électriques (cuivre) à paires torsadées, ressemblent aux câbles téléphoniques. Les torsades diminuent la sensibilité aux perturbations électromagnétiques, la diaphonie (mélange de signaux entre paires) et l'atténuation du signal tout au long du câble. Il existe des versions blindées (STP Shielded Twisted Pair) Et non blindées (UTP Unshielded Twisted Pair). Les Câbles à paires torsadées sont actuellement les plus utilisés.

  - La fibre optique : Les câbles à fibres optiques transmettent les informations par modulation d'un faisceau lumineux. Ils sont composé d'une fibre de réception.
  - Support hertzien (onde électromagnétique) : Les communications par faisceaux hertziens se font en ligne directe de la tour d'émission à la tour de réception et ont un rayonnement très directif. Ce type de transmission permet le multiplexage de nombreux canaux de communication autorisant ainsi un très bon débit de données.

I.7 Les outils d'interconnexion

Des équipements spécifiques sont nécessaires pour assurer la communication et l'interconnexion. Ces principaux équipements sont :

- **Répéteur :** C'est un équipement permettant de régénérer le signal entre deux nœuds de réseau, il permet de prolonger facilement un support de transmission existant et d'interconnecter deux segments d'un même réseau.
- **Hub (concentrateur) :** C'est un boitier qui a la fonction de récepteur, mais sa fonction principale est de pouvoir connecter plusieurs lignes. Il sert d'emplacement central pour relier les ordinateurs et autres périphériques. Le concentrateur dispose d'un certain nombre de ports auxquels viennent se connecter les PC clients. On utilise quelque fois le terme de répéteur multi port car il transfère ou renvoient tous les paquets qu'il reçoit à tous ses ports. Les concentrateurs n'effectuent aucun contrôle ou filtrage de données qui les traversent.
- **Pont (bridge) :** C'est un dispositif matériel ou logiciel permettant de relier des réseaux travaillant avec les mêmes protocoles. Il permet aux différentes parties d'un réseau d'échanger et de filtrer des informations, la connexion des réseaux similaires et la création d'inter-réseaux.
- **Switch :** Aussi appelé commutateur, en général, les stations de travail d'un réseau Ethernet sont toutes connectées directement à lui. Un commutateur relie les hôtes qui y sont connectés en lisant leurs adresses MAC comprise dans les trames. Intervenant au niveau de la couche 2, il ouvre un circuit virtuel unique entre les nœuds d'origine et de destination, ce qui limite la communication à ces deux ports sans affecter le trafic des autres ports.
- **Routeur :** Aussi appelé commutateur de niveau 3 car il effectue le routage et l'adressage, il permet d'interconnecter deux ou plusieurs réseaux. Possédant les mêmes composants de base qu'un ordinateur, le routeur sélectionne le chemin approprié (au travers de la table de routage) pour diriger les messages vers leurs destinations. Cet équipement est qualifié de fiable car il permet de choisir une autre

route en cas de défaillance d'un lien ou d'un routeur sur le trajet qu'empreinte un paquet.

- **Passerelle(Gateway) :** Système logiciel et/ou matériel gérant le passage d'un environnement réseau à un autre, en assurant la conversion des données d'un à format un autre, en assurant la conversion des données d'un format à un autre.
  La passerelle peut se présenter sous la forme d'un connecteur physique au réseau et être utilisée comme une interface pour transférer les informations entre les différents réseaux. Elle peut également se présenter sous forme d'un logiciel conçu pour permettre à deux protocoles différents d'échanger des informations.

- **MODEM (Modulateur-DEModulateur) :** Est le périphérique utilisé pour transférer des informations entre plusieurs ordinateurs via les lignes téléphoniques. Le modem module les informations numériques en ondes analogiques, en sens inverse il retranscrit les données sous forme analogique en données numériques.

I.8 Les modèles de références

Dans le monde des réseaux informatique, il existe deux modèles de référence :

I.8.1 Le modèle OSI

Un aspect important dans l'ouverture des réseaux a été la mise en place d'un modèle de référence, le modèle OSI de l'ISO. Celui-ci définit un modèle de sept couches réseaux, Présente sur chaque station qui désire transmettre. Chaque couche dispose de fonctionnalités qui lui sont propres et fournit des services aux couches immédiatement adjacentes. Même si le modèle OSI est très peu implémenté, il sert toujours de référence pour identifier le niveau de fonctionnement d'un composant réseau.

I.8.1.1 Principes

L'organisme ISO a défini en 1984 un modèle de référence, nommé Open System Interconnection (OSI) destiné à normaliser les échanges entre deux machines. Il définit ce que doit être une communication réseau complète. L'ensemble du processus est ainsi découpé en sept couches hiérarchiques.

Ce modèle définit précisément les fonctions associées à chaque couche. Chacune d'entre elles se comporte comme un prestataire de service pour la couche immédiatement supérieur. Pour qu'une couche puisse envoyer une commande ou des données au niveau équivalant du correspondant, elle doit constituer une information et lui faire traverser toutes les couches inferieurs, chacune d'elles ajoutant un en-tête spécifique à ce qui devient une sorte de train. à l'arrivés, cette information est décodée, la commande ou les données sont libérées.

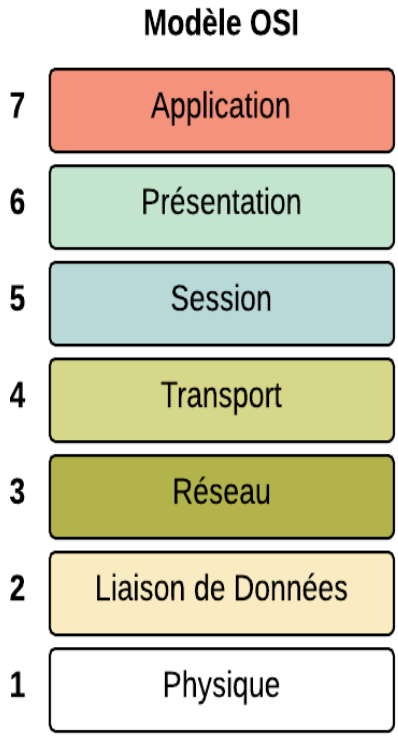

Figure I.4 : représentation de modèle OSI.

I.8.1.2 Rôle des différentes couches

Chaque couche réseau définie par le modèle a un rôle bien précis, qui va du transport du signal codant les données à la présentation des informations pour l'application destinataire.

- **Physique :** La couche physique gère la communication avec l'interface physique afin de faire transiter ou de récupérer les données sur le support de transmission, qui peut être électronique, mécanique, fonctionnel ou procédural.

Ce sont les contraintes matérielles du support utilisé qui décident des objectifs à atteindre pour cette couche : conversion en signaux électriques, taille et forme de connecteurs, dimensions et position des antennes, etc.

- **Liaison de données :** La couche liaison s'occupe de la bonne transmission de l'information entre les nœuds via le support, en assurant la gestion des erreurs de transmission et la synchronisation des données, Là aussi, le support de transmission conditionne les protocoles à mettre en œuvre.
- **Réseau :** La couche réseau a en charge de déterminer le choix de la route entre les nœuds afin de transmettre de manière indépendante l'information ou les différents paquets la constituant en prenant en compte en temps réel le trafic. Cette couche assure aussi un certain nombre de contrôles de congestion qui ne sont pas gérés par la couche liaison.
- **Transport :** La couche transport supervise le découpage et réassemblage de l'information en paquets, contrôlant ainsi la cohérence de la transmission de l'information de l'émetteur vers le destinataire.
- **Session :** La couche session gère une communication complète entre plusieurs nœuds, permettant ainsi d'établir et de maintenir un réel dialogue, pouvant être constitué de temps mort pendant lesquels aucune donnée n'est physiquement transmise.
- **Présentation :** La couche présentation a en charge la représentation des données, c'est-à-dire de structurer et convertir les données échangées ainsi que leur syntaxe afin d'assurer la communication entre des nœuds différents.
- **Application :** La couche application est le point d'accès des applications aux services réseaux. On y retrouve toutes les applications de communication via le réseau communément utilisée sur un LAN ou sur une application interne (applications de transfert de fichiers, courrier électronique, etc.).

I.8.2 Le modèle TCP/IP

TCP diffère fortement du modèle OSI, non seulement par le nombre de couches, mais aussi par l'approche. Le modèle OSI spécifie des services (approche formaliste), TCP/IP des protocoles (approche pragmatique). Développé au-dessus d'un environnement existant,

TCP/IP ne décrit, à l'origine, ni de couche physique ni de couche liaison de données. Les applications s'appuient directement sur le service de transport. L'architecture TCP/IP ne comprend que 2 couches : la couche transport (TCP) et la couche inter réseau (IP). La figure 5 compare les deux architectures.

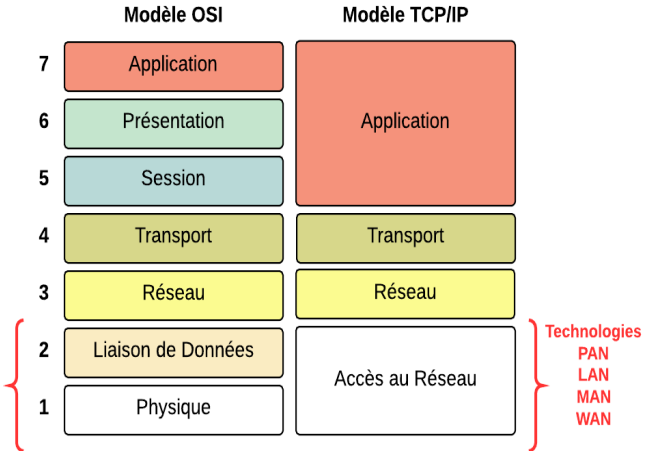

Figure I.5 : l'architecture en couche de modèle TCP/IP.

I.8.2.1 IP (Internet Protocol)

IP est un protocole qui se charge de l'acheminement des paquets pour tous les autres protocoles de la famille TCP/IP. Il fournit un système de remise de données optimisées sans connexion. Le terme « optimisé » souligne le fait qu'il ne garantit pas que les paquets transportés parviennent à leur destination, ni qu'ils soient reçus dans leur ordre d'envoi. Ainsi, seuls les protocoles de niveau supérieur sont responsables des données contenues dans les paquets IP et de leur ordre de réception.

Le protocole IP travaille en mode non connecté, c'est-à-dire que les paquets émis sont acheminés de manière autonome (datagrammes), sans garantie de livraison.

I.8.2.2 TCP (Transmission Control Protocol)

TCP est le protocole IP de niveau supérieur. Il fournit un service sécurisé de remise des paquets. TCP fournit un protocole fiable, orienté connexion**,** au-dessus d'IP (ou encapsulé à

l'intérieur d'IP). TCP garantit l'ordre et la remise des paquets, il vérifie l'intégrité de l'en-tête des paquets et des données qu'ils contiennent. TCP est responsable de la retransmission des paquets altérés ou perdus par le réseau lors de leur transmission. Cette fiabilité fait de TCP/IP un protocole bien adapté pour la transmission de données basées sur la session, les applications client-serveur et les services critiques tels que le courrier électronique.

La fiabilité de TCP a son prix. Les en-têtes TCP requièrent l'utilisation de bits supplémentaires pour effectuer correctement la mise en séquence des informations, ainsi qu'un total de contrôle obligatoire pour assurer la fiabilité non seulement de l'en-tête TCP, mais aussi des données contenues dans le paquet. Pour garantir la réussite de la livraison des données, ce protocole exige également que le destinataire accuse la réception des données**.**

Ces accusés de réception (ACK) génèrent une activité réseau supplémentaire qui diminue le débit de la transmission des données au profit de la fiabilité. Pour limiter l'impact de cette contrainte sur la performance, la plupart des hôtes n'envoient un accusé de réception que pour un segment sur deux ou lorsque le délai imparti pour un ACK expire.

Sur une connexion TCP entre deux machines du réseau, les messages (ou paquets TCP) sont acquittés et délivrés en séquence.

I.8.3 Description des couches TCP/IP

Les couches du modèle TCP/IP sont plus générales que celles du modèle OSI et elles sont comme suit :

I.8.3.1 Couche application

La Couche Application reprend les applications standards en réseau informatique et Internet et dispose des protocoles suivants : SMTP (Simple Mail Transport Protocol), POP (Post Office Protocol), TELNET (Telecommunication Network), FTP (File Transfert Protocol).

I.8.3.2 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.

I.8.3.3 Couche Internet

La couche Internet est chargée de fournir le paquet des données. Elle définit les datagrammes et gère la décomposition / recomposition des segments. La couche Internet utilise Cinque protocoles suivants : IP (Internet Protocol), ARP (Adresse Resolution Protocol), ICMP (Internet Control Message Protocol), RARP (Reverse Address Resolution Protocol), IGMP (Internet Group Management Protocol).

I.8.3.4 Couche Accès 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.

Conclusion

Ce chapitre nous a permis de découvrir et de mieux comprendre les notions et les aspects élémentaires des réseaux informatiques à savoir leurs équipements de transmission, leurs outils d'interconnexion, les réseaux locaux, ainsi il nous a permis de différencier entre le modèle OSI qui présente un standard de communication entre les ordinateurs d'un réseau et le modèle TCP/IP qui est un ensemble de communication.

Dans le chapitre qui suit on va parler sur la sécurité des réseaux informatique.

CHAPITRE II

Généralité sur la sécurité informatique

Introduction

L'univers des systèmes d'information composé de réseaux et de systèmes informatiques prend un rôle et une place chaque jour plus importante dans les entreprises.

Cependant, l'actualité présentée par les médias nous démontre que le système d'information est vulnérable et qu'il peut subir des piratages, des attaques (virus, hackers…), des pertes de données, des sinistres. Il est donc indispensable pour les entreprises de savoir définir et de garantir la sécurité de ses ressources informatiques.

Nous entamerons ce chapitre par une définition et une exposition des objectifs de la sécurité informatique, nous parlerons ensuite des différentes menaces, vulnérabilités et attaques qui pèsent sur les réseaux, et enfin, nous bouclerons ce chapitre par une présentation des différents mécanismes de défense et de sécurité tels que les pare-feux, les DMZ et les VLANs.

II.1 Définition

Stéphane Natkin[1] a défini la sécurité informatique comme étant un ensemble de moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces

[1] Stéphane Natkin est professeur titulaire de la chaire Systèmes Multimédia au département STIC du Conservatoire National des Arts et Métier. Il est le directeur du laboratoire de recherche en Informatique du CNAM, le CEDRIC. Il enseigne la les réseaux et systèmes répartis, la sûreté et la sécurité des systèmes complexes et est l'auteur de plusieurs ouvrages

accidentelles (accidents dus à l'environnement, les défauts du système) ou intentionnelles (actions malveillantes intentionnelles) pour éviter les erreurs, afin d'assurer le bon fonctionnement de tel système [1].

Géraldine Vache-Marconato l'a définie comme étant un terme large qui réunit les moyens humains, techniques, organisationnels et juridiques qui tentent de garantir certaines propriétés d'un système d'information.

II.2 Objectifs de la sécurité

La sécurité des données couvre quatre objectifs principaux que nous allons citées ci-dessous [2]:

- **L'intégrité** est la certitude de la présence non modifiée ou non altéré d'une information et de la complétude des processus de traitement. Pour les messages échangés, il concerne la protection contre l'altération accidentelle ou volontaire d'un message transmis.
- **La confidentialité** est l'assurance que l'information n'est accessible qu'aux personnes autorisées, qu'elle ne sera pas divulguée en dehors d'un environnement spécifié. Elle traite de la protection contre la consultation de données stockées ou échangées.
- **L'authentification** est le moyen qui permet d'établir la validité de la requête émise pour accéder à un système. L'authenticité est la combinaison d'une authentification et de l'intégrité.
- **La non-répudiation** est considérée comme un service de sécurité pouvant être rendu par un mécanisme comme la signature numérique, l'intégrité des données ou la notarisation. l'élément de la preuve de non-répudiation doit permettre l'identification de celui qu'il représente, il doit être positionné dans le temps (horodatage), il doit présenter l'état du contexte dans lequel il a été élaboré (certificat).

D'autres principes de sécurité peuvent être établis, il s'agit de :

- La disponibilité est l'assurance que les personnes autorisées ont accès à l'information quand elles le demandent ou dans les temps requis pour son traitement.
- La preuve consiste à garantir que l'émetteur d'une information soit bien identifié et qu'il a les droits et les accès logiques, que le récepteur identifié est bien autorisé à accéder à l'information.

II.3 menaces sur les réseaux

II.3.1 Les vulnérabilités

Pour le domaine de la sécurité informatique, il existe trois familles de vulnérabilités [2]:

- **Vulnérabilités liées aux domaines physiques :** elle résulte souvent d'un manque de redondance et de ressource au niveau équipement, d'un accès aux salles informatiques non sécurisé ou bien d'une absence de stratégie de sauvegarde.
- **Vulnérabilités liées aux domines organisationnels :**
  -manque de personnels qualifiés et de communication.
  -absence de contrôle périodique et de moyens adaptés aux risques encourus.
- **Vulnérabilités liées aux domaines technologiques :**
  -failles nombreuses dans les services et applicatifs Web et les bases de données.
  -réseaux complexes, non protégés, mal organisés, non redondants.
  -récurrence des failles et absences de supervision des événements.
  -absence de contrôle suffisant sur les logiciels malveillants.

II.3.2 Les menaces et leur impacts

Les systèmes d'information sont vulnérables par rapport à plusieurs menaces susceptibles de leur infliger différents types de dommages et de pertes significatives. L'importance des dégâts peut s'échelonner de la simple altération de données à la destruction complète de centres informatiques.

Les impacts des différentes menaces varient considérablement suivant les conséquences affectant l'entreprise, certains affectent la confidentialité ou l'intégrité des données, d'autres agissent sur la disponibilité des systèmes [2].

Les menaces les plus communes sont décrites ci-dessous [2]:

- **Erreur et omissions :** ce sont des menaces importantes pour l'intégrité des données et des systèmes ces erreur sont souvent d'origine humaine. En effet, même les programmes les plus sophistiqués ne peuvent pas tout détecter. N'importe quelle personnes intervenant sur le système d'information contribue directement ou indirectement a ces dangers mettant en péril la sécurité des systèmes.
- **Fraude et vol :** les fraudes ou vols peuvent être commis par l'intérieur ou l'extérieur de l'entreprise. Par expérience, il s'avère, la plupart du temps, que la menace vient de l'intérieur (des utilisateurs ayant des accès privilégiés aux systèmes).
- **Hackers :** le terme **hacker** fait référence à la personne qui s'introduit dans les systèmes d'information sans autorisation pour, dans le pire des cas, provoquer des dégradations dans les données ou les applications. Ses actions peuvent s'effectuer à partir de l'intérieur (dans le cas ou il a pu obtenir un accès sur le réseau) ou de l'extérieur de l'entreprise.
- **Espionnage industriel ou commercial :** appelé **Social Engineering**, il consiste à récupérer des données confidentielles de l'entreprise dans le cas de concurrence économique ou industrielle. Cette menace n'implique pas, en général, d'altération des données internes. Par contre, elle peut avoir un impact important sur les actifs sensibles de l'entreprise (données client, brevets industriels…).
- **Programmes malveillants :** ils font référence aux virus, chevaux de Troie, bombe logique et autres logiciels indésirables. Souvent, leur point d'entrée se situe au niveau des ordinateurs personnels mal protégés lors de leur connexion sur internet. Leurs effets peuvent s'étendre à tout le réseau de l'entreprise en contaminant d'autres matériels.

II.3.3 Les attaques

II.3.3.1 définition

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées, à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques (hackers ou biens crackers).

En d'autre terme, une attaque est l'exploitation d'une vulnérabilité d'un système informatique par des actions qui sont soit accidentelles, malveillantes ou intentionnelles [1].

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

- **Attaques passives :** consiste à écouter et à analyser le trafic échangé sans modifier les données ou le fonctionnement du réseau. Elles sont généralement indétectables mais leur prévention est possible.
- **Attaque actives :** les attaques actives concernent celles qui entraînent une modification des données ou création de données incorrectes. Autrement dit, celles qui portent atteinte à l'intégrité, l'authenticité et la disponibilité.

II.3.3.2 quelques techniques d'attaque

Les attaques réseau sont aujourd'hui si nombreuses qu'il serait imaginaire de prétendre les décrire toutes. Elles touchent généralement les trois composante d'un système : la couche réseau, le système d'exploitation et la couche application, pourvu qu'il existe une vulnérabilité exploitable. Voici les attaques les plus utilisées [3] :

- **Le Flooding** consiste à envoyer à une machine de nombreux paquets IP de grosse taille, la machine cible ne pourra donc pas traiter tous les paquets et finira par se déconnecter du réseau.
- **Le smurf** est une attaque qui s'appuie sur le ping (Packet Internet Groper) et les serveurs de broadcaste. On falsifie d'abord son adresse IP pour se faire passer pour la machine cible. On envoie alors un ping sur un serveur de broadcaste. Il le fera suivre à toutes les machines qui sont connectées qui renverront chacun un « pong » au

serveur qui fera suivre à la machine cible. Celle-ci sera alors inondée sous les paquets et finira par se déconnecter.

- **Man-in-The-middle** consiste à faire passer les échanges réseaux entre deux systèmes par le biais d'un troisième, sous le contrôle du pirate. Ce dernier peut transformer à sa guise les données à la volée, tout en masquant parfaitement à chaque acteur de l'échange la réalité de son interlocuteur.
- **Le craquage de mots de passe** consiste à faire de nombreux essais pour trouver le bon mot de passe, soit en essayant toutes les possibilités qui sont faites dans l'ordre pour trouver la bonne solution (la méthode brute), soit en testant un mot pris dans une liste prédéfinie contenant les mots de passe les plus courants et aussi des variantes de ceux-ci.

II.4 Les mécanismes de défense et de sécurité

La mise en œuvre des mesures de sécurité consiste à déployer des moyens et des dispositifs visant à sécuriser le système d'information ainsi que de faire appliquer les règles définies dans la politique de sécurité. De nombreux mécanismes ont été développés pour assurer la sécurité, qu'il est souvent indispensable de combiner pour atteindre un niveau de sécurité suffisant.

II.4.1 Firewalls (pare-feux)

II.4.1.1 Définition

Un pare-feu est un élément du réseau informatique, logiciel et/ou matériel, qui est aujourd'hui incontournable dans la sécurité de tout système informatique car il permet de protéger le réseau des intrusions extérieures. Ces dispositifs filtrent les trames (contenant des données) des différentes couches du modèle TCP/IP afin de contrôler leur flux et de les bloquer en cas d'attaques, celles-ci pouvant prendre plusieurs formes.

Le filtrage réalisé par le pare-feu constitue le premier rempart de la protection du système d'information. Il est installé le plus souvent en périphérie du réseau local de l'entreprise ce qui lui permet de contrôler l'accès des ressources externes vers l'intérieur mais également entre entités éloignés de l'entreprise mais reliées par un réseau de type extranet.

Leur utilisation permet de contrôler la connectivité des communications, une entreprise peut empêcher des accès non autorisés aux ressources et systèmes de son réseau local et plus précisément pour ses environnements les plus sensibles [2].

II.4.1.2 Principe de fonctionnement

- **Le filtrage statique :** c'est le filtrage le plus simple. Un pare-feu qui fonctionne selon ce mode de filtrage inspecte les entêtes de chaque paquet qui le traverse et décide selon la politique de sécurité de le laisser passer ou de le supprimer et ce sans tenir compte des autres paquets.
- **Le filtrage applicatif :** Cette technique a été proposée pour palier à certaines limites de pare-feux utilisant le filtrage simple. L'idée est de conserver les traces de sessions et de connexions dans les tables d'états internes aux pare-feux. Ces traces seront également prises en considération par les pare-feux lors de prises de décisions. Ces informations augmentent considérablement les capacités des pare-feux à détecter des attaques sophistiquées.
- **Le filtrage dynamique :** Un firewall effectuant un filtrage applicatif est appelé généralement passerelle applicative ou proxy. Le serveur Proxy permet de faire le relais au niveau des applications pour rendre les machines internes invisible à l'extérieur. Il permet la destruction des en-têtes précédant le message applicatif ce qui fournit un niveau de sécurité supplémentaire. La plupart du temps le serveur proxy est utilisé pour le web, il s'agit donc d'un proxy http, toutefois il peut exister des serveurs proxy pour chaque protocole applicatif.

II.4.2 La DMZ

La DMZ (DeMilitarized Zone) est un environnement de sous-réseau positionné entre un réseau interne de confiance et un réseau externe non sécurisé.les serveurs installés dans la partie externe de la DMZ permettent de fournir des services aux réseaux externes, tout en protégeant le réseau interne contre des intrusions possibles.

La figure ci-après montre l'exemple d'un environnement composé d'une DMZ interne et externe avec plusieurs serveurs et des périphériques de détection d'intrusion. Dans cet exemple, le serveur VPN est combiné avec le pare-feu principal. Les autres serveurs accessibles de l'extérieur sont positionnés aussi sur la DMZ externe. Tous les autres serveurs internes sont situés dans la DMZ interne, protégés à la fois des menaces internes et externes [2].

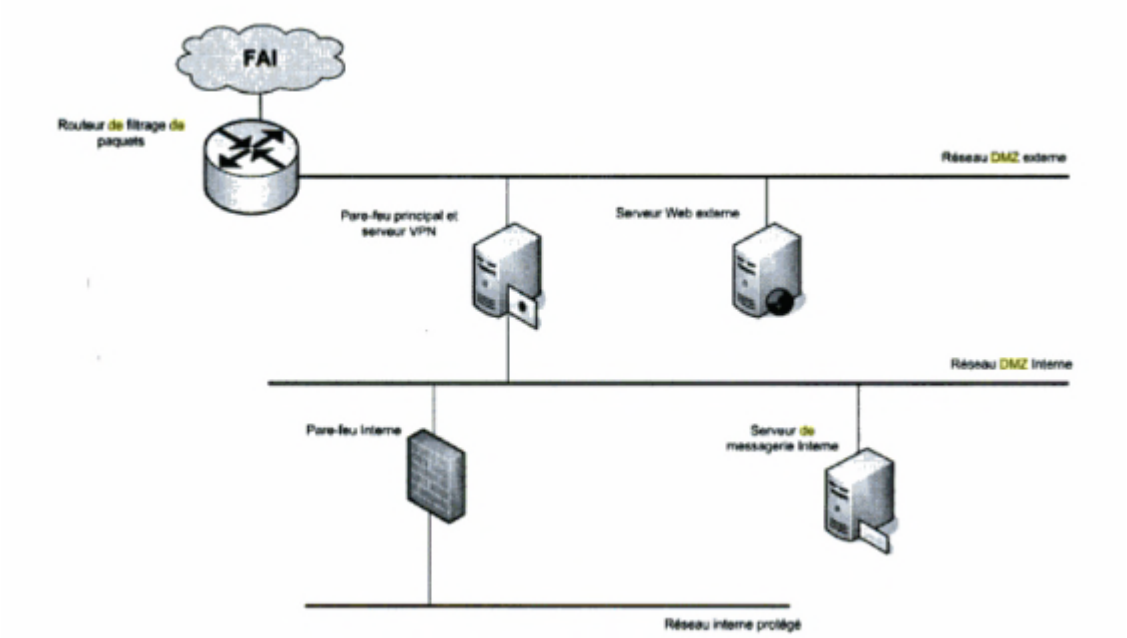

Figure II.1: exemple d'environnement de DMZ

II.4.3 La technologie AAA

Nous vivons dans un monde ou presque tout doit être protégé. Que vous soyez administrateur système, responsable, ingénieur réseau ou étudiant. Lorsque nous accédons à un réseau, nous sommes toujours confrontés aux trois aspects [4]:

- **Authentification :** il s'agit de la vérification de l'identité d'un utilisateur, elle est généralement assuré au moyen d'un secret partagé ou d'un logiciel approuvé.
- **Autorisation :** elle intervient à l'issue de l'authentification. Une fois l'utilisateur authentifié, il faut s'assurer qu'il est autorisé à accomplir les actions qu'il demande,

tels que l'accès à des fichiers, le droit d'écrire, etc. l'autorisation est gérée au moyen de liste ACL ou de stratégie

- **Traçabilité :** elle permet de collecter des informations sur les utilisateurs et les actions qu'ils accomplissent lorsqu'ils sont connectés aux équipements du réseau.

II.4.4 Système de détection d'intrusion (IDS)

Les outils de détection d'intrusion viennent compléter les fonctions du pare-feu. Au travers d'une surveillance de l'identité des requêtes en circulation sur le réseau, ces outils sont à même de repérer les requêtes malintentionnées, de repérer les intrus dans le flot du trafic courant transitant par les ports de communication laissés ouverts par le pare-feu.

Les systèmes de détection sont conçus pour informer des accès non autorisés ou des intrusions dans les réseaux. Les pare-feux qui opèrent avec les systèmes de détection d'intrusion sont capable de détecter automatiquement les menaces venant de l'extérieur, plus rapidement qu'une vérification par un opérateur.

Il existe deux types de détection d'intrusion :

- Le premier système, basé sur l'hôte, doit être installé sur chaque machine à protéger. Il est, en général, intégré au système d'exploitation qu'il protège. Ce types d'IDS sont prévus pour la détection des menaces à un haut niveau de sécurité.

- Le premier système, basé sur le réseau, est implémenté en tant qu'analyseur intelligent de protocole. Ses composants surveillent le trafic réseau au niveau physique [2].

II.4.5 Les réseaux privés virtuels (VPN)

II.4.5.1 Définition

Les VPNs est une technique permettant à un ou plusieurs poste distant de communiquer de manière sur, tout en empruntant les infrastructures publiques, ce type de liaison est apparu suite à un besoin croissant des entreprises de relier les différents sites et ce de façon simple et économique.

En d'autre terme, c'est un tunnel sécurisé permettent la communication entre deux entités y compris au travers des réseaux peu surs comme peut l'être le réseau Internet. L es VPNs ont pour objectif de contribuer à la sécurisation des échanges de données privées, sensible sur les réseaux publics [5].

II.4.5.2 Principe de fonctionnement

Un VPN fonctionne selon un système de tunnelisation privé, c'est-à-dire qu'un tunnel est créé, à l'intérieur duquel transitent toute la communication et ou toutes les données transmises qui sont cryptées. Un VPN est très fermé, un utilisateur non autorisé, ne peut en aucun cas avoir accès aux données transmises sur le réseau et en cas d'interceptions, les informations interceptées sont cryptées, illisibles, et donc inutilisables.

Le fonctionnement des VPN repose sur des technologies appelées protocoles de tunnelisation ou protocoles VPN. Ce sont ces protocoles qui sécurisent les données au moyen d'algorithmes de cryptographie, et qui leurs permettent de circuler en toute sécurité d'un bout à l'autre [6].

II.4.5.3Les types de VPNS [7]

On peut dénombrer trois types de VPN, chacun d'eux caractérise une utilisation bien particulière de cette technologie :

- **VPN d'accès :** il permet à un utilisateur isolé de se connecter dans un réseau local interne. De ce cas, il peut avoir son propre client VPN afin de se connecter directement au réseau.

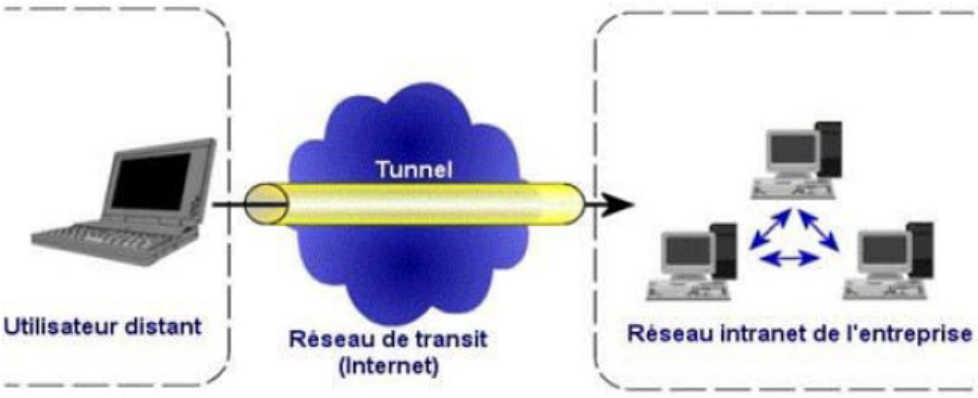

Figure II.2: VPN d'accès

- **Intranet VPN :** est utilisé pour relier deux ou plusieurs intranet d'une même entreprise entre eux. ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants.

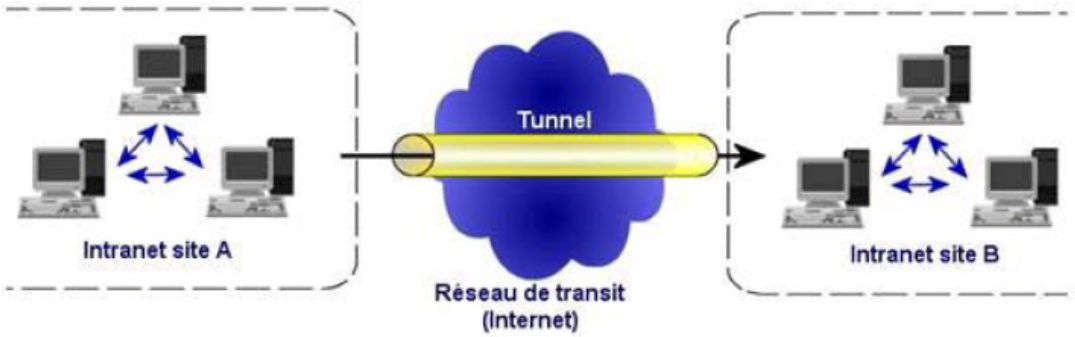

Figure II.3: Intranet VPN

- **Extranet VPN :** une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans ce cas, il nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès.

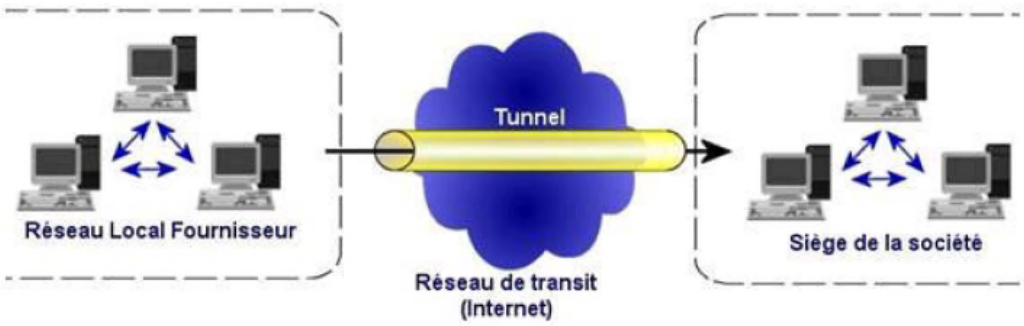

Figure II.4: Extranet VPN

II.4.5.4 Les différents protocoles utilisés dans les VPNs

Les protocoles utilisés dans le cadre d'un réseau privé virtuel sont deux types, suivant le niveau de la couche (PPTP, L2TP et L2F pour le niveau 2, IP Sec pour le niveau)

- **Point-to-Point Protocol :** Ce protocole n'est pas un protocole sécurisé mais sert de support aux protocoles PPTP ou L2TP, il permet de transférer des données sur un lien synchrone ou asynchrone. Il full duplex et garantit l'ordre d'arrivée des paquets.
- **Point-to-point Tunneling Protocol :** PPTP est le protocole standard pour créer des VPN sous Windows. Il encapsule les paquets dans PPP, lui-même encapsulé dans du GRE (Generic Routing Encapsulation). PPTP permet à PPP d'être transporté dans un tunnel au travers d'un réseau IP mais n'apporte aucun changement au protocole PPP.
- **Layer 2 Forwarding :** Ce protocole est développé par CISCO, Northen Telecom et Shiva. Il permet à un serveur d'accès distant de véhiculer le trafic sur PPP et transférer ces données jusqu'à un serveur L2F (routeur). Le serveur L2F désencapsule les paquets et envois sur le réseau. L2F est progressivement remplacé par L2TP qui est plus souple.
- **Layers 2 Tunneling protocol** : crée par CISCO et Microsoft, il réunit les avantages de PPTP et L2F. ce protocole réseau encapsule des trames PPP pour les envoyer sur des réseaux IP, X25, WAN (relais de trames) ou ATM. Lorsqu'il est configuré pour transporter les données sur IP, L2TP peut être utilisé pour faire du tunnelling sur Internet.
- **Internet Protocol Security** : Aujourd'hui, le protocole le plus utilisé pour la mise en place des VPNs.il est l'un des standards les plus diffusés et les plus ouverts. Effectivement, IP Sec offre plusieurs services : le chiffrement, le contrôle de l'intégrité et l'authentification. De plus, il est nativement implémenté dans IPv6 qui le rend par conséquent le protocole incontournable pour les communications sécurisées dans les années à venir.

II.4.6 Les VLANs

Dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographique, contraintes d'adressages,

…) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéro de port, protocole, etc.).

II.4.6.1 Définition

Les réseaux virtuels (VLAN) sont apparus comme une nouvelle fonctionnalité dans l'administration réseau avec le développement des commutateurs. La notion de VLAN est un concept qui permet de réaliser des réseaux de façon indépendante du système de câblage. Ces réseaux permettent de définir des domaines de diffusions restreints, cela signifie qu'un message émis par une station du VLAN ne pourra être reçu que par les stations de ce même VLAN [8]**.** Cette technologie apporte des solutions nouvelles dans la segmentation et la sécurisation des réseaux locaux. Les VLAN ont été uniformisés conformément a la spécification IEEE 802.Q1. Il subsiste cependant des variantes d'implémentation d'un constructeur à l'autre [9].

II.4.6.2 typologies des VLANs

Les VLANS différent selon les informations utilisées pour regrouper les stations. Il en existe trois modèles [10]:

- **VLAN par port :** dans ce modèle chaque port d'un commutateur est attribué à un VLAN. Toutes les stations connectées à un port appartiennent au VLAN correspondant. Lorsqu'une station est déplacée sur un autre port, celui-ci est également attribué au VLAN de la station. De même, si une situation change de VLAN, le port auquel elle est connectée est attribué à son nouveau VLAN. Ce type est facile à mettre en place et offrent une bonne flexibilité en utilisant le protocole DHCP cependant tout déplacement d'une station nécessite une reconfiguration des ports (manque de souplesse).
- **VLAN par adresse MAC :** c'est un VLAN de niveau 2 qui est constitué en associant les adresses MAC des stations à chaque VLAN. Les VLANS de niveau 2 permettent une sécurité au niveau de l'adresse MAC, c'est-à-dire qu'un pirate souhaitant se connecter sur le VLAN devra au préalable récupérer une adresse MAC du VLAN pour

pouvoir entrer mais l'inconvénient est la nécessité de maintenir à jour l base e données des adresses MAC ainsi que les performances sont ralenti du a l'échange des tables d'adressage MAC entre les commutateurs.

- **VLAN par protocole :** ou VLAN de niveau 3, est obtenu en associant un réseau virtuel par type de protocole du réseau. On peut ainsi constituer un réseau virtuel pour les stations communiquant avec le protocole TCP/IP, et un autre pour les stations communiquant avec le protocole IPX.
- **VLAN par sous-réseau :** il utilise les adresses IP. Un réseau virtuel est associés à chaque sous réseau IP. Dans ce cas, les commutateurs apprennent aussi la configuration et il est possible de changer à une station de place sans reconfigurer le VLAN. Par contre, il souffre de lenteur par rapport au VLAN de niveau 1 et 2.

II.4.6.3 Les avantages des VLANs

Les VLANs présentent de nombreux avantages pour l'optimisation des réseaux et leur sécurité parmi eux [11]:

- **Renforcement de la sécurité du réseau :** les frontières virtuelles créées par les VLANs ne pouvant être franchies que par le biais de fonctionnalités de routage, la sécurité des communications est renforcées ;
- **Meilleur utilisation des serveurs réseaux** : quand un serveur possède une infrastructure compatible avec les VLANs, le serveur peut appartenir à plusieurs VLAN en même temps, ce qui permet de réduire le trafic qui doit être routé ;
- **Augmentation considérable des performances du réseau** : comme le trafic réseau d'un groupe d'utilisateurs est confiné au sein du VLAN lui est associé, de la bande passante est libérée, ceci augmente la performance du réseau ;
- **Simplification de la gestion** : l'ajout de nouveaux éléments ou le déplacement d'éléments existant peut être réalisé rapidement et simplement sans devoir manipuler les connexions physique dans le local technique ;
- **Flexibilité de segmentation du réseau :** le regroupement des ressources et des utilisateurs sans devoir prendre en considération leur localisation physique.

II.4.7 Les ACLs

II.4.7.1 Définition

Une liste de contrôle d'accès permet d'autoriser ou de refuser des paquets en fonction d'un certain nombre de critères, tels que :

-L'adresse d'origine

-L'adresse de destination

-Le numéro de port

-Les protocoles de couches supérieures

-D'autres paramètres (horaires par exemple)

Les listes de contrôle d'accès permettent à un administrateur de gérer le trafic et d'analyser des paquets particuliers. Elles sont ainsi associées à une interface du routeur, et tout trafic acheminé par cette interface est vérifié afin d'y déceler certaines conditions faisant partie de la liste de contrôle d'accès.

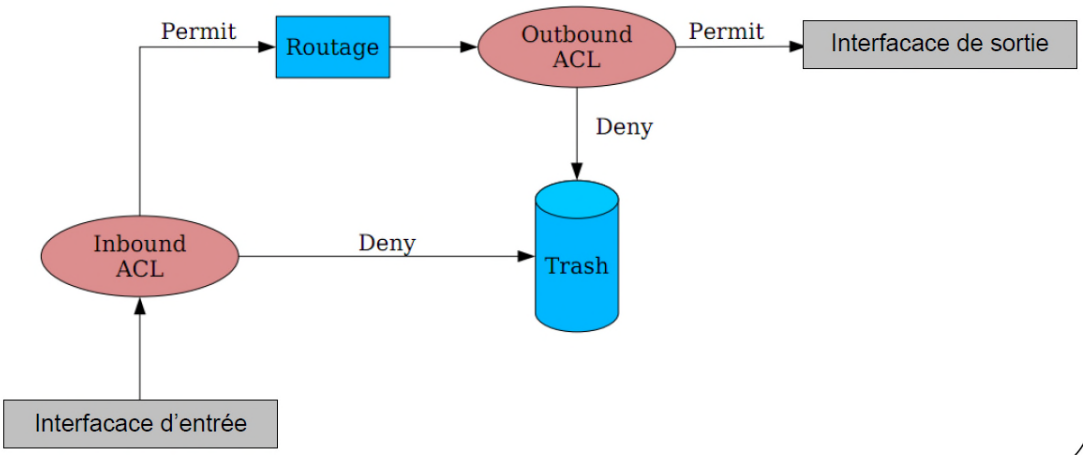

Figure II.5: principe de fonctionnement des ACLs

II.4.7.2 Les différents types d'ACL

Il existe 3 types de liste de contrôle d'accès : les ACLs standards, les ACLs étendues et les ACLs nommées.

- **Les ACLs standards** utilisent des spécifications d'adresses simplifiées et autorisent ou refusent un ensemble de protocole. Les ACLs standard sont à appliquer le plus proche possible de la destination en raison de leur faible précision.
- **Les ACLs étendues** utilisent des spécifications d'adresses plus complexes et autorisent ou refusent des protocoles précis .Les ACLs étendues sont à appliquer le plus proche possible de la source.
- **Les ACLs nommées** peuvent être soit standards, soit étendues ; elles n'ont pour but que de faciliter la compréhension et de connaître la finalité de l'ACL.

Conclusion

Nous avons vu à travers ce chapitre l'importance de la sécurité informatique sur les réseaux. En effet, afin de garantir une meilleure sécurisation, on doit d'abord identifier les différentes menaces et vulnérabilités des systèmes pour pouvoir contrer aux différents types d'attaques. Pour cela des outils et techniques de sécurisations sont mis en place, technique que nous avons présentée dans ce chapitre tel que les pare-feux, les VPNs, Les VLANs et les ACLs, afin de garantir l'intégrité et la confidentialité des données.

CHAPITRE III

Présentation de l'organisme d'accueil

Introduction

Actuellement, la puissance d'un pays se mesure essentiellement par sa part de participation au marché international et son autosatisfaction. Ainsi, NAFTAL est considéré comme l'un des paliers de l'industrie au niveau national. Ce chapitre sera consacré à la présentation de NAFTAL et de son district à Bejaia ainsi que sa structure hiérarchique. Ensuite nous allons étudier la topologie de son réseau local afin de définir une ligne à suivre pour la suite de notre projet.

III.1 Historique de NAFTAL

Issue de SONATRACH, (société nationale pour la recherche, transport, production, transformation, la commercialisation des hydrocarbures), l'entreprise nationale de raffinage et de distribution de produits pétroliers (ERDP) à été crée par le décret N°80-101 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 n°80-101 du 6 Avril 1980, modifié, portant création de l'Entreprise nationale de raffinage et de distribution de produits

pétroliers, il y a eu 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 statue et devient société par action filiale à 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.

III.2.NAFTAL District Carburants de Bejaia

Le District CBR Bejaia est organisé comme suit :

III.2.1 Direction

Sont rattachés: Une secrétaire, le responsable de la sécurité industrielle, le laboratoire, le juridique, 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 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 régionales 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 de 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.

III.2.2 Département AMG (administration et moyen 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.

Toutes ses missions sont assurées par les services suivants :

III.2.2.1 Service administration

Ce service, l'un des plus importants, se compose en trois sections :

- **Section gestion du personnel :** cette dernière s'occupe de la gestion administrative du personnel, la gestion du volet disciplinaire et l'application de la réglementation, suivie du pointage du personnel,… etc.
- **Section gestion paie :** elle se charge de la préparation et de l'établissement de la paie mais aussi les déclarations fiscale, parafiscale et relevés des émoluments.
- **Section prestations sociales :** s'occupe des différents dossiers d'allocation, médicaux et de retraite.

III.2.2.2 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 ;
- Suivi des stagiaires.

III.2.2.2 Services du moyen généraux

Ses activités sont assurées par trois sections :

- **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 Standard ;
- **Section entretien bâtiment :** Assurer l'entretien des locaux, meubles et immeubles ainsi que la gestion des charges (Electricité, eau, téléphone…..) ;
- **Section économat :** Assurer la gestion du magasin pour l'approvisionnement en consommable de bureau et informatique et fournir les documents de gestion.

III.2.2.3 Cellule OSC (Ouvre 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.

III.2.3 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 :

III.2.3.1 Service trésorerie:

Il est composé de deux sections, la Section recettes et la Section dépense. Sa mission est de :

- Traiter les dossiers de paiement d'investigation, fournisseurs et 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.

III.2.3.2 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 ;
- Elaborer les documents comptables (Bilans, balances et livres) ;
- Contrôler les arrêtés de comptes et préparer les inventaires et bilans ;
- Elaborer les analyses et synthèses comptables.

III.2.3.2 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.

III.2.4 Département Transport & Technique

Il a pour mission :

- Elaborer les plans de maintenance préventive et curative des équipements, dépôts, canalisation et en suivre l'exécution ;
- Elaborer les plans annuels et pluriannuels de transport, en prenant en charge les besoins de distribution nets ravitaillement des produits commercialisés ;

- Elaborer les plans et budgets d'investissement (rénovation, extension, remise à niveau, remplacement) des installations fixes, canalisation, réseaux de stations services et autres ;
- Etablir un rapport d'activité périodique.

Ce département comporte les services suivants :

III.2.4.1 Service exploitation et maintenance

Sa mission est de :

- Vérifier l'application des prescriptions du règlement d'exploitation, de sécurité des équipements et installation fixes ;
- Etablir les performances de maintenance ;
- Assurer la maintenance des installations au niveau des dépôts carburants.

III.2.4.2 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.

III.2.4 Département Informatique

Le département informatique est assuré par un chef de département, sont rôle principal est de garantir la continuité de service des systèmes informatiques déployés au niveau du Districts et centres opérationnels et 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 :

III.2.4.1 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.

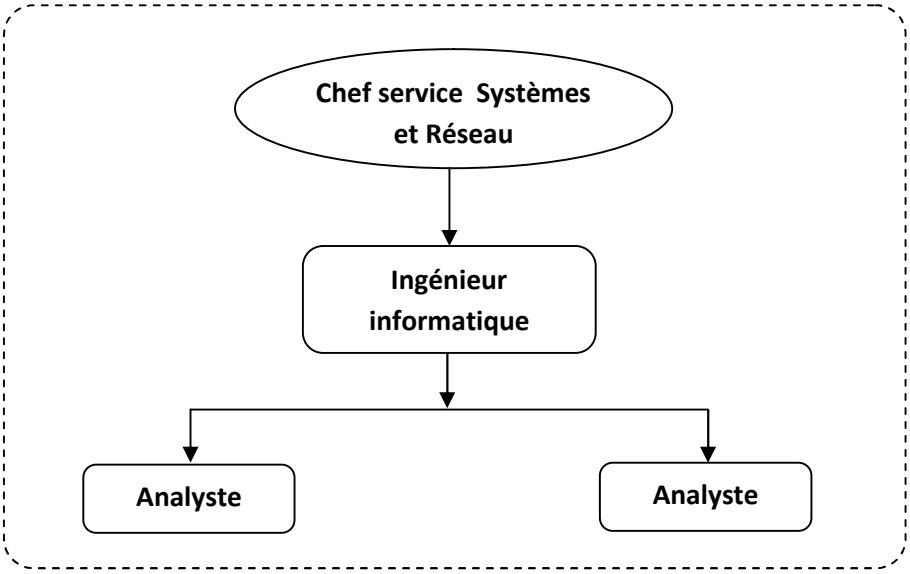

Figure III.1 : Organigramme du service Système et Réseau

Le rôle du service *Systèmes & réseau* est de prendre en charge les infrastructures réseaux filaires et Wifi, et des services généralistes (sécurité, distribution logicielle, gestion des postes de travail…), assure aussi la maintenance des équipements informatiques et établir des formations sur le fonctionnement de certain logiciels ou applications. Ce service assure deux rôles :

- **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 où partie de l'installation et de la mise en route des matériels informatiques. Prendre en charge aussi l'installation de matériels neufs, de modifications et d'adaptation des matériels.
- **L'infrastructure réseau :** Mise en place et configure le **réseau informatique** de l'entreprise, il intervient à chaque étape de la mise en place d'un réseau local, où s'en occuper intégralement de fournir le matériel nécessaire et faire :
  - La pose du câblage informatique.
  - La configuration des postes utilisateurs, système d'exploitation, messagerie, internet, intranet, FTP.
  - Assure aussi la gestion des domaines, groupe et ressource du réseau.
  - Administrer les serveurs de réseaux (serveur FTP, messagerie, web,…).

III.2.4.2 Service information de gestion (ING)

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

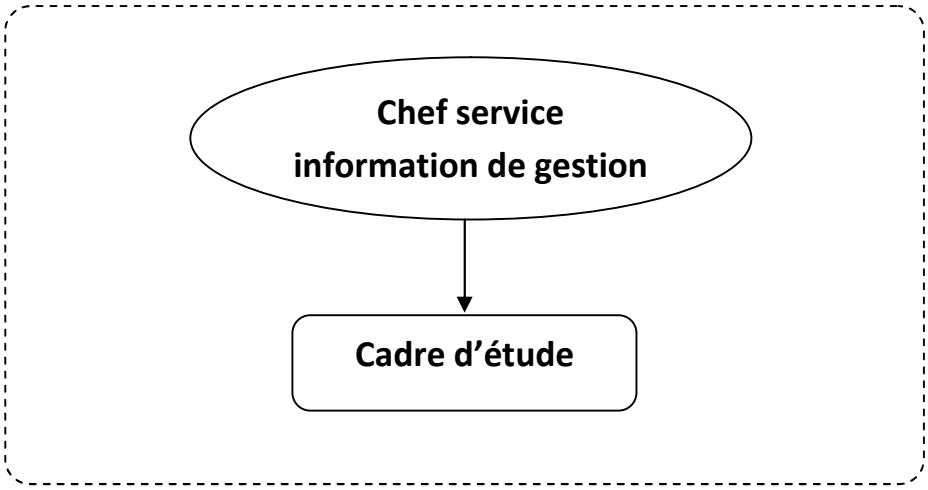

Figure III.2 : Organigramme du service information de gestion

Le rôle du service information de gestion est :

- 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 & analyser les informations concernant les activités du District ;
- Participer à l'élaboration des rapports d'activités 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.

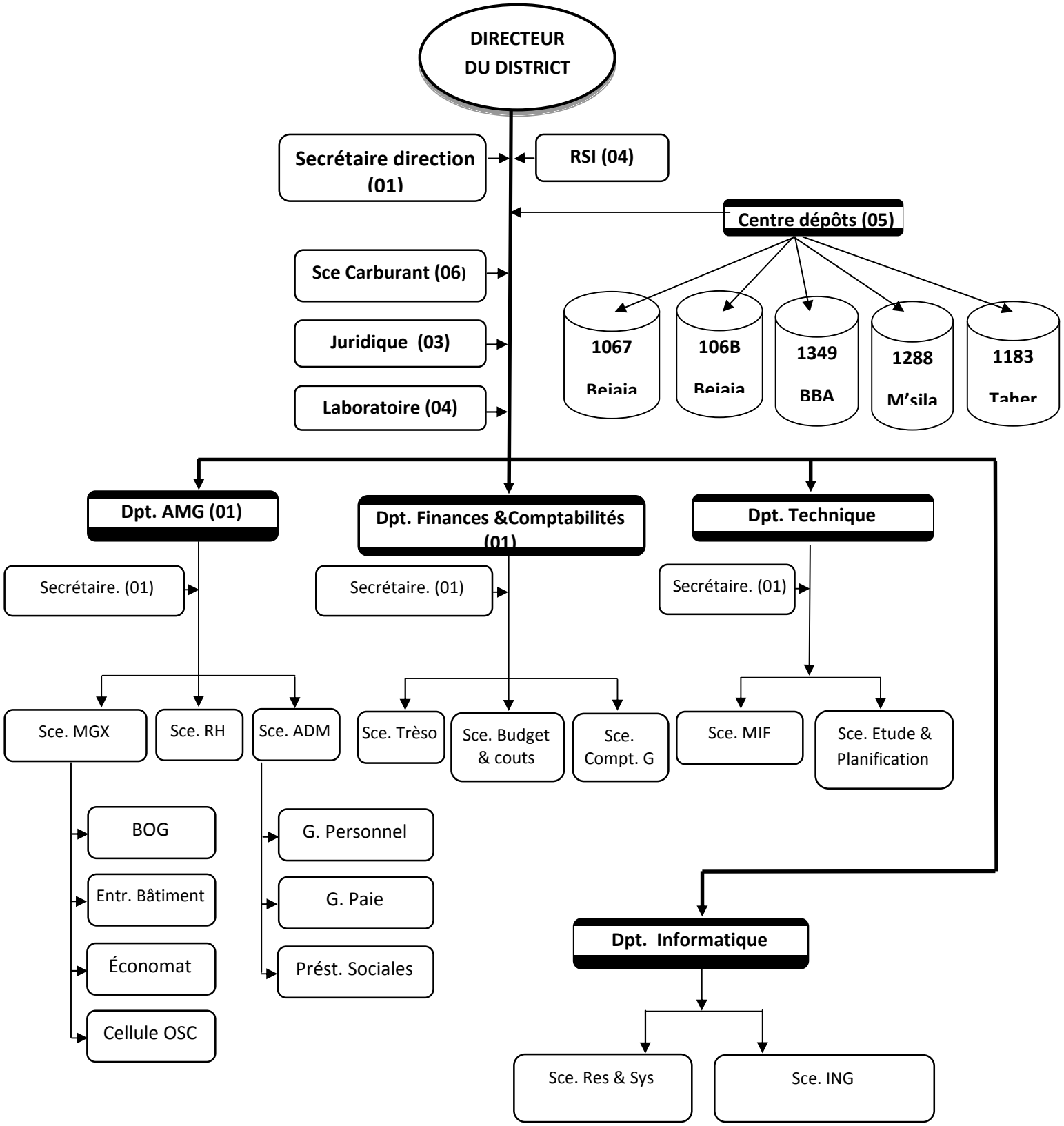

Figure III.3 : l'organigramme général de l'entreprise

III.3.Etude du réseau de l'entreprise

Une bonne compréhension de l'environnement informatique aide à déterminer la portée du projet d'implémentation de la solution. Il est essentiel de disposer d'informations précises sur l'infrastructure réseau physique et les problèmes qui ont une incidence sur le fonctionnement du réseau. En effet, ces informations affectent une grande partie des décisions que nous allons prendre dans le choix de la solution et de son déploiement.

III.3.1. Infrastructure matériel

Le réseau actuel de NAFTAL est constitué d'un Serveur, un routeur et 14 Switch interconnectés entre eux en cascade. En effet, nous avons 4 étages, qui ont chacun une armoire, chaque armoire contient différent matériels d'interconnexion. On a le routeur ainsi que trois Switch au rez-de-chaussée et les autres Switch sont répartis dans les trois autres étages et sont interconnectés en cascade.

L'équipement	Nombre	La marque et le type	Description
Serveur	1	Fujitsu Siemens Primergy D2529 RC	Ce dernier permet de gérer d'importants besoins en termes d'informatique et de stockage à grande échelle avec des moyens, un budget et un espace limité relève de l'exploit. Ce serveur a été conçu dés le départ comme une infrastructure informatique polyvalente et conviviale. Il est aussi facile à installer et à gérer qu'à utiliser.
Routeur	1	Cisco 2911	il permet d'interconnecter deux ou plusieurs réseaux. Possédant les mêmes composants de base qu'un ordinateur, le routeur

			sélectionne le chemin approprié (au travers de la table de routage) pour diriger les messages vers leurs destinations.
Switch Fibre Optic	1	CATALYSTE 3750	c'est une gamme qui améliore l'efficacité de l'exploitation des réseaux locaux grâce à leur simplicité d'utilisation et leur résilience la plus élevée disponible pour des commutateurs empilables.
Switch	13	Cisco CATALYSTE 2960	Ce Switch est une configuration fixe, empilable commutateur autonome qui fournit un accès rapide à vitesse filaire Ethernet et Gigabits Ethernet.

Tableau III.1 : **Présentation des équipements.**

La figure ci-dessus représente l'architecture de réseau actuelle « NAFTAL » :

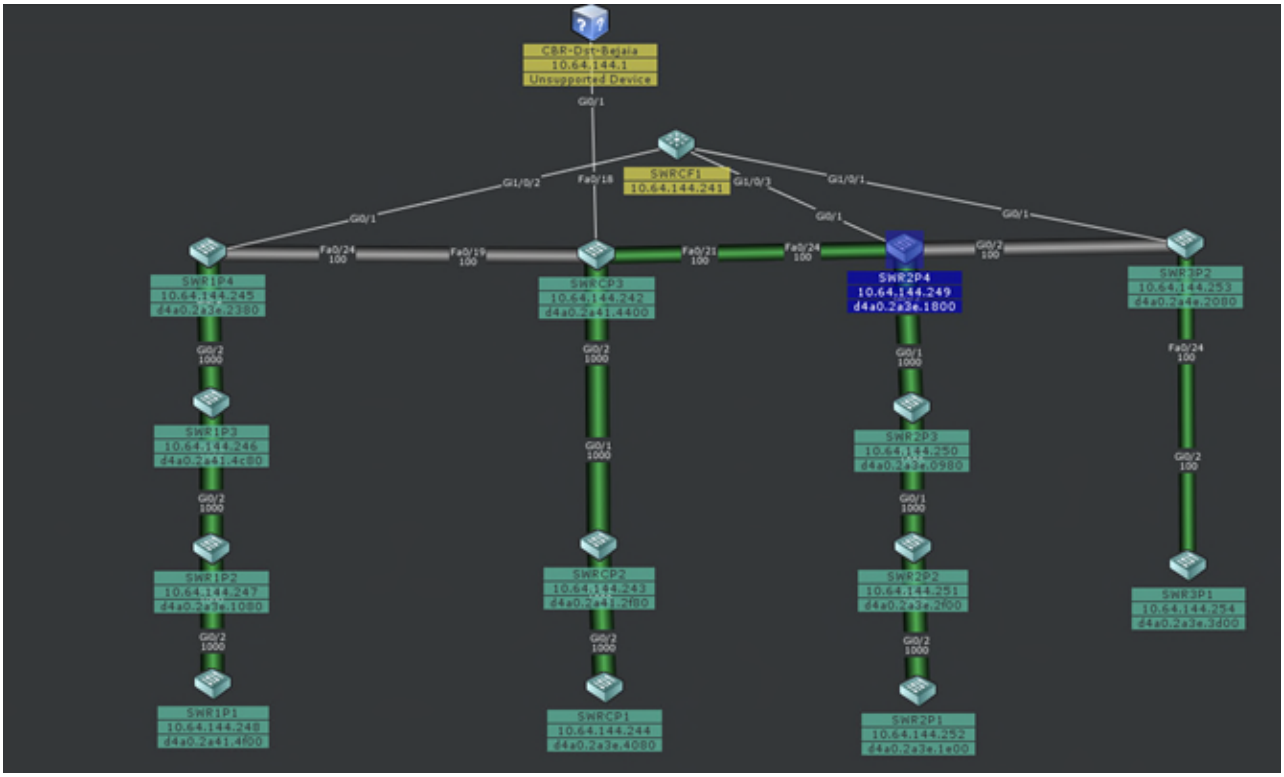

Figure III.4 : Topologie actuelle du réseau.

III.3.2 Les supports de transmissions

Pour relier les différents équipements qui sont utilisés dans le réseau, NAFTAL opte pour les deux types de média :

- **Le câble à paire torsadées :** on distingue deux catégories, le câblage 'UTP', terminé par des connecteurs RJ45 et le câble à paire torsadées blindées 'STP' ;
- **La fibre optique :** le câblage en fibre otique utilise des fibres de verre ou de plastique pour guider des impulsions lumineuses de la source à la destination.

III.3.3.La sécurité au niveau du réseau NAFTAL

L'entreprise NAFTAL utilise un firewall comme mécanisme de barrière, interdisant l'entrée à un certain types de trafic et en autorisant à d'autres trafic (filtrer les paquets)

suivant une politique de sécurité pour sécurisé son réseaux , plus une application de sécurité (Kaspersky Security) pour surveiller l'état de ces machines.

Dans le but de faciliter la gestion du système d'information, il existe des services au sein de l'entreprise, on cite parmi eux :

- Le contrôleur de domaine « Active Directory » : est un service d'annuaire, qui fournit un certain nombre de différents services relatifs au stockage des ressources du réseau.

Chaque employé possède un compte sur son ordinateur (attribuer par le service informatique), sécurisé par un mot de passe. Lorsque l'ordinateur s'allume le nom d'utilisateur et le mot de passe sont demandés par le serveur, c'est lui qui s'occupe d'authentifier l'utilisateur et lui autoriser l'accès à son poste de travail.

Le serveur va également mettre à disposition des employés des dossiers partagés, accessible à certains et pas a d'autres, selon le poste de l'employé.

III.3.4.Problématique

La situation actuelle souffre de défaillance du fait que le réseau n'obéit pas à certaines règles de sécurités. Nous citons après à titre d'exemple certains problèmes :

- On remarque que la sécurité de l'information échangée entre les divers services et départements est très faible et cela a cause de l'absence de segmentation du réseau local ;
- Risque d'attaque ou plutôt de piratage au niveau du réseau interne. en effet, l'Active Directory n'assure pas totalement l'intrusion de personnes extérieures à l'entreprise. En effet, il est facile de récupérer le mot de passe d'un employé et ainsi accéder à des informations et données ;
- Il y a une absence de sécurisation de la liaison du réseau local de Bejaia et Alger car jusqu'à l'information empreinte le chemin public (internet) sans aucune sécurité ni cryptage ou autres moyens de sécurité ce qui fait que les informations sont extrêmement exposées ;
- Du fait que les Switch soient reliés en cascade, la moindre défection d'un de ces Switch entrainera une panne du système. Par exemple, si le Switch relié

directement au routeur tombe en panne tout le réseau sera bloqué jusqu'à réparation de ce dernier ;

- La saturation de la bande passante diminue fortement les capacités du réseau et son bon fonctionnement.

III.3.5.Solutions proposées

L'objectif de notre projet est la proposition d'une nouvelle configuration du réseau local de NAFTAL et ceci dans le but de faciliter la préparation et la réalisation des projets de la société. On reliera le router a un Switch multilayer, ce dernier sera connecté au quatre Switch de la couche accès qui seront tous reliées a leur tour au quatre autre Switch de distribution. La figure ci-dessous représente l'architecture proposée :

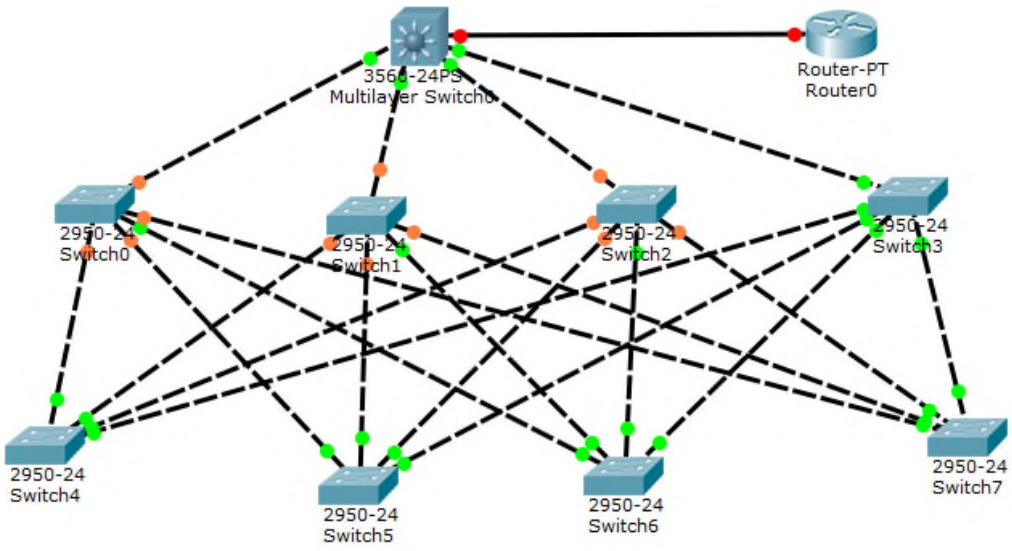

Figure III.5 : Architecture Proposée

La segmentation du réseau en utilisant les VLANs permettra de créer un ensemble logique isolé pour améliorer la sécurité du réseau en isolant les utilisateurs accédant aux données et applications sensibles. C'est pour cela qu'on découpera le LAN en plusieurs VLANs en utilisant la segmentation par sous-réseau. En effet chaque département aura son propre Vlan qui comportera les différents services de ce dernier. Ça permettra un échange

d'information sécurisé entre les services d'un même département et augmentera considérablement la qualité de la bande passante. Le tableau ci-dessous nous montre la segmentation :

Nom Vlan	**Vlan-ID**	**Description**
Vlan direction	1	Vlan pour la direction
Vlan AMG	2	Vlan pour le département AMG qui englobera les trois services RH, MGX et ADM
Vlan F_comp	3	Vlan pour le département finance et comptabilité qui englobera les services trésoreries, budgets et comptabilité.
Vlan Tech	4	Vlan pour le département technique qui englobera les services MIF, étude et planification
Vlan info	5	Vlan pour le département Informatique qui comporte les deux services ING et systèmes réseaux

Tableau III.2 : Tableau représentatif des VLans

Nous appliquerons aussi des listes de contrôle afin de fortifier le partage de données et de conforter l'Active Directory en définissant les accès de chaque utilisateur.

Et enfin un VPN est particulièrement bien adapté à l'interconnexion du site de Bejaia et Alger. Il permet un partage sécurisé des données et la confidentialité des données échangées via un canal sécurisé.

Conclusion

Dans ce chapitre nous avons commencé par présenter l'organisme d'accueil « NAFTAL » et sa structure, puis nous avons étudié la topologie du réseau local. Ainsi que les problèmes de ce réseau, parmi ces dernier celui de la sécurité. Dans le chapitre qui suit nous allons décrire les étapes de la mise en œuvre des solutions proposées.

CHAPITRE IV

Réalisation des solutions proposées

Introduction

Dans ce chapitre, nous allons passer à la dernière étape qui est la réalisation. Cette dernière est une étape cruciale pour la mise en place de tout ce que nous avons vu auparavant ou nous implémenterons la solution précédemment proposée et conçu, pour ce faire nous commencerons par la présentation du simulateur utilisé, puis nous expliquerons en détail les différentes étapes suivies dans la réalisation de notre réseau LAN.

IV.1 Présentation de simulateur « Cisco Packet Tracer »

C'est un outil pédagogique et simulateur de réseau, développé par CISCO Systems pour concevoir configurer, dépanner et visualiser le trafic réseau dans un environnement de programmes simulé et contrôlé. Packet Tracer permet d'élaborer des représentations virtuelles de réseaux et d'émuler un grand nombre des fonctions offertes par le périphérique réseau. La figure [IV.1] est une image montrant l'interface principale.

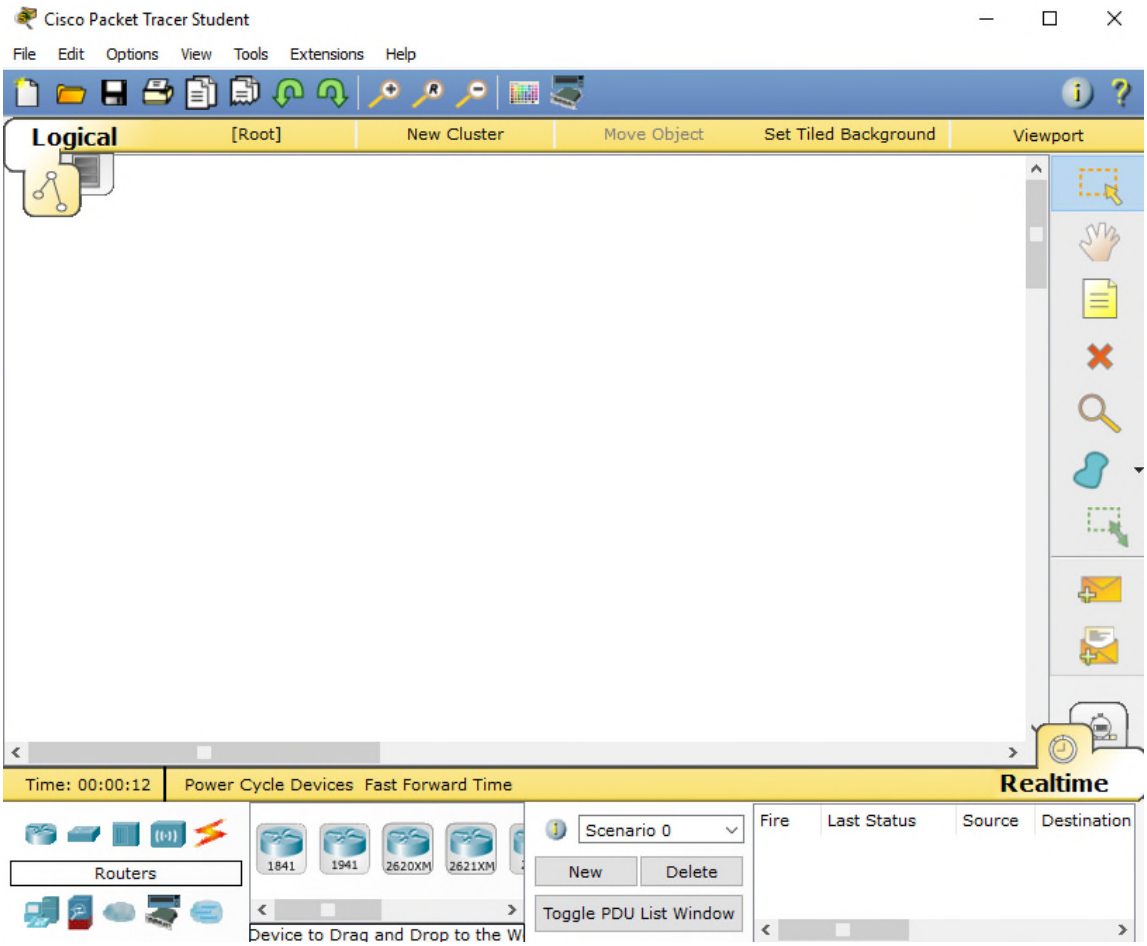

Figure IV.1 : Interface Cisco Packet Tracer.

IV.2 Méthode de configuration des équipements

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

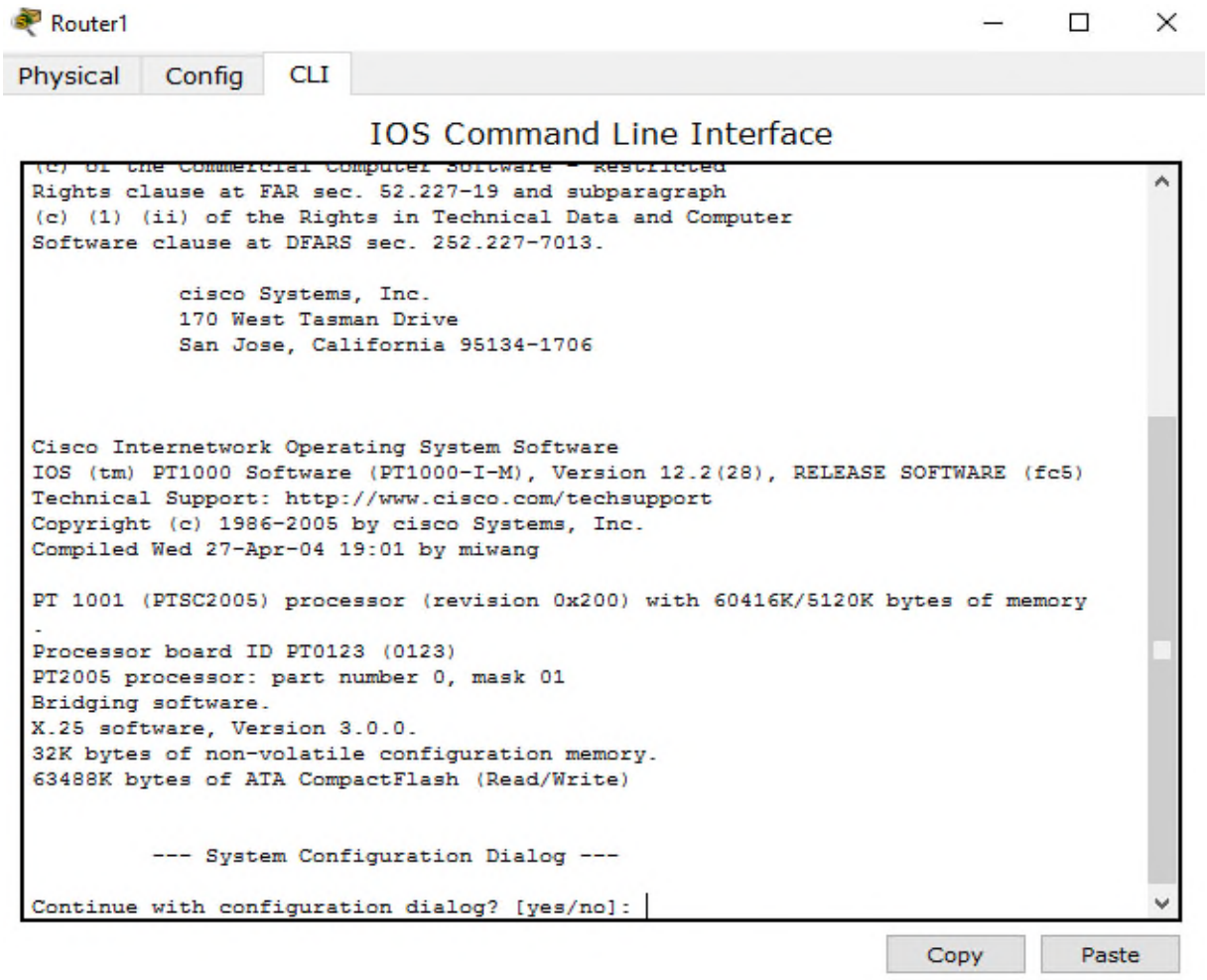

Figure IV.2 : Interface CLI.

IV.3 La réalisation

IV.3.1 Matériel utilisé

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

- Un routeur
- 8 Commutateurs Cisco 2950
- 40 pc pour le test
- Un Multilayer 3560
- Des câbles droits pour connecter les commutateurs ou ordinateurs aux commutateurs ou routeur.

Le réseau de District CBR Bejaia sera comme suit sous Packet Tracer :

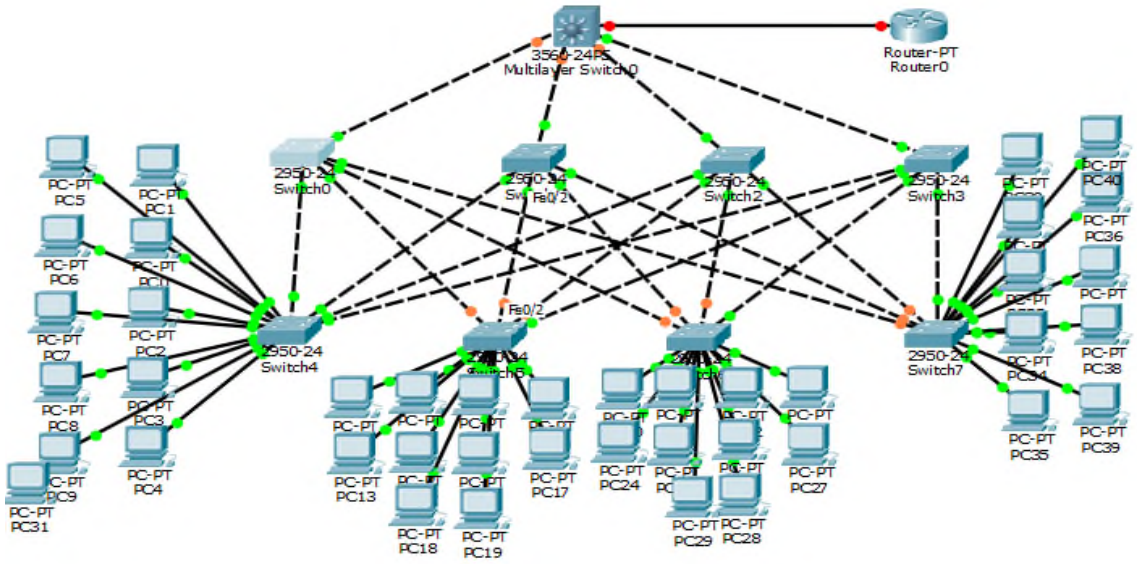

Figure IV.3 : l'architecture proposée de NAFTAL sous Packet Tracer.

IV.3.2 Les étapes de simulation

Nous avons deux étapes de configuration, une pour les commutateurs (ou Switch) et une autre pour le routeur.

IV.3.2.1 Configuration des commutateurs

Nous allons lancer une série de configuration pour la réalisation de notre réseau local.

- **1ière étapes :** Configuration des Switch

Au début d'une configuration de base du commutateur, on commence par l'attribution d'un nom au commutateur avec la commande suivante :

Switch# hostname <nom-Switch>

✓ Pour le Switch serveur (fédérateur) :

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname s-ser
s-ser(config)#exit
```

✓ Pour les Switch qui restent :

```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S0
S0(config)#exit
```

- **2ième étape :** Configurer les lignes pour les consoles et les mots de passes d'accès, et pour cela, on tape les commandes suivantes :

Switch(config)#line console 0

S0(config)#password <mot-de-passe>

Différentes commandes à suivre pour la configuration des lignes de console et de mot de passe :

```
Switch>enable
Switch#confi t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S0
S0(config)#line console 0
S0(config-line)#password naftal
S0(config-line)#login
S0(config-line)#line vty 0 15
S0(config-line)#password naftal
S0(config-line)#login
S0(config-line)#exit
S0(config)#exit
S0#
%SYS-5-CONFIG_I: Configured from console by console
copy r s
```

- **3ième étape :** Configuration d'un domaine VTP sur tous les Switch

Le protocole VTP (Virtual Trunking Protocol), protocole propriétaire Cisco permet, aux commutateurs et routeurs qui l'implémentent, d'échanger des informations de configuration des VLAN.

Il permet donc de redistribuer une configuration à d'autres commutateurs, évitant par la même occasion à l'administrateur de faire des erreurs, en se trompant par exemple de nom de VLAN.

Dans un domaine VTP, on distingue une hiérarchie comprenant trois modes de fonctionnement :

- ✓ Client
- ✓ Serveur
- ✓ Transparent

Le protocole VTP doit être configuré sur tous les commutateurs du réseau en leur attribuant un nom au domaine VTP et un mot de passe. Les commandes de configuration du VTP sont les suivantes :

Switch(config)# vtp mode (server | client)
Switch(config)# vtp domain domain-name
Switch(config)# vtp password mot-passe

Maintenant nous allons configurer le protocole VTP, le Switch cœur sera configurer en mode serveur et les Switchs d'accès en mode client. On prendra le multi switchers et le Switch S0 comme exemple, la même chose sera appliquer aux autres commutateurs. Le nom de domaine VTP est test, les deux figures suivantes illustres nos configurations :

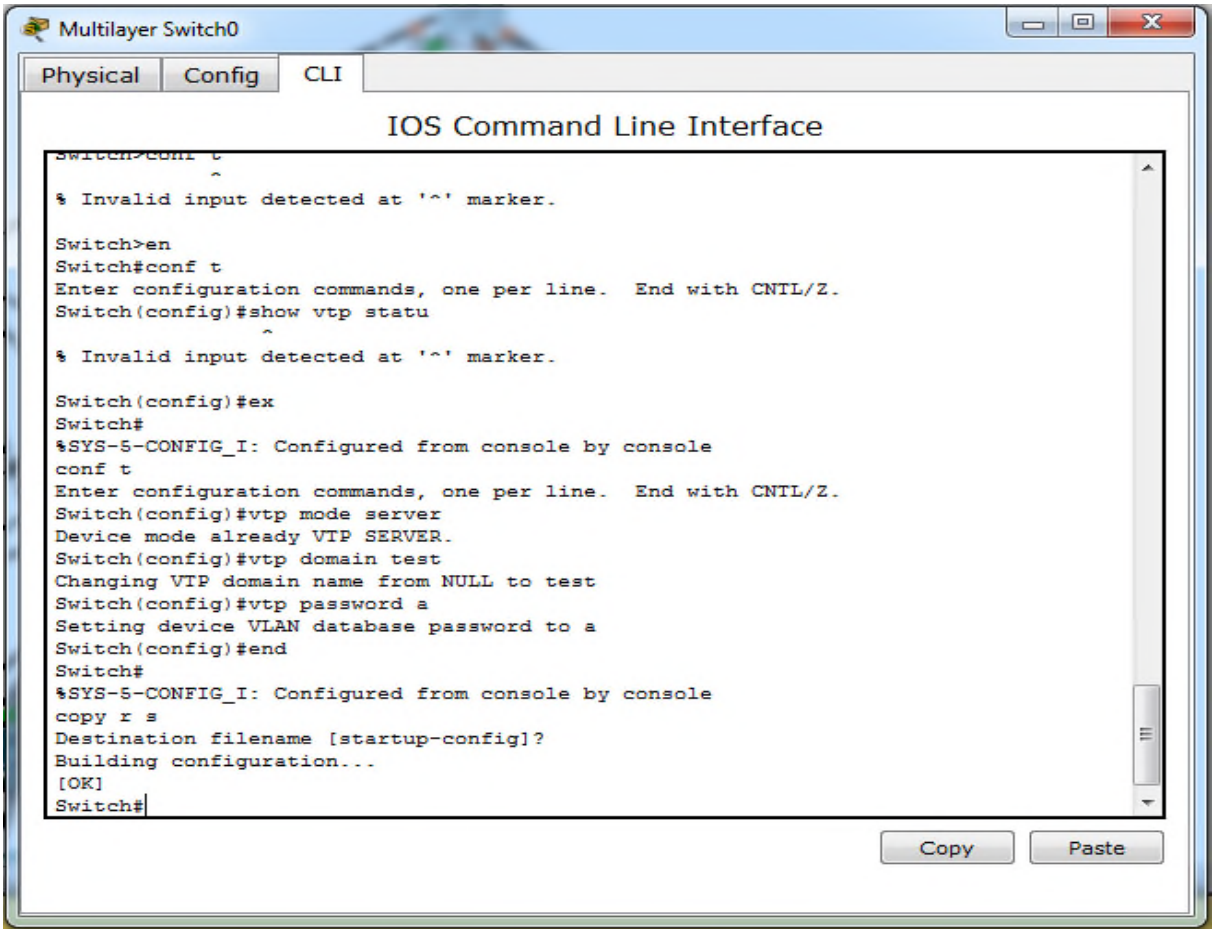

Figure IV.4 : Configuration du serveur VTP sur le Switch fédérateur.

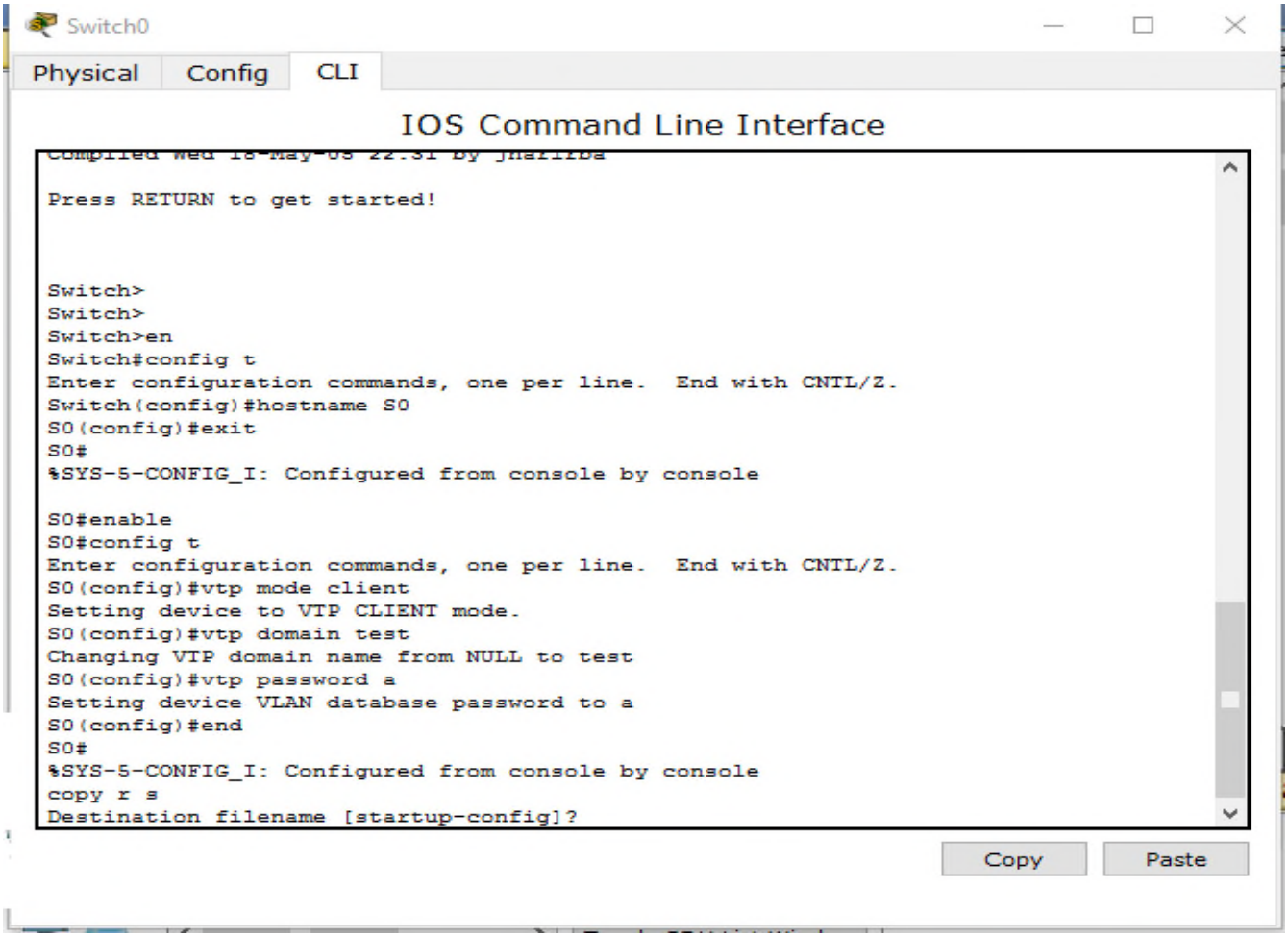

Figure IV.5 : La configuration du mode client sur tout les Switch

- **5ième étape :** Configuration des VLANs

Après avoir configuré le serveur VTP, nous allons créer le réseau virtuel. Pour se faire, nous devon créer des VLANs dans le serveur VTP, ce dernier diffusera ses configurations, tandis que le client VTP mettra à jour sa configuration VLANs en fonction des informations reçues du serveur. La syntaxe des commandes utilisées pour créer les VLANs sont :

Switch(config)#Vlan <num_vlan>

Switch(config)#name <nom_vlan>

La figure ci-dessous nous montre sa configuration sur le multi Switcher :

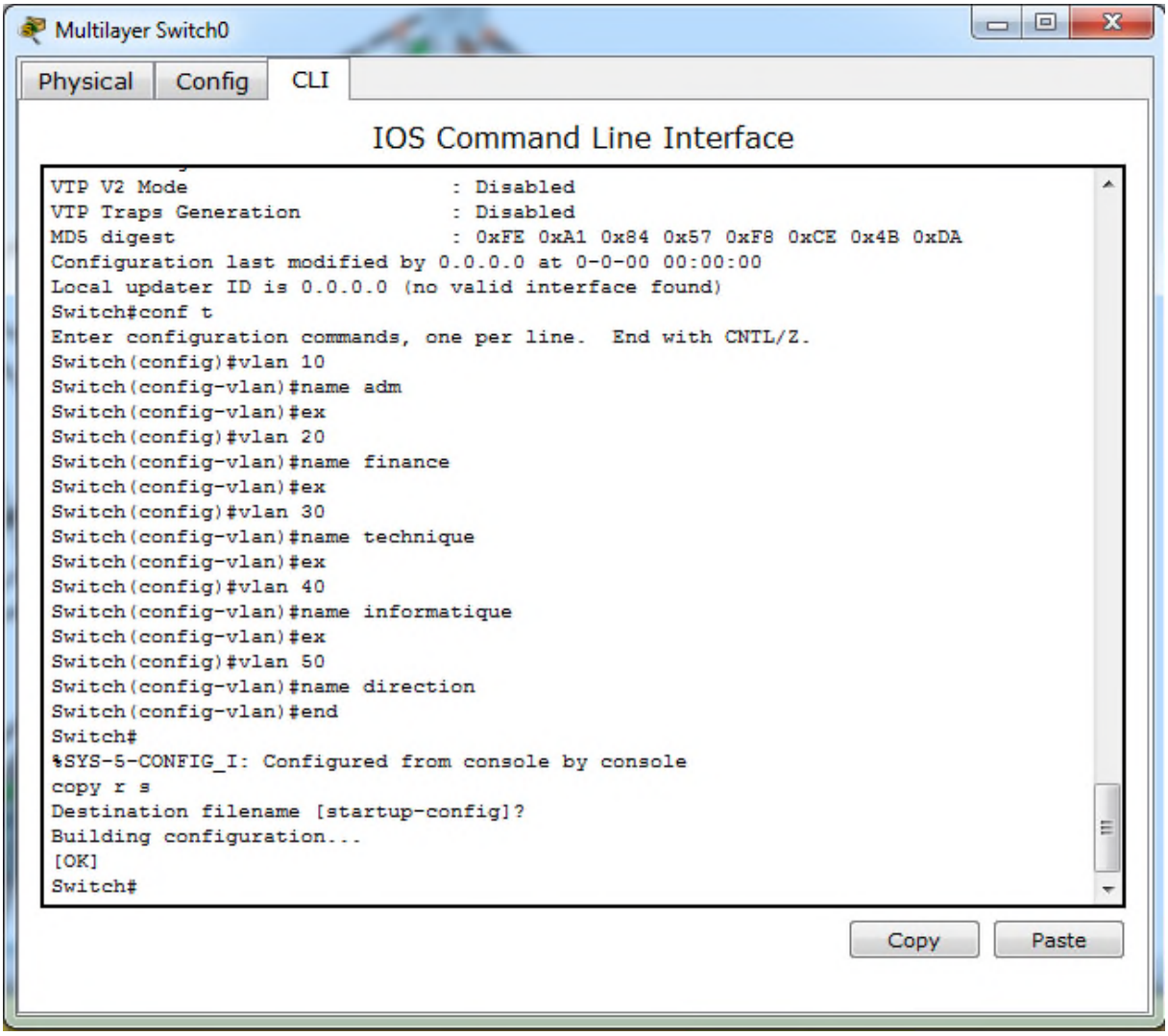

Figure IV.6 : La configuration des VLANs sur le multi Switcher

Ensuite on va crée les interfaces et les pools DHCP pour chaque VLANs, les figure ci-dessous nous montre les différentes commandes à suivre :

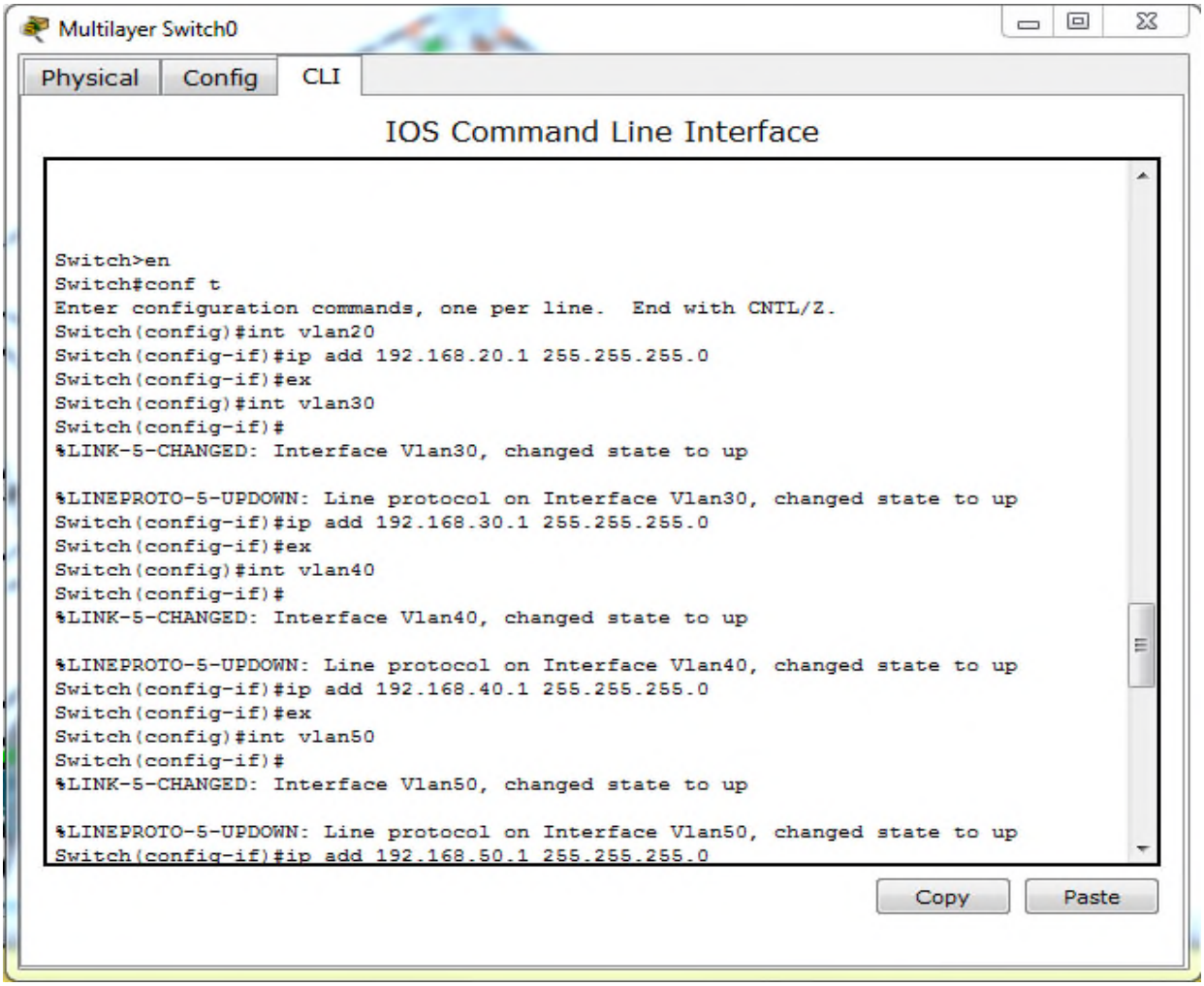

Figure IV.7 : La configuration des adresses IP des Switch.

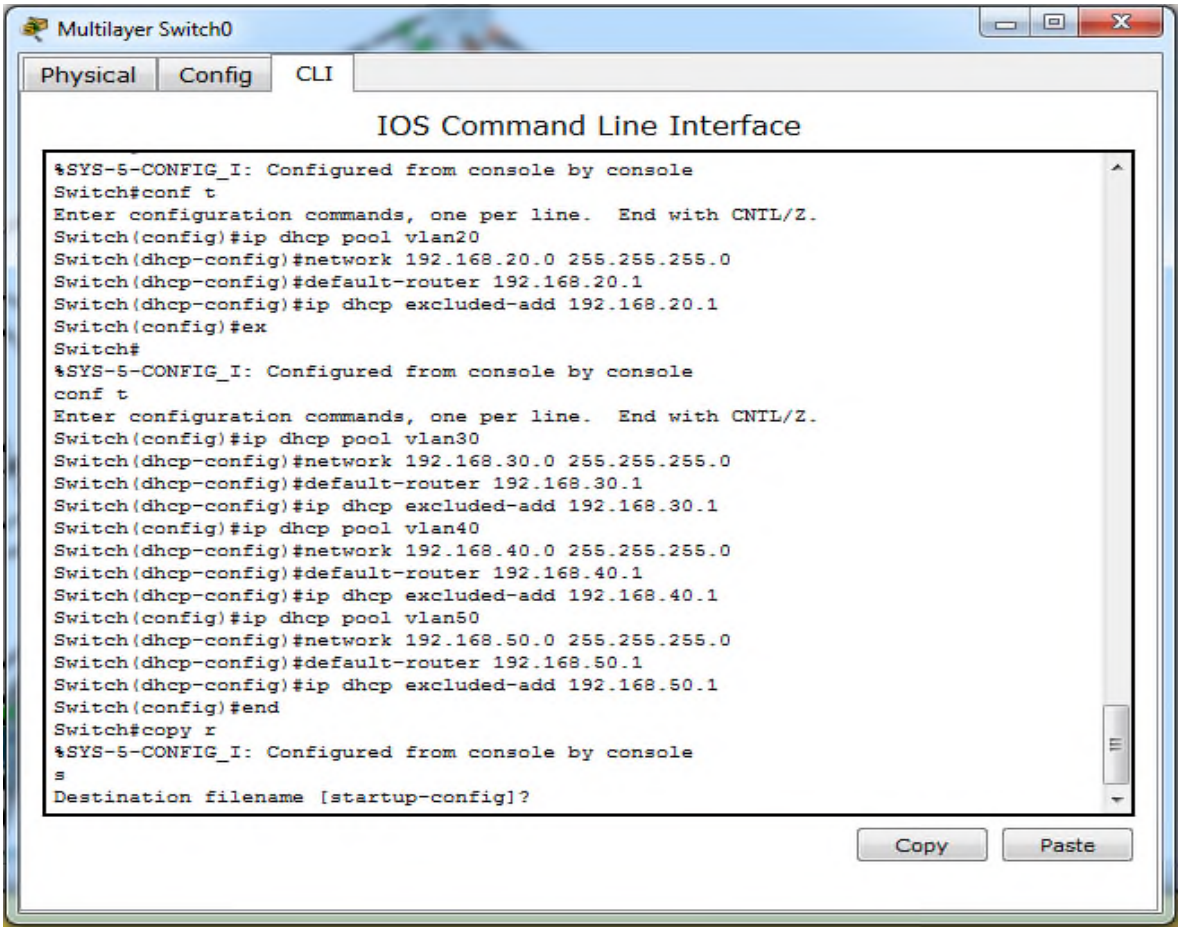

Figure IV.8 : La création des pools DHCP pour chaque VLANs.

- **6ième étape :** La configuration en mode trunk ou mode access

Dans cette étape nous configurons tous les ports qui relient les Switch en mode trunk et les ports des Switch qui sont reliés au PC vont être en mode access.

La Figure ci-dessous nous montre la configuration du mode Trunk au niveau du Switch fédérateur :

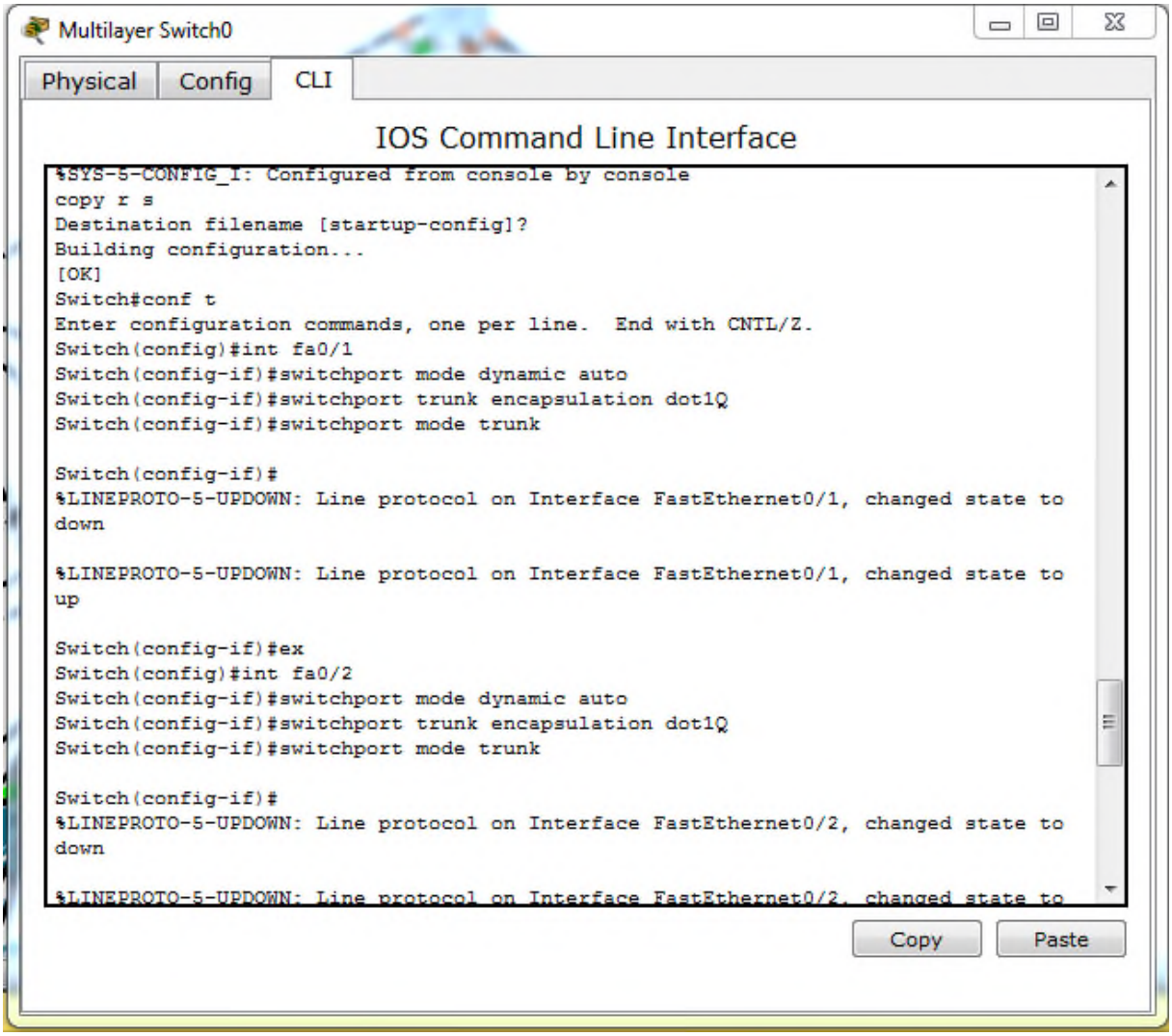

Figure IV.9 : la configuration du mode Trunk au niveau du Switch fédérateur.

Ensuite, la figure ci-dessous montre la configuration des autres Switch toujours en mode Trunk :

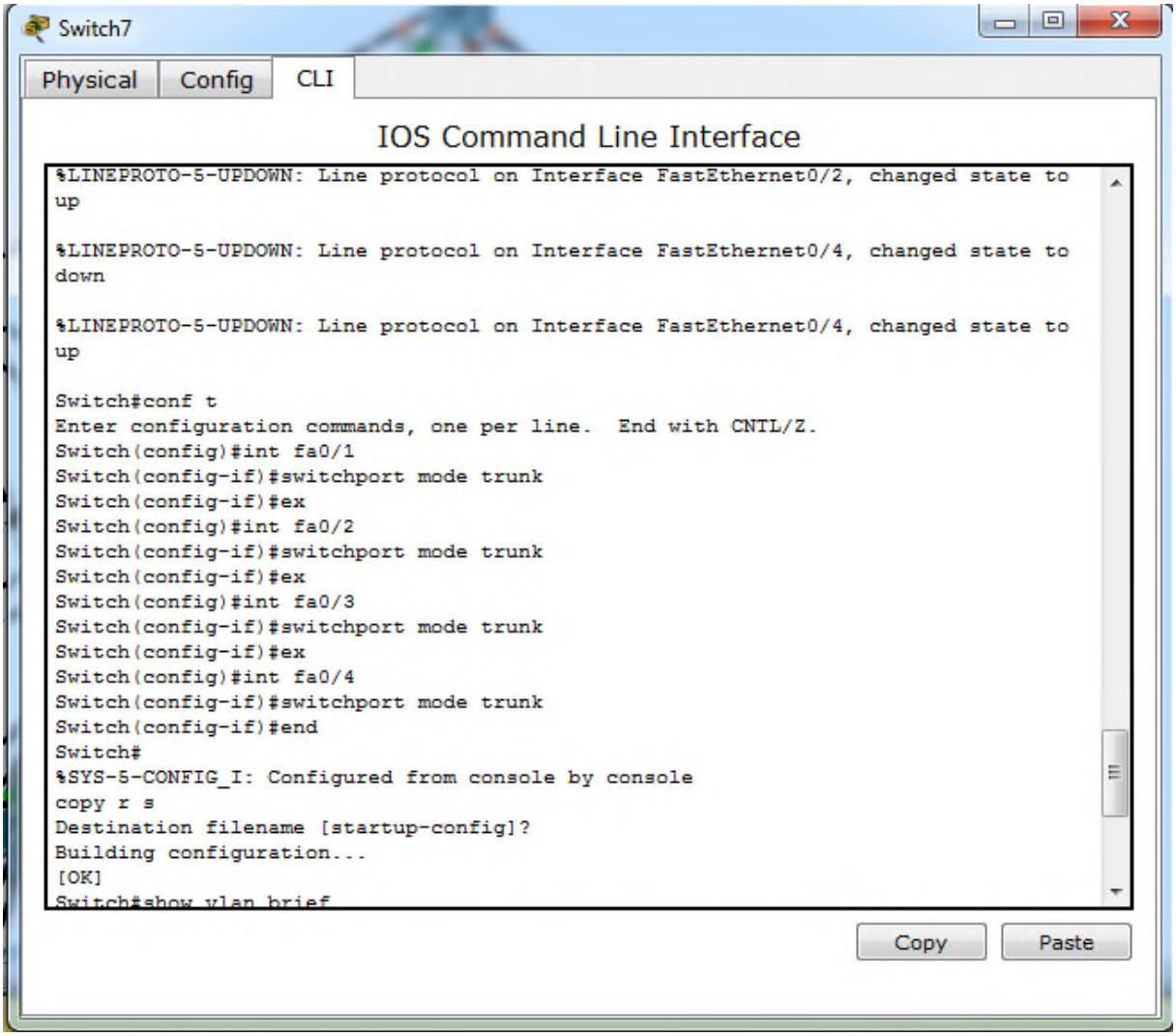

Figure IV.10 : la configuration des autres Switch en mode Trunk.

Les ports reliées au PC seront quand a eux configurer en mode access et en affectant a chaque port son réseau virtuel adéquat. La figure ci-dessous nous montre un exemple de configuration qui sera appliqué à tout les switch :

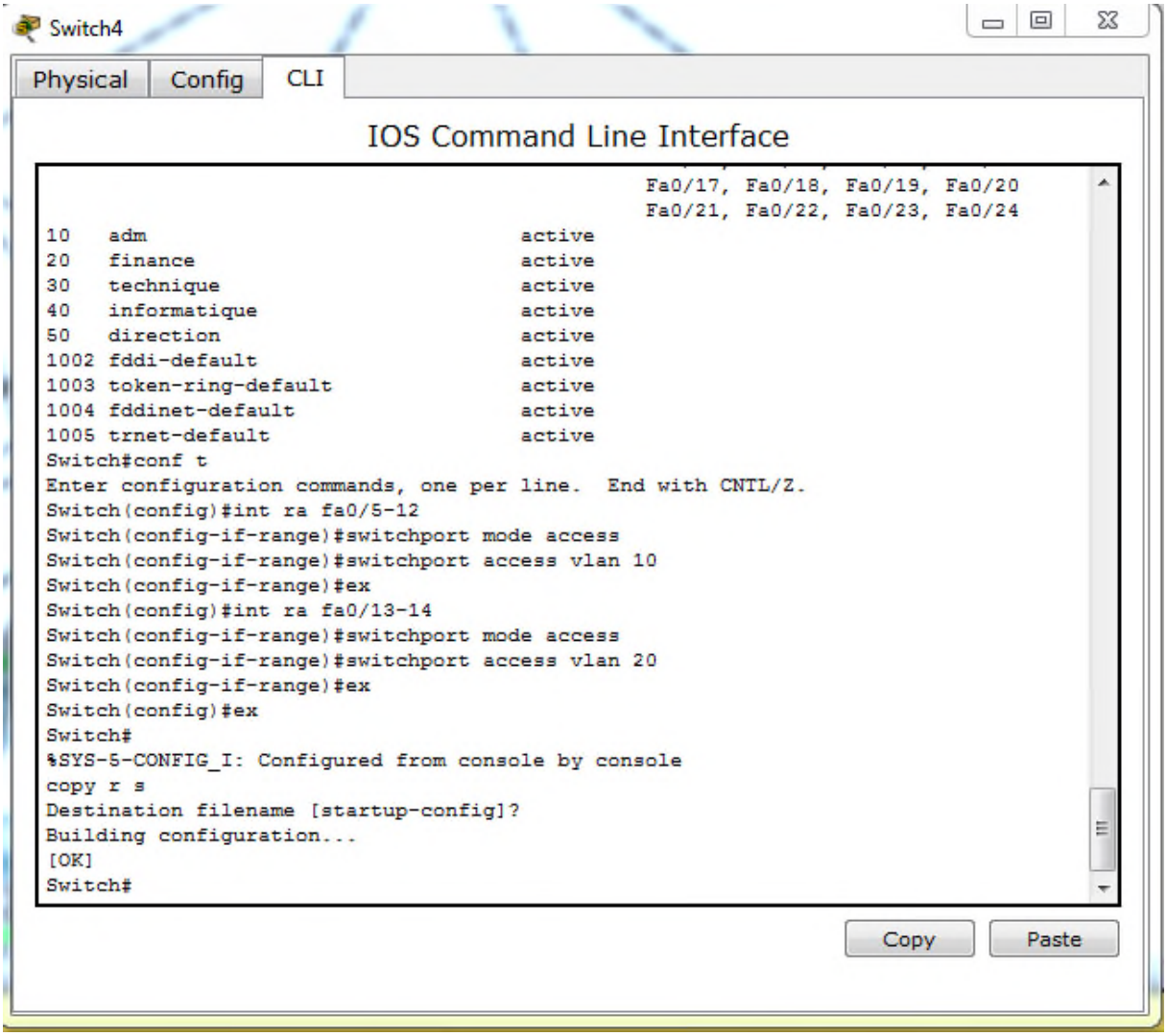

Figure IV.11 : La configuration des ports reliés au Pc en mode Access.

- **7^{ieme} étape :** configuration sécurisées des ports des commutateurs

On est dans l'obligation de sécuriser des ports sur un port du commutateur. La figure ci-dessous nous montre les différentes commandes utilisées :

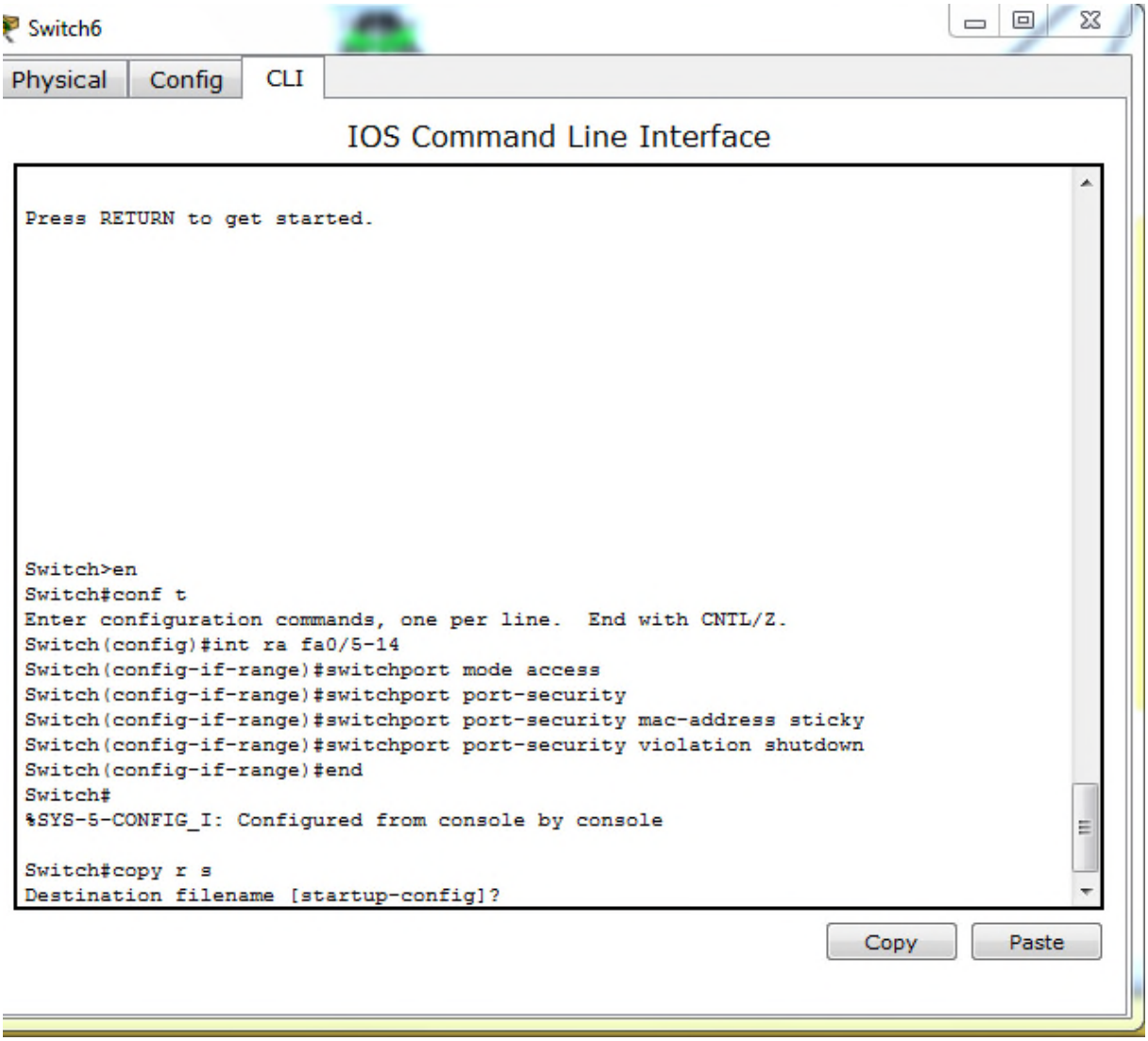

Figure IV.12 : configuration sécurisées des ports des commutateurs.

IV.3.2.2 Configuration du routeur

Pour la configuration des routeurs nous allons suivre les étapes de configurations suivantes :

- Configuration du routeur.
- Routage inter vlan.
- Configuration des liste de contrôle ACL.

- **1ière étape** : attribution d'un nom et d'un mot de passe au routeur

On va tout d'abord attribuer un nom, un mot de passe et un nom de domaine.la figure ci-dessous nous montre les commande :

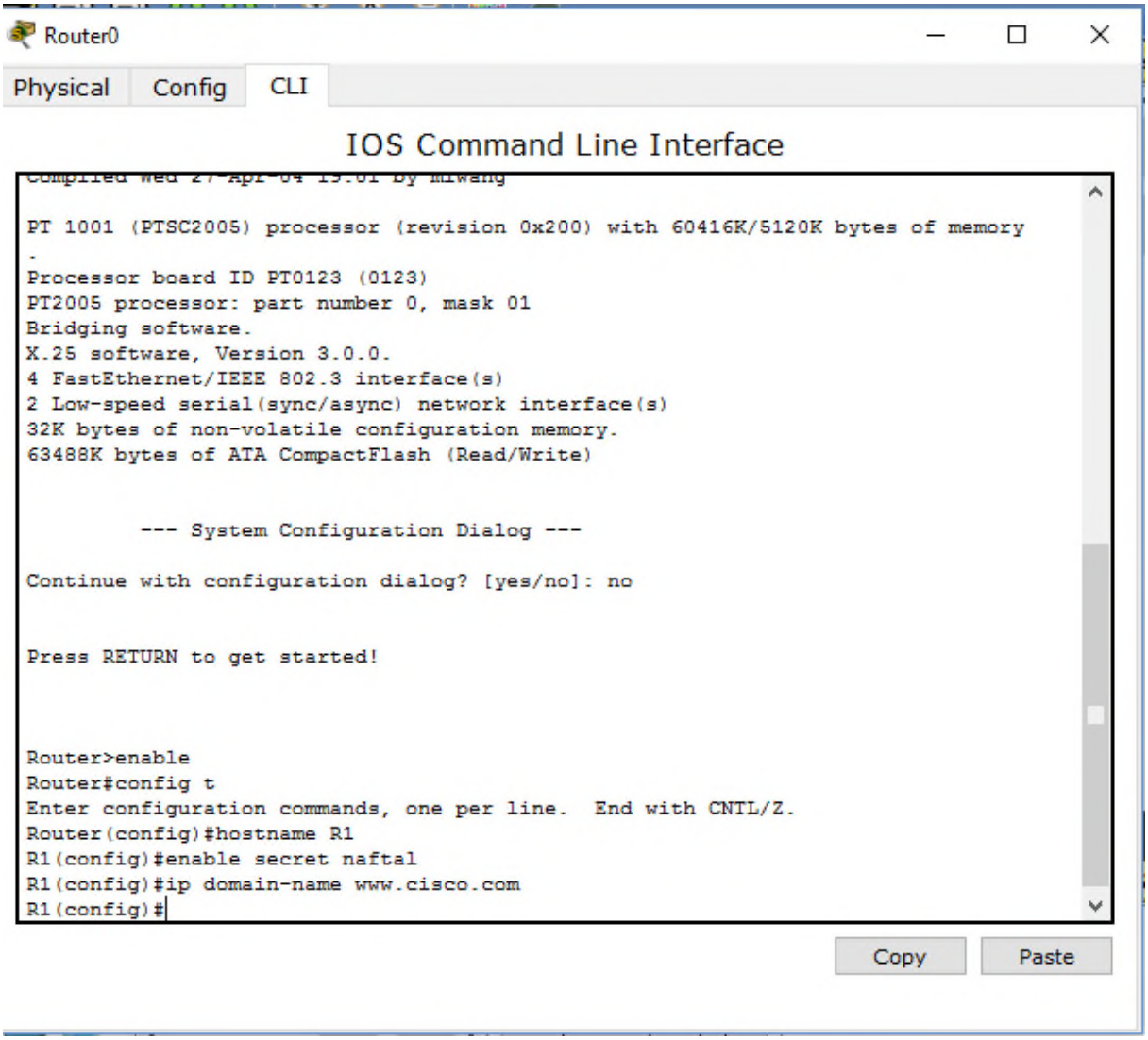

Figure IV.13: configuration du routeur.

- **2eme étape :** routage inter-vlan

Le routage inter-Vlans permet à plusieurs Vlans différents de communiquer.les figures ci-dessous nous montre les commande obligatoire pour réussir le routage :

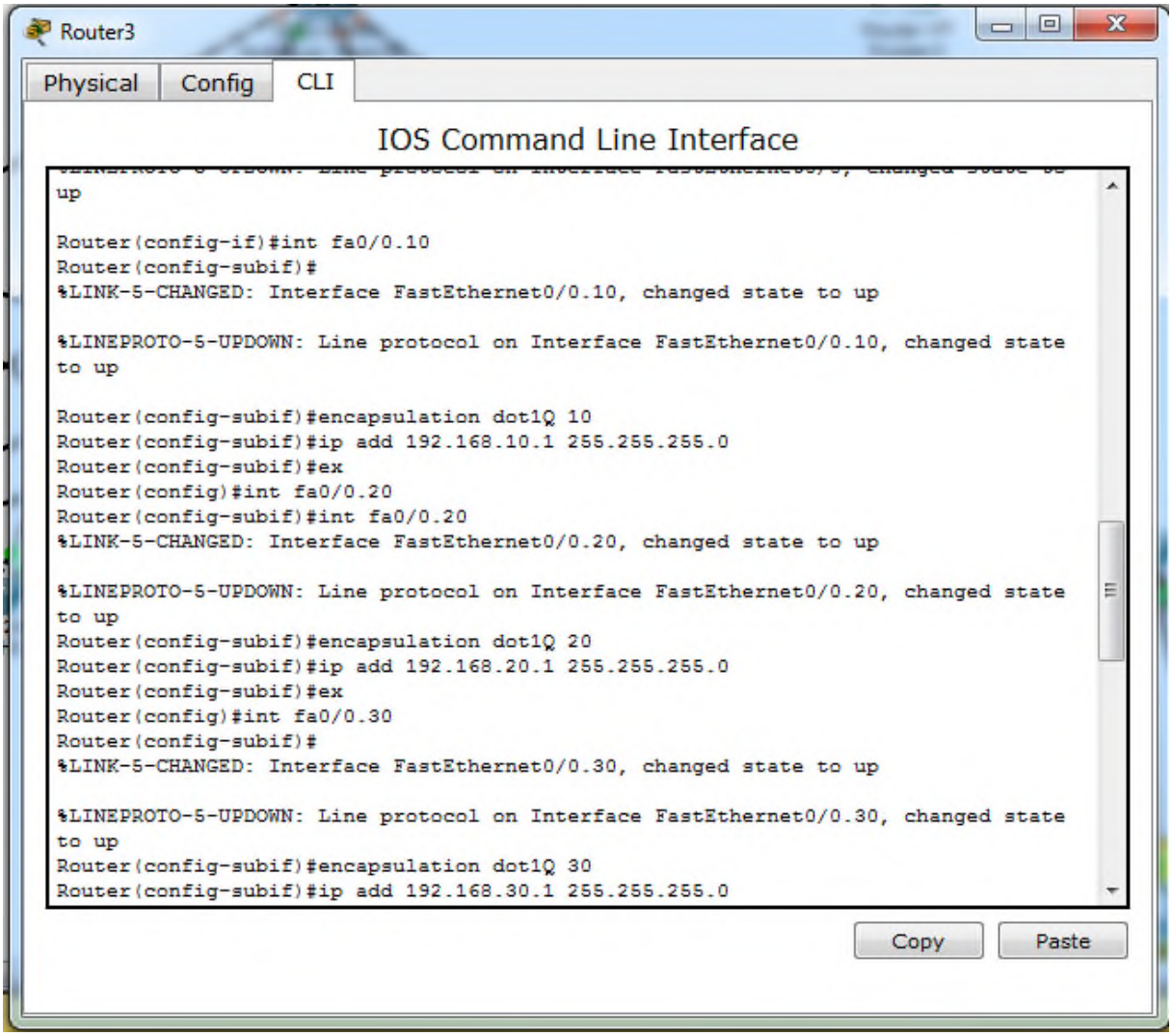

Figure IV.14: Le routage inter-VLANs.

3eme étape : configuration des listes de contrôle

Pour cette étape nous allons créer un certain nombre de liste de contrôle afin de mieux sécurisée la circulation des données au sein du réseau local et confortée l'active directory dans son travail. En premier lieu, Nous allons créer une liste d'accès pour chacun des chefs de département en bloquant l'accès entrant vers eux c'est-à-dire que les autres n'auront pas accès sur leur donnés. La figure ci-dessous montre sa configuration au niveau du router :

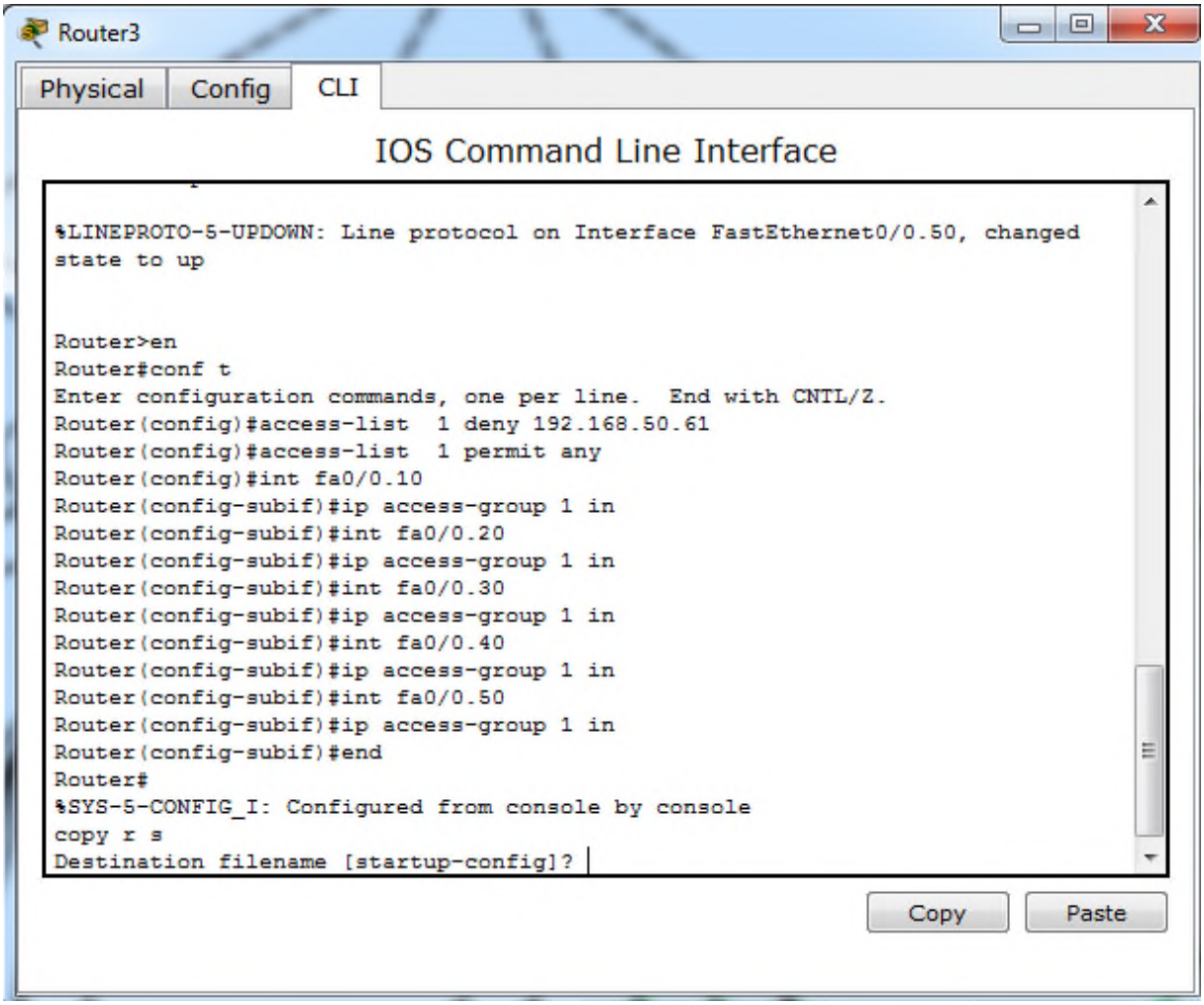

Figure IV.15 : configuration de la liste d'accès liés au directeur.

Dans la deuxième figure nous montrons la configuration de la liste d'accès qui bloque le sous réseau du département informatique. En effet, ce dernier qui s'occupe de la gestion de tout le réseau de l'entreprise doit être au maximum protégé

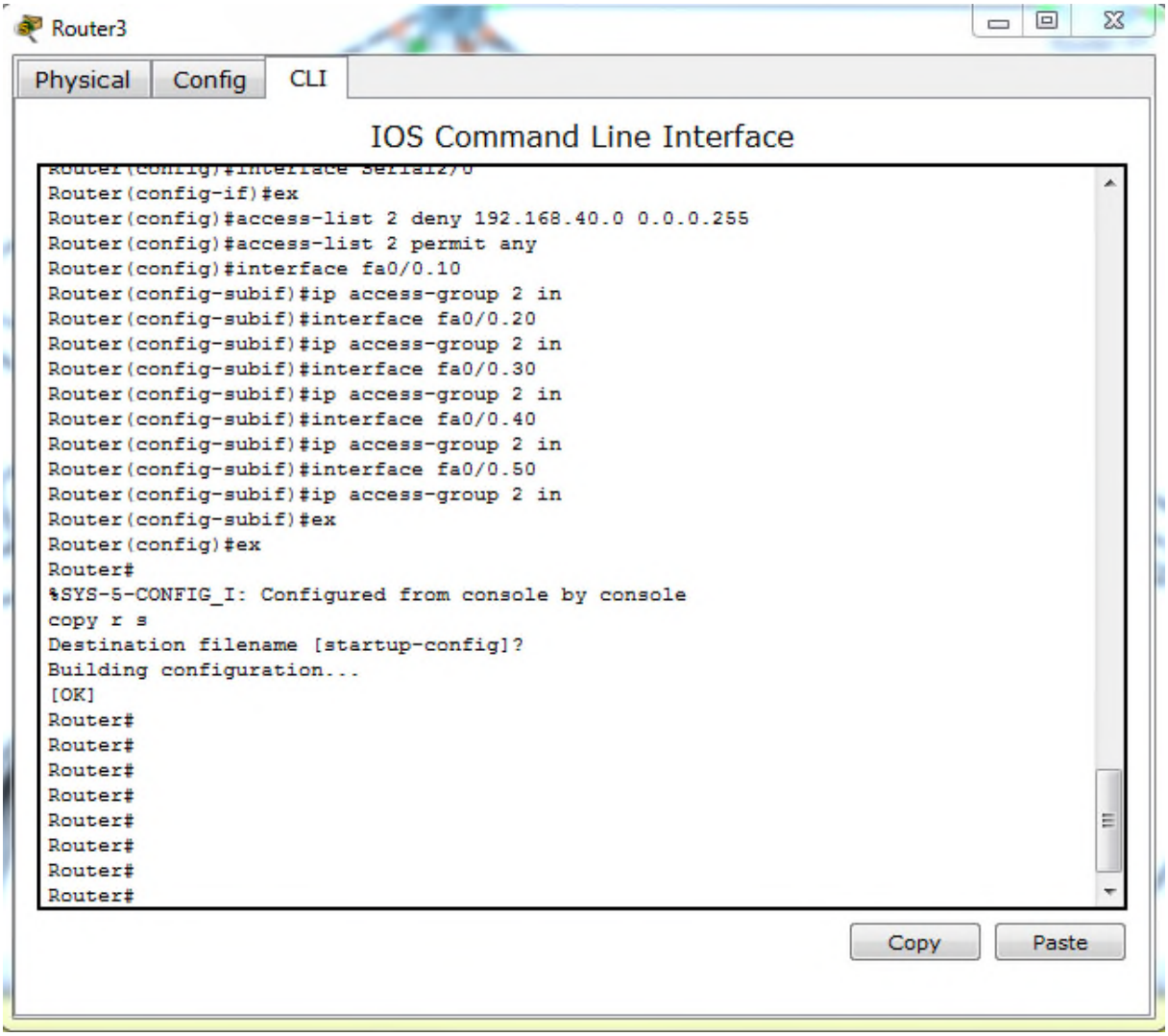

Figure IV.16 : configuration de la liste d'accès du département informatique.

Conclusion

Pour conclure notre projet, nous avons commencé par introduire le simulateur Packet Tracer, que nous avons par la suite utilisé pour la configuration de notre architecture. Nous avons donc partagé notre réseau en divers Vlan et nous appliquerons divers listes d'accès afin d'assurer une certain sécurité pour les données échangé.

Conclusion générale

Le secteur des technologies de l'information étant en constante mutation, le présent travail fait état des résultats obtenues lors de la mise en place d'un réseau local sécurisé et fonctionnel partagé en différant Vlan et régis par divers liste de contrôle.

En effet, nous avons présenté un travail divisé en deux grandes parties, à savoir l'approche théorique qui subdivisé en deux chapitre : le premier a porté sur les généralités sur les réseaux informatique et ses concepts fondamentaux ainsi qu'un aperçu sure les différentes topologies et les équipements d'interconnexion des réseaux locaux. Le second quant a lui porté sur les différent mécanismes de sécurité applicable aux réseaux locaux afin de mieux cerné les point sur les quelles nous allons axer notre travail.

La seconde partie consacrée quant a elle à la finalisation du projet a été aussi subdivisé en deux chapitres. Le premier qui a porté sur l'étude préalable dans laquelle nous avons présenté l'entreprise et exposé la problématique, laquelle nous avons solutionné par la proposition d'une nouvelle architecture et une fragmentation en Vlan de cette dernier afin d'assurer la sécurité de l'information échangée localement mais aussi la mise en place d'une solution VPN pour les donnée partagée avec d'autres sites.

Le deuxième et dernier chapitre de cette seconde partie a été consacré quant a lui a la réalisation du projet, où nous avons introduit les outils et logiciels ayant servis à l'élaboration du projet à savoir Packet Tracer tout en expliquant les différentes configurations.

Le besoin de sécuriser les données échangés avec le site d'Alger nécessite l'implémentation d'un VPN, permettant de crées un chemin virtuel sécurisé entre le site de

Conclusion générale

Bejaia et celui d'Alger. Grâce à un principe de tunnel dont chaque extrémité est identifiée, les données transitent après avoir été éventuellement chiffrées. Pour pousser davantage notre étude, la perspective VPN est recommandé, pour compléter le travail effectué dans ce mémoire.

Ce travail nous permis d'acquérir une expérience personnelle et professionnelle très bénéfique. Ce fut une occasion pour nous de se familiariser avec l'environnement du travail et de la vie professionnelle, d'élargir et d'approfondir nos connaissances sur l'administration des réseaux informatique.

Références bibliographiques

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

[2] : Guy Pujolle, Initiation aux réseaux, EYROLLES, 1re édition 2000, 3eme tirage 2003.

[3] : Claude Servin, Réseaux et télécoms, DUNOD, Paris, 2003.

[4] : Jean-Luc, Réseaux d'entreprise par la pratique, EYROLLES.

[5] : José DORDOIGNE, Réseau informatiques, ENI, février 2011.

[6] : Gerardo RUBINO et Laurent TOUTAIN, Réseaux locaux, Ecoule Nationale Supérieure des télécommunications de Bretagne, Campus de rennes.

[7] : Cédric Lorens, Informatique et Réseau d'un opérateur de télécommunication.

[8] : Andrew Tanenbaum, Réseaux, 3e édition, DUNOD.

[9] : Stéphane Natkin, les protocoles de sécurité d'internet, DUNOD science SUP, mai 2002.

[10] : Jean-François CARPENTIER, La sécurité informatique dans la petite entreprise, édition ENI décembre 2012

[11] : Cédric Lorens, Informatique et Réseau d'un opérateur de télécommunication, édition

[12] : TOM Thomas, La sécurité des réseaux, First-step, ISBN : 2-7440-17868, 2005

[13] : M.GUERMAH, les réseaux privés virtuels : accès sécurisé aux réseaux informatique, conférences BLIDA 2010.

[14] : www.les meilleursvpn.fr, Derniers accès Avril 2016.

[15] : http://fr.scribd.com/doc/101326989/Chap-8-Les-VPN Derniers accès Juin 2015.

[16] : Christophe WOLFHUGEL, Déploiement de VLAN 802.1Q/ISL dans un environnement hétérogène, France Telecom Oléane, 2000

[17] : CHAMILLARD G., ROHAUT S., (création, configuration et gestion d'un réseau local d'entreprise), ENI édition, 2013.

Références bibliographiques

[18] : Génael VALET, les LANs virtuels (VLANs), support de cours, Greta industriel de technologies avancées, Avril 2007

[19] : C.Llorens, L. levier, D. Valois. Tableaux de bord de la sécurité. Groupe Eyrolle, 2003-2006, ISBN : 2-212-119

[20] : http://www.ybet.be Derniers accès Avril 2016

Résumé

De nos jours, la sécurité informatique est quasi-indispensable pour le bon fonctionnement de n'importe quel réseau informatique. Pour cela, les administrateurs réseau doivent mettre des mécanismes de gestion et de sécurité plus robuste de leur réseau. Notre travail consiste en une proposition d'une configuration sécurisé pour le réseau informatique de NAFTAL. Les concepts fondamentaux des réseaux locaux sont bien explicités, les différents mécanismes de sécurité y sont étudiés. Nous avons présenté et étudié l'architecture du réseau, ensuite, nous avons implémenté une solution sécurisé comprenant les listes de contrôle et des mots de passe au niveau du routeur avec le logiciel Cisco Packet Tracer basé sur les Vlans.

Mots clés : réseau local, sécurité, VLAN, ACL, Packet Tracer.

Abstract

Nowadays, computer security is almost indispensable for the proper functioning of any computer network. To do this, network administrators must put more robust management and security mechanisms in their network. Our work is a proposal of a secure configuration for the computer network NAFTAL. The fundamental concepts of local networks are well clarified, different security mechanisms are studied there. We presented and studied architecture of the network, then, we have implemented a secure solution including control list and password on the router with the Cisco Packet Tracer software based on VLANs.

Keywords: LAN, security, VLAN, ACL, Packet Tracer.