**Université Abderrahmane Mira –Bejaia**

**Faculté des Sciences Exactes**

**Département d'Informatique**

# Mémoire de fin de cycle

***En vue de l'obtention du Diplôme de Master professionnel en Informatique***

**Option : Administration et Sécurité des Réseaux**

THÈME

# Etude et amélioration de l'architecture et sécurité du réseau NAFTAL BITUMES de la Wilaya de BEJAIA

***Réalisé par :***

M^elle^ KESSOURI hanane

M^elle^ MAIZIA Kamilia

***Devant le jury composé de :***

**Président :** Mr. KHENOUS Lachemi

**Examinateur :** Mr. LARBI Ali

**Encadreur :** Mr. SADI Mustapha

**Coo-Encadreur :** Mr. BOUYOUCEF Adel

**Promotion 2019-2020**

# *Remerciements*

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

Nous tenons à remercier Mr SADI Mustapha notre promoteur pour ses précieux conseils et son orientation tout au long de notre recherche.

Nous remercions de même notre encadreur de stage Mr. BOUYOUCEF Adel l'administrateur réseau au sein de l'entreprise NAFTAL BITUMES de la wilaya de BEJAIA pour son encadrement et encouragement pendant la réalisation de notre travail.

Nos remerciements s’adressent également aux membres du jury qui nous ont honorés en acceptant d’examiner notre travail et surtout d’y avoir apporté un jugement critique et objectif à ce travail.

Enfin, nous tenons également à remercier nos parents, toutes nos familles, nos ami(e)s et tous ceux qui ont participé de près ou de loin à la réalisation de ce travail.

# Dédicaces

*Je dédie ce modeste travail :*

*À ma chère mère tes encouragements et tes prières ont été d'un grand soutien pour moi je te remercie infiniment.*

*À mon cher père pour sa présence dans ma vie, de son soutien et tous ses sacrifices et ses précieux conseils.*

*À mon marie qui m'a soutenu et qui a toujours été là pour moi, à toi Halim.*

*À mes frère hasni et chawki, à qui je souhaite toute la réussite du monde ainsi que tout le bonheur et que Dieu vous protège inchallah.*

*À ma belle-famille pour l'encouragement.*

*À mes chers grands-parents pour leurs prières et leurs conseils.*

*À celle qui a partagé tout cela avec moi Kamilia et toute sa famille.*

*À Toute ma famille sans exception, à tous nos chers amis (e) pour leurs encouragements.*

*Hanane*

# Dédicaces

*Du profond de mon cœur, je dédie ce modeste travail à tous ceux qui me sont chers :*

*À mon père qui m'as encouragé à aller de l'avant et qui m'a donné tout son soutien moral et matérielle afin de réaliser mes projets.*

*À ma mère qui m'a soutenu et m'a donné la force et la volonté durant ma scolarité.*

*À mes frères Habib, Mehrez et ma sœur Anissa à qui je souhaite toute la réussite et le bonheur de monde.*

*À mes chers grands-parents pour leurs prières et leurs conseils.*

*À toute ma famille.*

*À celle qui a partagé tout ce travail avec moi hanane et toute sa famille.*

*À Toute ma famille sans exception, à tous nos chers amis (e) pour leurs encouragements.*

*Kamilia*

# Liste d'abréviations

| | |
|---|---|
| **ACE** | Access Control Entry |
| **ACL** | Access Control List |
| **ADSL** | Asymetric Digital Subscriber Line |
| **AES** | Advanced Encryption Standard |
| **AH** | Authentification Header |
| **ARP** | Address resolution Protocol |
| **BOOTP** | Bootstrap Protocol |
| **BWA** | Broadband Wireless Access |
| **CD** | Centre de Stockage |
| **CFI** | Canonical Format Identifier |
| ***DoS*** | Denial of Service |
| **DHCP** | Dynamic Host Configuration Protocol) |
| **ESP** | Encapsulating Security Payload |
| **FDDI-2** | Fiber Distributed Data Interface |
| **FTP** | File Transfer Protocol |
| **Http** | HyperText Transfer Protocol |
| **HTTPS** | HyperText Transfer Protocol Secure |
| **IP** | Internet Protocol |
| **IPsec** | Internet Protocol Security |
| **ISAKMP** | Internet Security KeyManagement Protocol |
| **ISL** | Inter Switch Link Protocol |
| **LAN** | Local Area Network |
| **LLC** | Limited Liability Company |
| **L2F** | Layer Tow Forwarding |
| **L2TP** | Layer Two Tunneling Protocol |
| **MAC** | Media Access Control |

| | |
|---|---|
| **MAN** | Metropolitan Area Network |
| **MAU** | Multistation Access Unit |
| ***MITM*** | Man In The Middle |
| **MPLS** | Multi Protocol Label Switching |
| **MVRP** | Multiple VLAN Registration Protocol |
| **MPLS** | Multi Protocol Label Switching |
| **NIC** | Network Interface Card |
| **OSI** | Open System Interconnection |
| **PAN** | Personnal Area Network |
| **PME** | Petites et Moyennes Entreprises |
| **POP3** | Post Office Protocol |
| **PPP** | Point to Point Protocol |
| **PPTP** | Point To Point Tunneling Protocol |
| **QoS** | Quality of Service |
| **SA** | Security Association |
| **SHA** | Secure Hash Algorithm |
| **SLC** | Smart Link C ommunication |
| **SP** | Security Policy |
| **SSH** | Secure Shell |
| **SSL** | Secure Sockets Layer |
| **STP** | Spanning-Tree |
| **TCI** | Tag Control Information |
| **TCP** | Transmission Control Protocol |
| **TCP** | Transmission Control Protocol |
| **TCP** | Transmission Control Protocol |
| **TLS** | Transport Layer Security |
| **TPID** | Tag Protocol Identifier |
| **UDP** | User Datagram Protocol |

| | |
|---|---|
| **VID** | VLAN Identifier |
| **VLAN** | Virtual Local Area Network |
| **VPN** | Virtual Private Network |
| **VTP** | VLAN Trunking Protocol |
| **WAN** | Wide Area Network |

# Table des matières

# Table de figures

# Introduction générale

Dans les grandes entreprises internationales, l'informatique représente une pièce maîtresse et un outil stratégique dans le développement de ces entreprises. Il leur permet de réagir rapidement et de répondre aux besoins de leurs clients de plus en plus exigeants. De plus, elles doivent faire face à la concurrence active, souvent le système informatique est constitué par un système homogène de gestion et de communication de données permettant les échanges internes et externes d'une manière réactive et sécurisée.

Toute entreprise ou établissement ayant un accès à cet outil est en possession de diverses informations privées, peuvent être en proie de cyber attaques. Ces cybers attaques ont pour but d'interrompre le fonctionnement d'un réseau informatique, d'intercepter et modifier les informations.

La sécurité se place actuellement au premier plan de la mise en œuvre et de l'administration des réseaux Informatiques. De plus, elle est devenue l'un des éléments-clés de la continuité des systèmes d'information de l'entreprise quelles que soient son activité, sa taille et sa répartition géographique; ainsi la nécessité de protéger les données stratégiques et les services disponible d'un réseau des différentes attaques interne et externe, nous pousse à sécuriser le réseau de cette entreprise en organisant l'ensemble des accès, par l'implémentation des réseaux virtuel pour un meilleur contrôle d'accès, de ce fait nous améliorons la sécurité de réseau.

L'objectif de notre mémoire de fin de cycle est donc d'étudier et améliorer l'architecture et la sécurité du réseau au sein de l'entreprise NAFTAL BITUMES de la wilaya de BEJAIA.

Pour bien mener ce travail, nous présenterons en détail les étapes que nous avons suivi pour réaliser notre projet, qui est subdivisé en quatre chapitres, organisés comme suit :

Le premier chapitre sera consacré à « Généralités sur les réseaux et la sécurité informatique », en décrivant les types de réseau ainsi que leurs caractéristiques, ensuite nous présenterons des différentes techniques de sécurité utilisées et plus particulièrement celle des réseaux locaux.

Dans le deuxième chapitre nommé « Les réseaux virtuels », nous définirons en premier lieu ce qu'est un réseau local virtuel, ensuite nous parlerons sur les réseaux privés virtuel leur fonctionnement et leurs objectifs. Nous finirons par citer les différents protocoles de mise en place.

Le troisième chapitre titré « Etude de l'existant » consacré à l'étude de l'architecture actuelle du réseau Intranet de l'entreprise pour mieux comprendre l'organisme et sa structure. Nous allons donc évoquer la problématique ainsi que la solution adéquate.

Dans le quatrième et dernier chapitre, nous allons enfin passer à la « Réalisation ». Cette phase est décomposée en deux parties: dans la première nous introduirons l'outil ayant servi à l'élaboration du projet, tout en expliquant leurs détails, nous passerons ensuite à la deuxième partie qui sera principalement consacrée à l'implémentation des solutions, VLANs et les VPN.

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

# Chapitre 1 : Généralités sur les réseaux et la sécurité informatique

## Introduction

Le besoin de communication et de partage a poussé les entreprises à s'orienter vers les réseaux informatiques et travailler d'avantages pour les améliorer et pour les sécuriser. La sécurité consiste à assurer que les ressources matérielles ou logicielles d'une organisation soient uniquement utilisées dans le cadre prévu.

Ce chapitre a pour objectif de comprendre les notions de bases sur les réseaux informatiques, ainsi la sécurité informatique, nous allons montrer les moyens et les dispositifs de sécurité utilisés pour l'assurer afin de bien maitriser notre sujet.

## I. Généralité sur les réseaux

### I.1. Réseaux informatiques

Un réseau informatique est l'ensemble des ressources de communication (matérielles et logicielles), d'ordinateurs et des clients cherchant à exploiter ces ressources afin de répondre à un besoin d'échange d'informations**.**

### I.2. Classification des réseaux informatiques

On trouve différents types de réseaux selon leur taille, leur vitesse de transfert des données ainsi que leur étendue. Pour cela on distingue deux réseaux, les réseaux avec fil et les réseaux sans fil.

#### I.2.1. Réseaux avec fil

Le réseau filaire comme son nom l'indique est un réseau que l'on utilise grâce à une connexion avec fil. Ce réseau utilise des câbles Ethernet pour relier des ordinateurs et des périphériques grâce à un routeur ou à un commutateur [1].

- **Un réseau personnel (PAN : Personnal Area Network)** interconnecte (souvent par des liaisons sans fil) des équipements personnels comme un ordinateur portable, un agenda électronique, etc.
- **Un réseau local (LAN : Local Area Network**) peut s'étendre de quelques mètres à quelques kilomètres et correspond au réseau d'une entreprise. Il peut se développer sur plusieurs bâtiments et permet de satisfaire tous les besoins internes de cette entreprise.

- **Un réseau métropolitain (MAN : Métropolitain Area Network)** interconnecte plusieurs lieux situés dans une même ville, par exemple les différents sites d'une université ou d'une administration, chacun possédant son propre réseau local.
- **Un réseau étendu (WAN : Wide Area Network)** permet de communiquer à l'échelle d'un pays ou de la planète entière, les infrastructures physiques pouvant être terrestres ou spatiales à l'aide de satellites de télécommunications.
- **Un réseau de stockage (SAN : Storage Area Network)** est un réseau à haute performance dédié qui permet de transférer des données entre des serveurs et des ressources de stockage. Du fait qu'il s'agit d'un réseau dédié distinct, il évite tout conflit de trafic entre les clients et les serveurs et permet de bénéficier d'une connectivité haut débit.

Le schéma ci-dessous représente les types de réseaux avec fil


*Figure 1 : Types de réseaux avec fil.*

## I.2.2. Réseaux sans fil

Un réseau sans fil (en anglais wireless network) est un réseau dans lequel au moins deux équipements peuvent communiquer sans liaison filaire. Ils existent en plusieurs types :

- **Un réseau personnel sans fil (WPAN : Wireless Personal Area Network)** concerne les réseaux sans fil d'une faible portée : de l'ordre de quelques dizaines de mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques, ...).

- **Un réseau local sans fil (WLAN : Wireless Local Area Network)** est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres.

- **Un réseau métropolitain sans fils (WMAN : Wireless Metropolitan Area Network)** est connu sous le nom de Boucle Locale Radio (BLR), est destiné principalement aux opérateurs de télécommunication.

- **Un réseau étendu sans fil (WWAN : Wireless Wide Area Network)** est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fil les plus répandus, puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil.

La figure suivante représente les types de réseaux sans fil.

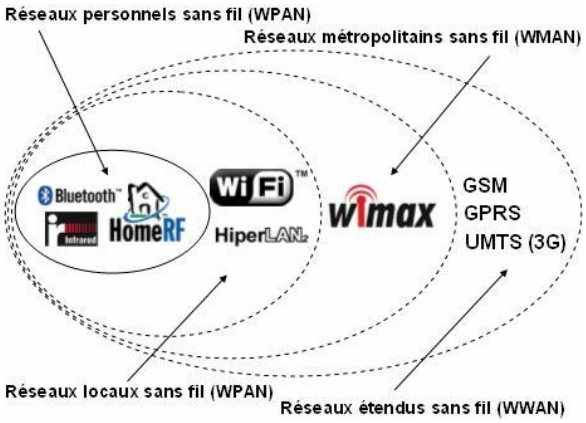


*Figure 2 : Types de réseaux sans fil.*

### I.2.2.1. WIMAX

WiMAX (acronyme pour Worldwide Interoperability for Microwave Access) désigne un standard de communication sans fil. L'utilisation de WiMAX est très semblable à celle d'un modem ADSL, au lieu de placer du câble on utilise la voie hertzienne. Aujourd'hui il est surtout utilisé comme mode de transmission et d'accès à Internet haut débit, portant sur une zone géographique étendue, basée sur le standard de transmission radio 802.16 validé en 2001 par l'organisme international de normalisation IEEE. Idéal pour les entreprises et les usagers, vise à satisfaire les besoins des entreprises en matière d'accès à l'internet haut débit. La solution WiMax est particulièrement appréciée par les professionnels, cette technologie délivre une connexion fiable et un volume de consommation de données illimitées afin de remplacer un débit ADSL médiocre [2].

### I.2.2.2. Fonctionnement des WIMAX

Les WIMAX fonctionne en mode point-multipoint, c'est-à-dire le mode infrastructure que l'on connait sur le Wifi ou encore le même fonctionnement que les technologies GSM. D'une façon hertzienne, la connexion Internet permet de se propager par la « voie des airs ». Un dispositif de réseau d'antennes est présent sur les reliefs afin de distribuer un débit internet dans les lieux à l'écart des villes, cette technologie est privilégiée pour les entreprises. Actuellement, le réseau permet de distribuer un flux Internet haut débit. Contrairement à l'Internet par satellite et l'Internet mobile, le WiMax propose un volume de données illimitées [2].

### I.2.2.3. Les avantages des WIMAX

Le WiMax offre un accès à l'Internet sans avoir besoin de ligne téléphonique, d'abonnement ADSL ou de câble de télédistribution. Cela veut donc dire que seule une prise de courant est nécessaire afin que le modem puisse faire le lien avec le réseau sans fil. Voici d'autres avantages de WIMAX [2] :

- Mobilité et interopérabilité.
- Facilité de déploiement.
- Connexion haut débit, permanente, sécurisée et large bande passante.
- Facilité de maintenance et d'administration.
- Adaptation au déploiement temporaire.
- Large zone de couverture.

### I.2.2.4. Domaines d'application des WIMAX

Le WIMAX est typiquement utilisé comme étant une alternative aux liaisons spécialisées et accès Internet de toutes sortes pour les applications suivantes :

- Réseaux privés inter-sites pour les entreprises.
- Communications sans fils intégrant la VoIP.
- Réseaux urbains avec de hautes vitesses de transmission pour la voix et les données.
- Sécurité publique et surveillance pouvant inclure des applications vidéo sur IP Relais sans fil pour les Hot Spot Wifi.
- Réseaux sans fils régionaux avec de applications données et voix pour l'industrie et les transports.

## I.3. Topologies des réseaux informatiques

La manière dont sont interconnectées les machines est appelée « topologie ». On distingue la topologie physique (la configuration spatiale, visible du réseau) de la topologie logique .

### I.3.1. Topologie logique

Elle représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token-ring et FDDI2.

### I.3.2. Topologie physique

Elle désigne la manière dont les équipements sont interconnectés en réseau. Dans cette topologie nous avons trois grandes topologies qui sont : topologie en bus, topologie en étoile et la topologie en anneau, la figure 3 illustre les types de topologies physiques.

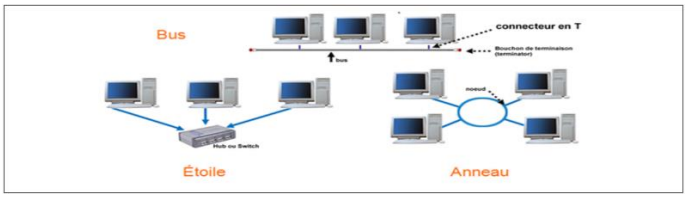


*Figure 3 : Types des topologies physiques.*

## I.4. Equipements d'un réseau informatique

Les équipements d'un réseau informatique sont les composants matériels et/ou logiciels nécessaire pour connecter un périphérique à un réseau ou pour connecter un réseau à un autre. On peut les classer en deux groupes : les équipements de base et les équipements d'interconnexion.

### I.4.1. Equipements de base

Les principaux équipements de bases nécessaire pour la mise en place d'un réseau sont : Les ordinateurs, les câbles réseaux et les serveurs. Ce schéma ci-dessous (Figure 4), nous illustre les équipements de base.

*Figure 4 : les équipements de base.*

### I.4.2. Equipements d'interconnexion

Un équipement d'interconnexion est un matériel qui permet de relier les ordinateurs d'un réseau ou plusieurs réseaux entre eux. Il existe plusieurs équipements d'interconnexion on peut citer : Hubs, Switch, Routeurs, Passerelles, voir la figure ci-dessous.


*Figure 4 : Les équipements d'interconnexion.*

## I.5. Modèle OSI (Open System Interconnection)

Le modèle OSI est un modèle de référence pour décrire et expliquer les communications dans un réseau. Il décrit sept couches portant les noms de couche physique, liaison, réseau, transport, session, présentation et application. Les divers protocoles qui définissent le réseau et les communications sont donc répartis dans chaque couche, selon leur utilité. Il est d'usage de diviser ces sept couches en deux : les couches basses, qui se limitent à gérer des fonctionnalités de base, et les couches hautes, qui contiennent les protocoles plus élaborés [3].

### I.5.1. Couches basses

Les couches basses aussi appelées *couches matérielles*, s'occupent de tout ce qui est traité au bas-niveau, c.à.d. au matériel. Elles permettent d'envoyer un paquet de données sur un réseau et garantir que celui-ci arrive à destination. Elle est généralement prise en charge par le matériel et le système d'exploitation, mais pas du tout par les logiciels réseaux. Les couches basses sont donc des couches assez bas-niveau, peu abstraites et de nombre de trois. Pour résumer, ces trois couches s'occupent respectivement de la liaison point à point (entre deux ordinateurs/équipements réseaux), des réseaux locaux, et des réseaux Internet.

- **La couche physique :** s'occupe de la transmission physique des bits entre deux équipements réseaux. Elle s'occupe de la transmission des bits, leur encodage, la synchronisation entre deux cartes réseau, etc. Elle définit les standards des câbles réseaux, des fils de cuivre, du WIFI, de la fibre optique, ou de tout autre support électronique de transmission.

- **La couche liaison :** s'occupe de la transmission d'un flux de bits entre deux ordinateurs, par l'intermédiaire d'une liaison point à point ou d'un bus. Pour simplifier, elle s'occupe de la gestion du réseau local. Elle prend notamment en charge les protocoles MAC, ARP, et quelques autres.
- **La couche réseau :** s'occupe de tout ce qui a trait à internet : l'identification des différents réseaux à interconnecter, la spécification des transferts de données entre réseaux, leur synchronisation, etc. C'est notamment cette couche qui s'occupe du routage, à savoir la découverte d'un chemin de transmission entre récepteur et émetteur, chemin qui passe par une série de machines ou de routeurs qui transmettent l'information de proche en proche. Le protocole principal de cette couche est le protocole IP.

### I.5.2. Couches hautes

Les couches hautes, aussi appelées couches logicielles, contiennent des protocoles pour simplifier la programmation logicielle. Elles requièrent généralement que deux programmes communiquent entre eux sur le réseau. Elles sont implémentées par des bibliothèques logicielles ou directement dans divers logiciels. Le système d'exploitation ne doit pas, en général, implémenter les protocoles des couches hautes. Elles sont au nombre de quatre :

- **La couche transport :** permet de gérer la communication entre deux programmes, deux processus. Les deux protocoles de cette couche sont les protocoles TCP et UDP.
- **La couche session :** comme son nom l'indique, permet de gérer les connexions et déconnexions et la synchronisation entre deux processus.
- **La couche présentation :** se charge du codage des données à transmettre. Elle s'occupe notamment des conversions de boutisme ou d'alignement, mais aussi du cryptage ou de la compression des données transmises.

La figure 5 montre les couches du modèle OSI.

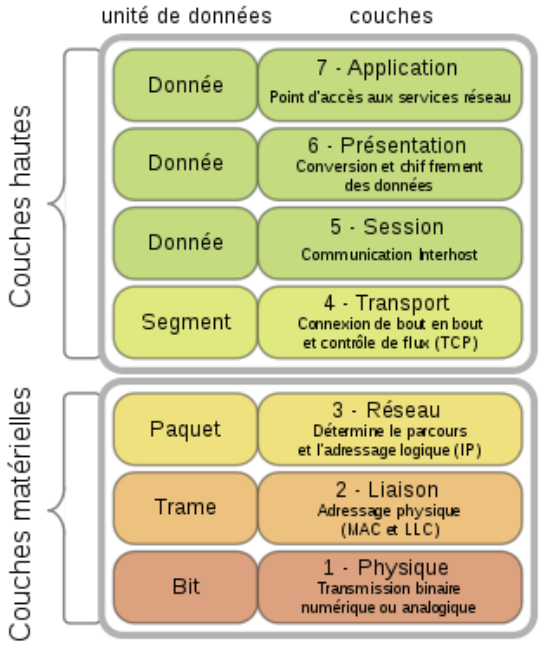


*Figure 5 : Les couches du Modèle OSI.*

## I.6. Modèle TCP/IP

Contrairement au modèle OSI, le modèle TCP/IP est né d'une implémentation mais il est inspiré du modèle OSI. Il reprend l'approche modulaire (utilisation de modules ou couches) mais en contient uniquement quatre. Les trois couches supérieures du modèle OSI sont souvent utilisées par une même application. Afin de connaitre les services de chaque couche on va les présenter brièvement ci-dessous l'une après l'autre [3] :

- **Couche application :** Le modèle TCP/IP regroupe en une seule couche tous les aspects liés aux applications et suppose que les données sont préparées de manière adéquate pour la couche suivante.
- **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, fournit d'excellents moyens de créer avec souplesse, des communications réseau fiables.
- **Couche Internet :** Le rôle de la couche Internet consiste à envoyer des paquets source à partir d'un réseau quelconque de l'inter réseau et à les faire parvenir à destination, indépendamment du trajet et des réseaux traversés pour y arriver. Le protocole qui régit cette couche est appelé protocole IP (Internet Protocol). L'identification du meilleur chemin et la commutation de paquets ont lieu au niveau de cette couche.

– **Accès Réseau :** C'est la couche la plus basse de la pile TCP/IP. Elle contient toutes les spécificités concernant la transmission des données sur un réseau physique, elle spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé et elle permet la Conversion des signaux analogiques/numériques. Elle est composée par deux niveaux MAC, LLC.

La figure (6) montre la correspondance entre le modèle OSI et TCP/IP :

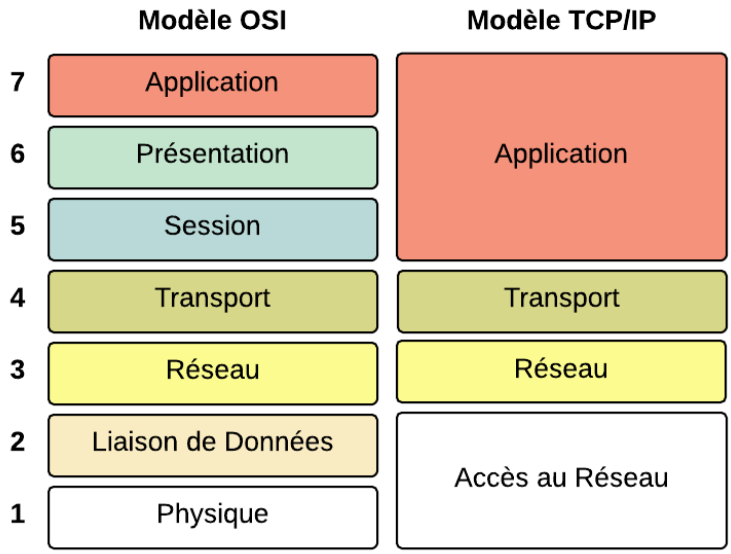


*Figure 6 : Comparaison entre le modèle TCP/IP et le modèle OSI.*

## I.7. Le protocole IP

Le protocole IP (Internet Protocol) est un protocole réseau de niveau trois, permet d'émettre des paquets d'informations à travers le réseau, il est utilisé pour dialoguer les machines entre elles. Ainsi, il offre un service d'adressage unique pour l'ensemble des machines. Il n'est pas orienté connexion, c'est à dire qu'il n'est pas fiable cela ne signifie pas qu'il n'envoie pas correctement les données sur le réseau, mais n'offre aucune garantie pour les paquets envoyés sur l'ordre d'arrivée et la perte ou la destruction des paquets, cette fiabilité dépend de la couche de transport [4].

# II. Sécurité informatique

## II.1. Définition

La notion de sécurité informatique c'est l'ensemble des moyens, outils, techniques et méthodes mise en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles où Intentionnelles.

## II.2. Objectif de la sécurité informatique

La sécurité informatique vise généralement cinq principaux objectifs :

- **L'intégrité**, permet de certifier que les données, les traitements ou les services n'ont pas été modifiés, altérés ou détruits tant de façon intentionnelle qu'accidentelle.
- **La confidentialité,** le service qui garantit que l'information est secrète, elle n'est compréhensible que par les entités ayant le droit d'y accéder.
- **La disponibilité,** l'information sur le système doit être toujours disponible aux personnes autorisées.
- **La non répudiation,** permettant de garantir qu'une transaction ne peut être niée.
- **L'authentification,** c'est la propriété qui vérifie l'identité d'un émetteur d'un message [5].

## II.3. Attaques informatiques

Une attaque est l'exploitation d'une faille d'un système informatique à des fins non connues par l'exploitant du système et généralement préjudiciable. Il existe différents types d'attaques, selon le mode d'opération utilisé. Nous en définirons certains des plus connues, et des plus répandues [6] :

- **Le déni de service :** Denial Of Service, plus communément abrégé *DoS*, est un fléau visant à atteindre tout serveur d'entreprise, en particulier relié à l'Internet. Cette attaque rend indisponible pendant un temps indéterminé les services ou ressources d'une organisation, dans le but non pas d'altérer les données mais de nuire à la réputation des sociétés et à leur fonctionnement. La plupart passant par des failles d'un protocole de modèle TCP/IP. Les attaques par déni de service ont pour principes de submerger des requêtes, en y envoyant des paquets IP afin de saturer les services réseau qu'elle propose.

- **L'usurpation d'adresse IP :** Plus communément appelé en anglais *SpoofingIP*, est une technique de remplacement d'adresse IP, usurpant alors l'identité de l'ordinateur, et permettant d'envoyer des paquets anonymement. Le pirate peut donc faire passer des paquets sur un réseau sans que ceux-ci ne soient interceptés par le système de filtrage (Pare-feu). Ainsi, un paquet *spoofé* avec l'adresse IP d'une machine interne semblera provenir du réseau interne et sera relayé à la machine cible, tandis que sans cela, si le paquet provenait d'une machine externe, le pare-feu le rejetterait.
- **Man In The Middle :** Parfois annoté *MITM*, est un type d'attaque visant à falsifier des échanges entre deux parties, en passant par l'écoute des communications. La plupart utilisant un outil appelé *sniffé.* Cela peut se produire, en se faisant passer pour l'un des deux interlocuteurs, ou encore dans un autre scénario, si le pirate intercepte une communication lorsque l'utilisateur est sur un serveur au moment de l'authentification, il se verra accéder à ses noms d'utilisateurs et mots de passe, et si le système le permet, il pourra même le modifier, y bloquant ainsi l'accès.
- **Attaques permettant d'écouter le trafic réseau (sniffing) :** L'attaque par sniffing est généralement utilisée par les pirates pour capturer les mots de passe. Lorsqu'on se connecte à un réseau qui utilise le mode broadcast, toutes les données en transit arrivent à toutes les cartes réseau connectées à ce réseau. En temps normal, seules les trames destinées à la machine sont lues, les autres étant ignorées. Grace à un snifer, il est possible d'intercepter les trames reçues par la carte réseau d'un système pirate et qui ne lui sont pas destinées.
- **Attaque par force brute :** On appelle ainsi « attaque par force brute » (en anglais « brute force cracking », parfois également attaque exhaustive) le cassage d'un mot de passe en testant tous les mots de passe possibles. Il existe un grand nombre d'outils, pour chaque système d'exploitation, permettant de réaliser ce genre d'opération. Ces outils servent aux administrateurs système à éprouver la solidité des mots de passe de leurs utilisateurs mais leur usage est détourné par les pirates informatiques pour s'introduire dans les systèmes informatiques.

## II.4. Stratégies de sécurité

Une stratégie de sécurité contient des procédures organisationnelles qui vous indiquent quoi faire pour prévenir les problèmes. Il est nécessaire, autant pour les réseaux d'entreprises que pour les internautes possédant une connexion de type câble ou ADSL, de se protéger des attaques réseaux en installant un dispositif de protection (Pare-feux, antivirus, réseaux privés

virtuels, systèmes de détection d'intrusions, Proxys, etc.) permettant d'ajouter un niveau de sécurisation supplémentaire.

### II.4.1. Solutions de sécurité primaire :

C'est l'ensemble des mesures offrant le minimum en matière de sécurité tel que : [7]

- Authentification des utilisateurs par login et mot de passe.
- Suppression des informations confidentielles des machines reliées au réseau si elles n'ont pas besoin d'y être.
- Protection physique des machines contenant des informations sensibles.
- Installation d'un logiciel anti-virus mit à jour.

#### II.4.1.1. Pare-feu

Appelé aussi Coupe-feu, Garde-barrière ou Firewall, est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers ,notamment Internet. Le Pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau (cartes réseau) suivantes :

- Une interface pour le réseau à protéger (réseau interne).
- Une interface pour le réseau externe.

Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes. Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel système pourvu que :

- La machine soit suffisamment puissante pour traiter le trafic.
- Le système soit sécurisé.
- Aucun autre service excepté le service de filtrage de paquets ne fonctionne sur le serveur [8].

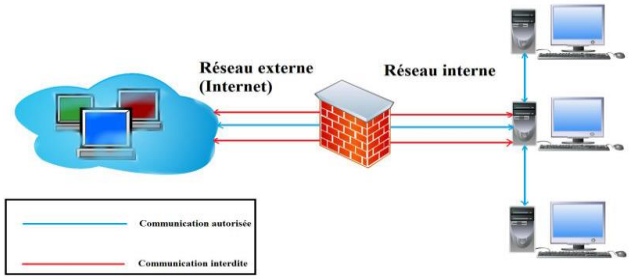


*Figure 7 : exemple d'un réseau avec pare-feu.*

### II.4.1.2. Liste de contrôle d'accès (ACL)

Les administrateurs réseau doivent trouver le moyen d'interdire l'accès au réseau à certains utilisateurs tout en permettant aux utilisateurs internes d'accéder aux services nécessaires. Les routeurs assurent cette fonction à l'aide des listes de contrôle d'accès. Une ACL est un ensemble de conditions qui est appliqué au trafic circulant via une interface du routeur. Elle indique au routeur les types des paquets à accepter ou à rejeter. Les ACLs permettent de gérer le trafic et de sécuriser l'accès d'un réseau en entrée comme en sortie, (la figure 8) [9].

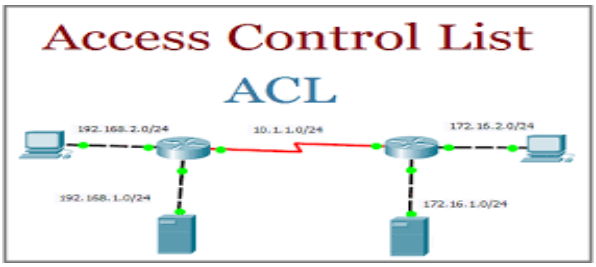


*Figure 8 : Schéma d'un réseau avec ACL.*

### II.4.1.3. Proxy

Un système mandataire (Proxy) repose sur un accès à l'Internet par une machine dédiée : le serveur mandataire ou Proxy server joue le rôle de mandataire pour les autres machines locales et exécute les requêtes pour le compte de ces dernières.

Un serveur mandataire est configuré pour un ou plusieurs protocoles de niveau applicatif (http, FTP, SMTP, etc.) et permet de centraliser, donc de sécuriser les accès extérieurs (filtrage applicatif, enregistrement des connexions, masquage des adresses des clients, etc.). Les serveurs mandataires configurés pour http permettent également le stockage de pages web dans un cache pour accélérer le transfert des informations fréquemment consultées vers les clients connectés. La figure 9 montre un réseau avec proxy [10].

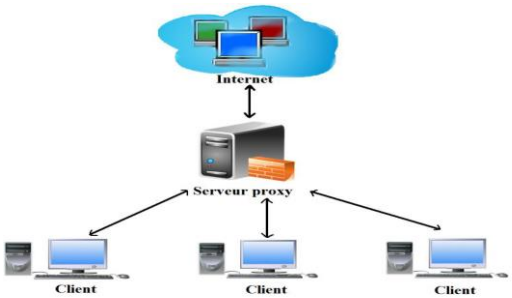


*Figure 9 : Schéma d'un réseau avec proxy.*

### II.4.1.4. Cryptographie

La cryptographie est l'étude de méthodes de chiffrement et de déchiffrement. Elle permet d'assurer l'authenticité, l'intégrité et la confidentialité des données, il existe deux types de cryptographies [10] :

- **Cryptographie symétrique :** Elle est basée sur une clé unique partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypter les messages la figure 10 montre la cryptographie symétrique.

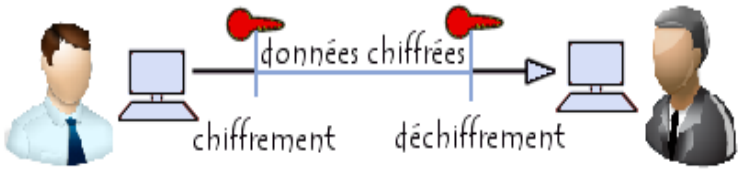


*Figure 10 : la cryptographie symétrique.*

- **Cryptographie asymétrique (à clé publique) :** Contrairement à la cryptographie symétrique, la cryptographie asymétrique utilise deux clés : une clé est privée et n'est connue que par l'utilisateur, l'autre est publique et donc accessible par tout le monde voir la figure 11.

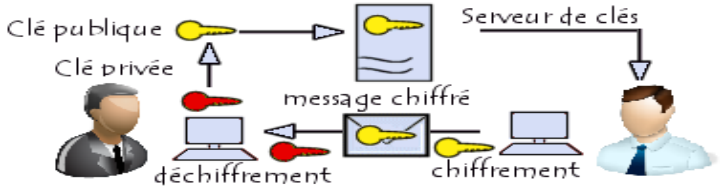


*Figure 11: la cryptographie asymétrique.*

### II.4.1.5. Hachage

Le hachage est appelé aussi fonction de hachage, c'est une fonction qui convertit une chaîne de longueur quelconque en une chaîne de taille inférieure et généralement fixe, le résultat de cette fonction est appelé une empreinte. Une fonction de hachage qui est aussi une fonction à sens unique, c'est-à-dire il est très difficile de trouver une chaîne qui donne cette empreinte.

### II.4.1.6. Signature numérique

Une signature numérique est une empreinte (d'un document) chiffrée par la clé privée de l'auteur, cette empreinte chiffrée étant jointe au document original. La signature permet ainsi de vérifier l'intégrité du document et l'identité de l'expéditeur. La signature d'un document est assurée via des fonctions de hachage.

### II.4.1.7. Réseau local virtuel (VLAN)

Nombreuse sont les entreprises à recourir à la technologie VLAN, afin d'améliorer la sécurité et les performances de leur réseaux locaux. Un VLAN est un regroupement de stations de travails indépendamment de la localisation géographique sur le réseau, ces dernières pourront communiquer comme si elles étaient sur le même segment. Un VLAN permet de créer des domaines de diffusion (domaines de *broadcast*) gérés par les commutateurs indépendamment de l'emplacement où se situent les nœuds, ce sont des domaines de diffusion gérés logiquement. La figure suivante représente un réseau VLAN.

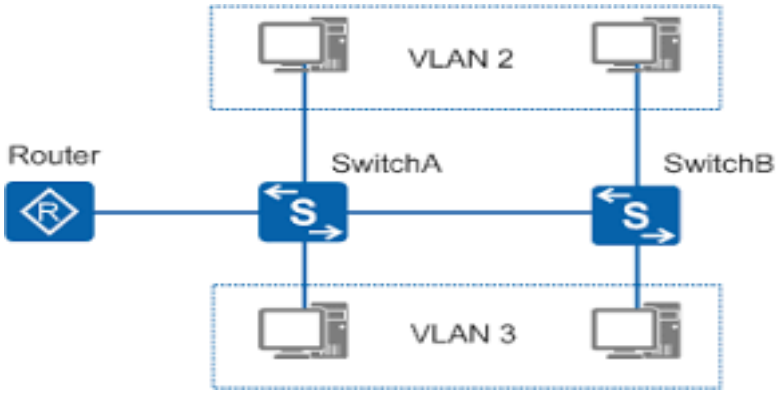


*Figure 12 : Schéma d'un réseau VLAN.*

### II.4.1.8. Les réseaux privés virtuel

Les réseaux privés virtuels sont utilisés pour interconnecter des réseaux locaux à travers un réseau public comme Internet. Ils reposent sur le principe de création d'un tunnel virtuel dont les extrémités identifiées appartiennent à deux réseaux locaux différents, les données circulent alors dans ce tunnel après avoir était chiffrée, le principale avantage des VPN est interconnecter des réseaux à moindre coût à travers un réseau publique au lieu d'utilisation de lignes dédiées très couteuses, voir la figure 13.


*Figure 13 : Schéma d'un réseau VPN.*

# III. Conclusion

Ce chapitre nous a permis en premier lieu de découvrir et de mieux comprendre les notions et les aspects élémentaires des réseaux informatiques, où nous avons décrit les modèles OSI et TCP/IP, et en deuxième lieu de comprendre les concepts et objectifs de la sécurité informatique, et plus particulièrement la sécurité des réseaux où nous avons présenté brièvement les différentes politiques sécuritaires, comme les pare-feu, les proxys et surtout les VLANs et VPNs que nous aborderons en détails dans le chapitre suivant

# CHAPITRE 2 : Les réseaux virtuels

## Introduction

De nos jours, il est pratiquement devenu indispensable pour toute entreprise de posséder son propre parc de réseau informatique interne, permettant ainsi la communication de données ou tout simplement d'informations d'un pôle d'une entreprise à une autre. Cependant, pour des raisons sécuritaires principalement, il est parfois nécessaire de segmenter le réseau de façon logique en plusieurs réseaux virtuels. Comme sur Internet, on ne sait pas par où passent les données car les chemins changent. Ces données peuvent donc être écoutées ou interceptées. Il n'est donc pas envisageable de faire connecter deux LAN entre eux par Internet sans sécuriser le cheminement des données échangées. Dans ces conditions, l'Internet fournit des solutions VPN (Virtual Private Network) idéale pour pouvoir exploiter au mieux les capacités de ce réseau des réseaux et relier des sites distants.

Dans ce chapitre, nous allons présenter les principales notions d'un réseau local virtuel, les méthodes d'implémentation des VLANs, ces protocoles de transport, ces protocoles d'administration et de gestion des VLANs et enfin les avantages des VLANs. Par la suite, nous allons présenter quelques notions sur les réseaux privés virtuels, fonctionnement de VPN et ces caractéristiques, les typologies, ces principaux protocoles ainsi les catégories des VPNs.

## I. Les réseaux locaux virtuels

### I.1. Définition des VLANs

Le développement rapide d'Internet a mené de nombreuses entreprises à étendre leur installation informatique. La technologie VLAN apporte des solutions nouvelles dans la segmentation et la sécurisation des réseaux locaux, tout en augmentant leurs performances. Par définition, un VLAN ou réseau virtuel est un regroupement de postes de travail indépendamment de la localisation géographique sur le réseau. Ces stations pourront communiquer comme si elles étaient sur le même segment. Un VLAN est assimilable à un domaine de diffusion (Broadcast Domain). Ceci signifie que les messages de diffusion émis par une station d'un VLAN ne sont reçus que par les stations de ce VLAN. Ces derniers n'ont été réalisables qu'avec l'apparition des commutateurs (Switches) [9].

## I.2. Types des VLAN

Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue [9] :

- VLAN de niveau 1 (aussi appelés VLAN par port, en anglais Port-Based VLAN) : définit un réseau virtuel en fonction des ports de raccordement sur le commutateur, cela permet entre autres de pouvoir distinguer physiquement quels ports appartiennent à quels VLAN.

- VLAN de niveau 2 (également appelé VLAN MAC, en anglais MAC Address-Based VLAN) consiste à définir un réseau virtuel en fonction des adresses MAC des stations. Ce type de VLAN est beaucoup plus souple que le VLAN par port, car le réseau est indépendant de la localisation de la station.

- VLAN de niveau 3 : on distingue plusieurs types de VLAN de niveau 3 :
  - Le VLAN par sous-réseau (en anglais Network Address-Based VLAN) associe des sous réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifient automatiquement en cas de déplacement d'une station. En contrepartie, une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.
  - Le VLAN par protocole (en anglais Protocol-Based VLAN) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.

## I.3. Type de configuration des ports

Il existe plusieurs types pour configurer les ports qui sont les suivants :

- **Trunk (Agrégation)** : Entre deux switchs ou un switch et un routeur, pour faire passer les trames des différents VLANs sur le même lien.
- **Access** : vers des équipements terminaux (pc, printer, phone, …), pour faire passer les trames d'un seul vlan.
- **Dynamic** : lié au protocole d'agrégation dynamique DTP (Dynamic Trunking Protocol), par défaut il est activé sur les équipements CISCO.
- **Voice** : vers des téléphones IP, se fait après le mode access.

## I.4. Protocoles de transport des VLANs

Dans ce qui suit, nous allons présenter les protocoles de transport des VLANs :

### I.4.1. Notion des TRUNKs

Le réseau local est distribué sur différents équipements via des liaisons dédiées appelées Trunks. Un trunk est une connexion physique unique sur laquelle on transmet le trafic de plusieurs réseaux virtuels. Les trames qui traversent le trunk sont complétées avec un identificateur de réseau local virtuel (VLAN id). Grâce à cette identification, les trames sont conservées dans un même VLAN (ou domaine de diffusion). Il existe différents types du trunk [11] :

- **Trunk entre deux commutateurs** : c'est le mode de distribution des réseaux locaux Le plus courant.
- **Trunk entre un commutateur et un hôte** : c'est le mode de fonctionnement à surveiller étroitement. Un hôte qui supporte le trunking a la possibilité d'analyser le trafic de tous les réseaux locaux virtuels.
- **Entre un commutateur et un routeur** : c'est le mode de fonctionnement qui permet d'accéder aux fonctions de routage, il interconnecte des réseaux virtuels par routage inter-VLANs.

La figure 14 suivante illustre l'Utilisation du trunk entre deux commutateurs.

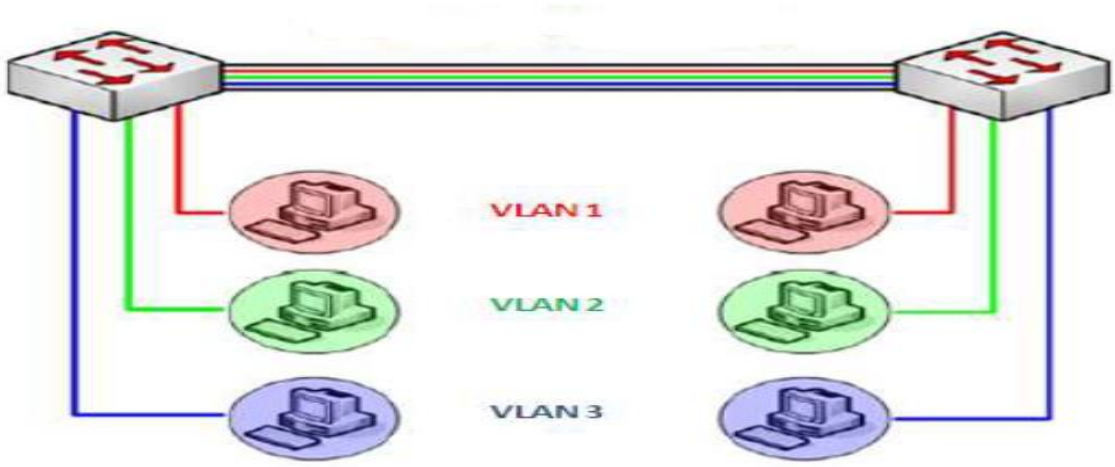


*Figure 14 : Utilisation du trunk entre deux commutateurs.*

### I.4.2. La norme IEEE 802.1Q

La norme IEEE 802.1Q est utilisée pour étendre la portée des VLANs sur plusieurs switch. Elle est basée sur le marquage explicite des trames, dans l'en-tête de niveau 2 de la trame est ajoutée un « tag » qui identifie le VLAN auquel elle est destinée, on parle alors de VLAN « taggés ». Le format de la trame est donc modifié, ce qui peut entraîner des problèmes de compatibilité avec les switchs ne supportant pas les VLANs et des soucis de taille maximale de trame sur le réseau. Il est noté que seuls les Switchs ajoutent et enlèvent les « tags » dans les trames [11].
Trois types de trames sont définis :

- Les trames non étiquetées (untagged frame en anglais) ne contiennent aucune information sur leur appartenance à un VLAN.
- Les trames étiquetées (tagged frame en anglais) possèdent un marqueur qui précise à quel VLAN elles appartiennent.
- Les trames étiquetées avec priorité (priority-tagged frame en anglais) sont des trames qui possèdent en plus un niveau de priorité défini selon la norme IEEE 802.1P.

### I.4.3. Protocole ISL (Inter Switch Link Protocol)

Pour étendre les réseaux virtuels sur plus d'un commutateur, CISCO a mis au point son propre protocole ISL (Inter Switch Link Protocol). Ce protocole achemine les informations d'appartenance aux réseaux virtuels. ISL représente en fait une structure de trame et un protocole qui, en plus de transport des informations d'appartenance aux réseaux virtuels, permet à ces réseaux d'échanger des trames.
Voici un schéma représentant l'encapsulation de la trame Ethernet par des en-têtes spécifiques ISL [11].

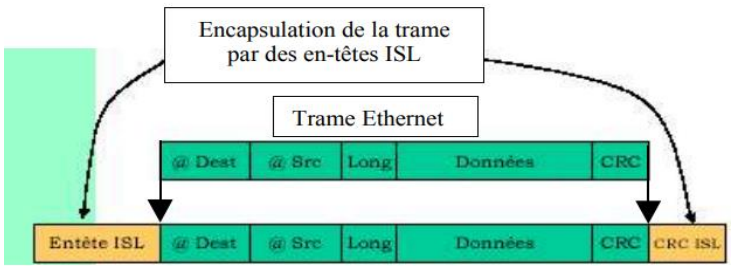


*Figure 15 : L'encapsulation de la trame Ethernet par des en-têtes ISL.*

### I.4.4. LAN et 802.10

Ces deux protocoles sont dépassés, ils sont utilisés avec des topologies de type TOKEN RING ou TOKEN BUS.

## I.5. Protocoles d'administration et de gestion des VLANs

Il est possible de configurer le 802.1q à la main pour permettre le transport des VLAN. Pour cela, il faut configurer chaque port se trouvant sur le chemin d'un port tagué d'un VLAN à un autre, il faut de plus répéter l'opération pour chaque lien défini. On peut comprendre que le processus s'avère long et fastidieux, la norme prévoit donc des mécanismes pour taguer les ports automatiquement et administrer les VLAN d'une manière plus simple, plus abrégée. Pour cela on a défini les protocoles suivants [11].

### I.5.1. VTP

Le protocole VTP (VLAN Trunking Protocol) a été créé par CISCO pour résoudre des problèmes opérationnels dans des réseaux commutés contenant des VLANs. Ce protocole est basé sur la norme 802.1q et exploite une architecture Client-serveur avec la possibilité d'instancier plusieurs serveurs. Le rôle de VTP est de maintenir la cohérence de la configuration VLAN sur un domaine d'administration réseau commun. VTP est un protocole de messagerie qui utilise les trames d'agrégation de couche 2 pour gérer l'ajout, la suppression et l'attribution de nouveaux noms aux VLAN sur un domaine unique. Un commutateur doit alors être déclaré comme serveur, on lui attribue également un nom de domaine VTP, c'est sur ce commutateur que chaque nouveau VLAN devra être défini, modifié ou supprimé. Ainsi chaque commutateur client présent dans le domaine héritera automatiquement des nouveaux VLANs créés sur le commutateur serveur.

Le VLAN Trunking Protocol (VTP) minimise donc l'administration dans le réseau commuté, ceci réduit le besoin de configurer les mêmes VLANs sur chaque commutateur individuellement [12].

Les dispositifs de VTP peuvent être configurés pour fonctionner suivant les trois modes suivants :

- **Le mode serveur**

  Qui est caractérisé par :

  – L'information est stockée dans la NVRAM.
  – Il définit le nom de domaine VTP.
  – Il peut ajouter, modifier ou supprimer un Vlan.
  – Il stocke la liste des VLAN du domaine VTP.

- **Le mode client VTP**

  Qui est caractérisé par :

  – Il possède un nom de domaine,
  – Il stocke une liste de Vlan non modifi

- **Le mode transparent**

  Qui est caractérisé par :

  – Il ne participe pas aux domaines VTP du réseau.
  – Il transmet les paquets VTP via ses liens trunk.
  – Il possède sa propre liste de Vlan qu'il est possible de modifier.
  – Si une des conditions suivantes n'est pas respectée, le domaine de VTP ne sera pas valide et l'information ne se propagera pas.
  – Il faut assigner le même nom de domaine de VTP à chaque commutateur.
  – L'option trunk pour l'interconnexion des commutateurs doit être activée.

### I.5.2. Protocole Spanning-Tree

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

### I.5.3. Protocole DHCP

DHCP (Dynamic Host Configuration Protocol). Il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau local d'obtenir dynamiquement et automatiquement sa configuration IP. Le but principal étant la simplification de l'administration d'un réseau. On voit généralement le protocole DHCP comme distributeur d'adresses IP, mais il a été conçu au départ comme complément au protocole BOOTP (Bootstrap Protocol) qui est utilisé par exemple lorsque l'on installe une machine à travers un réseau (on peut effectivement installer complètement un ordinateur, et c'est beaucoup plus rapide que de le faire à la main). Cette dernière possibilité est très intéressante pour la maintenance de gros parcs de machines. Les versions actuelles des serveurs DHCP fonctionnent pour IPv4.

## I.6. ACL (Access Control List)

Une liste de contrôle d'accès, ou ACL (Access control List) est un ensemble séquentiel d'instructions appelées ACE (Access Control Entry) basées sur des informations contenues dans l'en-tête de paquet des protocoles de couche 2 et supérieures permettant de filtrer le trafic [9].

Les ACL peuvent être utilisées pour :

- Filtrer le trafic réseau en fonction des stratégies de l'entreprise, comme autoriser les trafics HTTP et HTTPS mais refuser les trafics POP3 et FTP ou limiter les accès VTY(virtual terminal line).
- Filtrer le trafic réseau en fonction de sa priorité comme QoS (Quality of Service).
- Définir du trafic intéressant comme les données devant traverser un tunnel VPN.
- Limiter la propagation et la réception des mises à jour de routage.
- Contrôler l'accès inter-VLAN.
- Filtrer les annonces d'un protocole de routage.
- Filtrer des adresses MAC.

Il existe trois types d'ACL :

- Listes de contrôle d'accès standard.
- Listes de contrôle d'accès étendues.
- Listes de contrôle d'accès nommées.

## I.7. Catégories des VLANs

Il existe quatre catégories d'appartenance à un VLAN :

- **VLAN par défaut :** Tous les ports du commutateur deviennent membres du VLAN par défaut après le démarrage initial du commutateur, donc tous les ports du commutateur participent au VLAN par défaut.
- **VLAN de données :** Un VLAN de données est un réseau local virtuel qui est configuré pour ne transporter que le trafic généré par l'utilisateur.
- **VLAN natif :** Un VLAN natif est affecté à un port d'agrégation 802.1Q.
- **VLAN de gestion :** Un VLAN de gestion est un VLAN que vous configurez pour accéder aux fonctionnalités de gestion d'un commutateur.

- **Vlan Voice :** Un VLAN distinct est nécessaire pour prendre en charge la voix sur IP (VoIP). Le trafic de voix sur IP requiert les éléments suivants :
  - Bande passante consolidée pour garantir la qualité de la voix ;
  - Priorité de transmission par rapport aux autres types de trafic réseau ;
  - Possibilité de routage autour des zones encombrées du réseau ;
  - Délai inférieur à 150 ms sur tout le réseau.

## I.8. Avantages des VLANs

Les VLANs ont beaucoup d'avantages qui permettent une meilleure organisation d'un réseau local, ainsi d'améliorer son fonctionnement en termes de performances et d'efficacité. Ces avantages sont cités ci-dessous [9].

- **Limiter la propagation du trafic au seul VLAN concerné :** Un flux originaire d'un VLAN donné n'est transmis qu'aux ports qui appartiennent à ce même VLAN. Chacun des VLANs constitue ainsi un domaine de diffusion propre. C'est pourquoi le trafic doit être routé pour être acheminé entre différents VLANs. C'est-à-dire que la communication inter-VLAN doit se faire par le passage par un routeur pour acheminer le trafic entre les équipements appartenant à des VLANs différents.
- **Meilleures performances :** La création de domaine de diffusion plus petit amène une diminution de la quantité de trafic inutile sur le réseau, qui résulte une augmentation des performances.
- **Flexibilité de segmentation de réseau :** Les utilisateurs et les ressources peuvent être regroupées sans devoir prendre en considération leur localisation physique. C'est-à-dire de se faire connecter à un groupe logique des stations du travail, même si ces dernières ne sont pas géographiquement proches les unes des autres.
- **Simplicité de l'administration du réseau :** Les postes du travail appartenant à un même VLAN peuvent être déplacés d'un lieu à l'autre ou d'une zone à une autre sans devoir à modifier les connexions physiques. Ainsi que de nouveaux segments ou utilisateurs peuvent être ajoutés grâce à une simple configuration des commutateurs, soit par la création de nouveaux VLANs, soit par l'affectation de nouveaux utilisateurs à un VLAN.
- **Organisation du réseau :** Les VLANs permettent de constituer autant de réseaux logiques que l'on désire sur une seule infrastructure physique, donc, cela conduit à une organisation efficace du réseau (mieux organiser son réseau).

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

# II. Les réseaux virtuels privés

## II.1. Réseau privé

Un réseau composé d'ordinateurs d'une même entreprise interconnectés au moyen de lignes privées louées.

## II.2. Réseau privé Virtuel

Réseau privé virtuel (noté RPV ou VPN (Virtual Private Network)) : est une technique permettant à un ou plusieurs postes distants de communiquer de manière sûre. C'est un environnement de communication, dans lequel l'accès est contrôlé, afin de permettre des connexions entre une communauté d'intérêt seulement.

Ce réseau est dit virtuel car il relie deux réseaux « physiques » (réseaux locaux) par une liaison non fiable (Internet), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent voir les données [13].

## II.3. Fonctionnement d'un VPN

Un réseau privé virtuel repose sur un protocole, appelé protocole de tunneling qui permet aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie (entre l'entrée et la sortie du VPN, les données sont chiffrées (cryptées) et donc incompréhensibles pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel) la figure 16 montre les Fonctionnement d'un VPN [13].

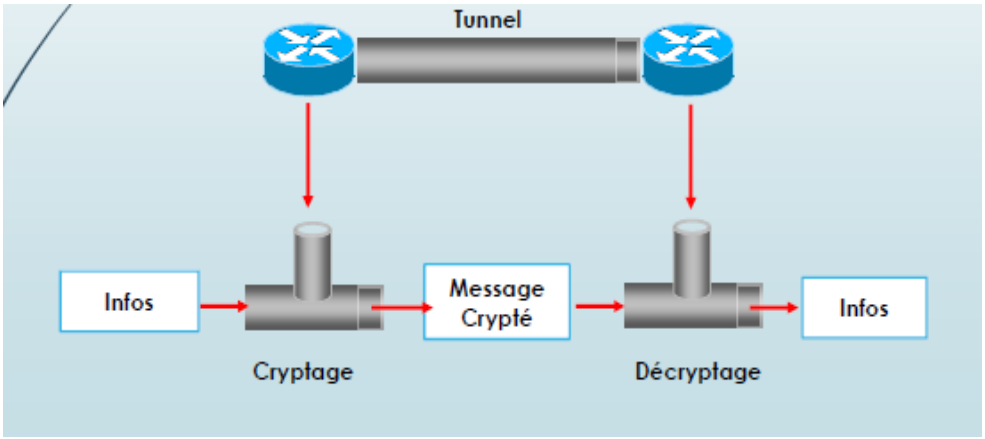


*Figure 16 : Fonctionnement d'un VPN.*

## II.4. Caractéristiques d'un VPN

Un système de VPN doit pouvoir mettre en œuvre les fonctionnalités suivantes [13] :

- **Authentification des utilisateurs** : Pour certains VPN (dans le cas du télétravail par exemple), il est important de savoir quels sont ceux qui participent au processus afin d'éviter les problèmes de sécurité liés à l'usurpation d'identité et par même à l'accès illicite aux réseaux privés. De plus, un historique des connexions et des actions effectuées sur Le réseau doit être conservé.
- **Cryptage des données** : Le chiffrement assure que le contenu des données transmises sur le réseau public n'est connu que des parties qui échangent l'information. De ce fait, un tiers interceptant le trafic du VPN n'aura pas la possibilité d'en déterminer la teneur.
- **Gestion d'adresses** : Chaque client sur le réseau doit avoir une adresse privée qui restera confidentielle. Un nouveau client doit pouvoir se connecter facilement au réseau et recevoir une adresse.
- **Gestion de clés** : Les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées après un certain temps bien déterminé par l'administrateur.
- **Prise en charge multi protocole** : La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier le protocole IP.
- **Intégrité des données** : Le chiffrement et le hachage assurent que les données reçues au travers du VPN par le destinataire sont identiques à celles envoyées par l'expéditeur : Il n'y aura ainsi aucune possibilité, pour une tierce partie, de changer les données en transit dans le VPN.

## II.5. Typologie des VPN

On peut distinguer deux grandes catégories de VPN : le VPN d'entreprise et le VPN d'opérateur. Chacune d'entre elle présente ses avantages et ses inconvenants et elles ne sont pas exclusive l'une de l'autre puisqu'il n'est pas rare de trouver les deux présente simultanément au sein d'une même entreprise.

### II.5.1. VPN d'entreprise

Dans ce cas l'entreprise garde le contrôle des établissements des VPN entre ses différents points de présence ainsi qu'entre ses postes situés à l'extérieur de l'entreprise et les sites principaux.

### II.5.1.1. VPN site à site

Le site à site permet de relier deux réseaux de façon transparente. Généralement les deux sites ont des tranches IP déférentes ce qui oblige les postes clients à passer par le routeur. Celui-ci est directement relié à l'équipement responsable du VPN ou implante directement les protocoles choisis pour la mise en place du VPN, la figure 17 représente un VPN site à site.

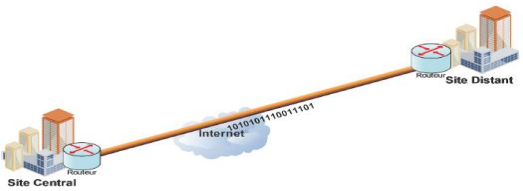


*Figure 17 : Exemple d'un VPN site à site.*

### II.5.1.2. VPN poste à site :

Il existe le type nomade, également appelé "Road Warrior (chemin de guerrier)" qui permet à un utilisateur distant de son entreprise de se connecter à celle-ci pour pouvoir profiter de ses services. Ainsi, il pourra lire ses mails, récupérer des fichiers présents sur le réseau de son entreprise, voir la figure 18.

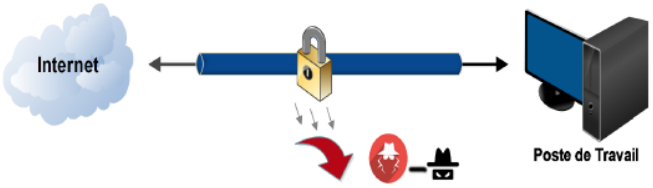


*Figure 18 : Exemple d'un VPN poste à site.*

### II.5.1.3. VPN poste à poste :

Dans ce cas de figure, on veut connecter deux ordinateurs distants pour des raisons de confidentialité. On crée donc un VPN entre eux, et toutes les données transmises ne sont encryptées et compréhensibles que par les deux paires correspondantes comme montre la figure ci-après.

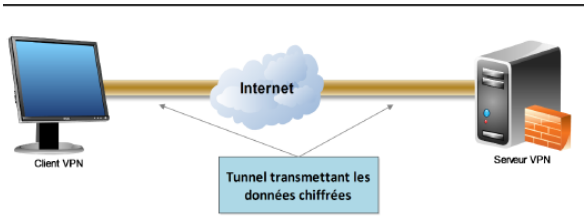


*Figure 19 : Exemple d'un VPN poste à poste.*

### II.5.2. VPN Operateur

Lorsqu'il s'agit d'interconnecter plusieurs sites d'une même entreprise avec des engagements de performances et de disponibilité il est plus judicieux, mais évidemment plus coûteux, de faire appel à un opérateur qui va donc mettre en place un réseau privatif entre tous les sites. Ce réseau tient plus d'un réseau de tunnels que d'un véritable réseau VPN mais il est assez courant de parler d'un VPN operateur car il est quand même difficile, sans la complicité du personnel de l'opérateur, d'intercepter les communications échangées entre les sites.

## II.6. Principaux protocoles

Voici une brève description des protocoles les plus communément utilisés dans le cadre de VPN qu'ils soient d'entreprise ou d'opérateur.
Ils sont classés ici selon leur place dans les couches OSI (Open Systems Interconnection) mais ce classement peut se révéler arbitraire pour certains d'entre eux qui recouvrent en fait plusieurs niveaux.

### II.6.1. Niveau 2

Ces VPN encapsulent les données dans des trames et ce sont ces trames que va véhiculer le tunnel dans une communication point à point.
Nous sommes donc bien ici au niveau 2 du modèle OSI. La plupart des protocoles de ce niveau sont progressivement délaissés au profit de protocoles plus souples comme peuvent l'être ceux des niveaux 3 à 7.

#### II.6.1.1. PPP (Point to Point Protocol)

Est un protocole qui permet le transfert des données sur un lien synchrone ou asynchrone. Il est full duplex et garantit l'ordre d'arrivée des paquets. Il encapsule les paquets IP dans les trames PPP, puis transmet ces paquets encapsulés au travers de la liaison point à point. Il est employé généralement entre un client d'accès à distance et un serveur d'accès réseau.
PPP est le fondement des protocoles PPTP et L2TP utilisés dans les connexions VPN sécurisés. PPP est la principale norme de la plupart des logiciels d'accès distant [14].

#### II.6.1.2. Protocole PPTP (Point To Point Tunneling Protocol)

Est un protocole réseau permettant un transfert sécurisé entre un client et un serveur privé. Il permet la création de VPN sur demande à travers des réseaux basés sur TCP/IP. Il peut de même être utilisé pour créer un VPN entre deux ordinateurs dans le même réseau local [14].

#### II.6.1.3. Protocole L2F (Layer Tow Forwarding)

Est un protocole qui permet à un serveur d'accès distant de véhiculer le trafic sur PPP et transférer des données jusqu'à un serveur réseau L2F. Ce serveur désencapsule les paquets et les envoie sur le réseau, L2F est progressivement remplacé par L2TP qui est plus souple [14].

#### II.6.1.4. Protocole L2TP (Layer Two Tunneling Protocol)

Avec ce protocole on peut accéder à un réseau privé par l'intermédiaire d'Internet ou d'autres réseaux publics au moyen d'une connexion à un VPN utilisant le L2TP.
Ce dernier est protocole de tunneling standard qui possède pratiquement les mêmes fonctionnalités que le protocole PPTP [15].

### II.6.2. Niveau 2 et 3

#### II.6.2.1. Le protocole MPLS (Multi Protocol Label Switching)

Le protocole MPLS est souvent considéré comme situé dans un niveau intermédiaire entre le niveau 2 et le niveau 3. C'est pourquoi on lui affecte souvent un niveau hybride 2.5 qui n'existe pas dans les couches OSI traditionnelles. Son placement en tant que protocole de VPN peut être contesté lorsqu'il est utilisé dans ses fonctions de base.
En effet il ne met pas en œuvre certaines fonctions de sécurité telles que le cryptage, ce qui est en principe un prérequis du VPN [16].

### II.6.3. Niveau 3

Nous retrouvons ici les protocoles opérant au moins au niveau 3, donc au niveau paquet.

#### II.6.3.1. SSL (Secure Sockets Layer)/TLS (Transport Layer Security)

Ce protocole ou plutôt ces protocoles sont en plein essor car c'est très simple de les mettre en œuvre et utilisant le port (443), ce qui facilite le franchissement des firewalls. Dans un certain nombre de cas, ils ne nécessitent qu'un simple navigateur pour être utilisables. Ils sont maintenant implémentés de façon native dans d'autres logiciels (client de messagerie, client FTP) [16].

#### II.6.3.2. SSH (Secure Shell)

Ce protocole était souvent utilisé pour protéger des communications de type console (équivalent de Telnet) ou transferts de fichiers (de type FTP notamment). Son essor est limité

à la fois par le succès grandissant de SSL/TLS et par son champ d'application plus restreint. Néanmoins il reste encore un protocole à considérer pour certains usages [16].

### II.6.3.3. Le protocole IPsec (Internet Protocol Security)

IPsec, défini par la RFC 2401, est un protocole qui vise à sécuriser l'échange de données au niveau de la couche réseau. Le réseau IPv4 étant largement déployé et la migration vers IPv6 étant inévitable, mais néanmoins longue, il est apparu intéressant de développer des techniques de protection des données communes à IPv4 et IPv6.

IPsec est basé sur deux mécanismes [17]:

- **AH (Authentification Header) :** C'est un protocole réseau, de couche 3, vise à assurer l'intégrité et l'authenticité des datagrammes IP. Il ne fournit, par contre, aucune confidentialité : les données fournies et transmises par ce mécanisme ne sont pas encodées.
- **ESP (Encapsulating Security Payload) :** C'est un protocole de couche 4, peut aussi permettre l'authentification des données mais est principalement utilisé pour le cryptage des informations.

Bien qu'indépendants, ces deux mécanismes sont presque toujours utilisés conjointement. Avec l'un ou l'autre de ces protocoles, IPSec peut fonctionner en mode transport ou en mode tunnel:

- **En mode tunnel :** chaque paquet IP est encapsulé dans un paquet IPSec lui-même précédé d'un nouvel en-tête IP et généralement utilisé quand on veut relier un site à un autre (de passerelle à passerelle).
- **En mode transport :** un en-tête IPSec est intercalé entre l'en-tête IP d'origine et les données du paquet IP. La figure ci-dessous montre les modes transport et tunnel dans IPSec.

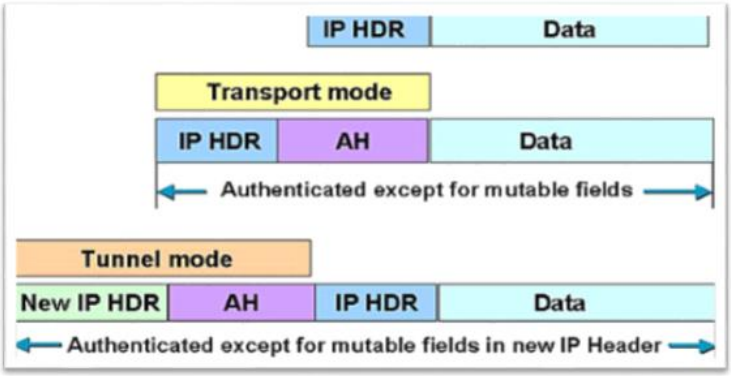


*Figure 20 : Modes transport et tunnel dans IPSec.*

- **Détails du protocole**

Le mécanisme interne d'IPSec est complexe. Le fait que ce protocole soit hautement configurable introduit des notions de gestion et configuration inconnues du monde IP :

- **Gestion des flux IPSec :** Les flux IPSec sont gérés unidirectionnelle ment. Ainsi, une communication bidirectionnelle entre deux machines utilisant IPSec sera définie par diverse processus pour chacun des sens de communication. Les procédés détaillés ci-dessous respectent les lois suivantes.
- **Security Policy :** Une SP définit ce qui doit être traité sur un flux et la manière dont nous voulons transformer un paquet. Notons qu'une SP ne définit qu'un protocole de traitement à la fois. Pour utiliser AH et ESP sur une communication, deux SP devront être créées.
- **Security Association :** Une SA définit la manière dont sera traité le paquet en fonction de sa SP associée. Elles ne sont que la réalisation des SP. Elle possède l'ensemble des propriétés de la liaison. Ainsi, elle sera représentée par une structure de donnée.
- **Base de données SPD et SAD :** Tout système implémentant IPSec possède donc deux bases de données distinctes dans laquelle ils stockent leurs SP (ici, SPDatabase) et leurs SA (ici, SADatabase).
- **SAD (Security Association Dtabase) :** Stocke les SA afin de savoir comment traiter les paquets arrivants ou sortants. Elles sont identifiées par de triplets :
  - Adresse de destination des paquets.
  - Identifiant du protocole AH ou ESP utilisé.
  - Un index des paramètres de sécurité (Security parameter index) qui est un champ de 32 bits envoyé en clair dans les paquets.
- **SPD (Security Policy Database) :** Est la base de configuration de IPSec. Elle permet de décider, pour chaque paquet, s'il se verra apporter des services de sécurité, s'il sera autorisé passer ou rejeté. C'est à sa charge de savoir avec quel SA fait-il le traitement.

- **Fonctionnement d'IPSec**

Le schéma ci-dessous représente tous les éléments présentés ci-dessus, leurs positions et leurs interactions [17] :

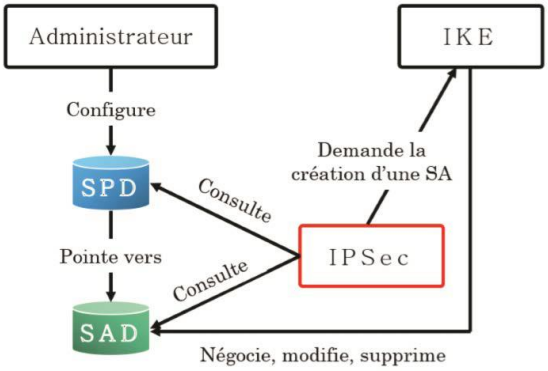


*Figure 21 : Principe de fonctionnement d'IPSec.*

Pour bien comprendre le fonctionnement d'IPSec, nous allons voir comment est traité le trafic sortant et le trafic entrant.

- **Trafic sortant :** Lorsque la "couche" IPsec reçoit des données à envoyer, elle commence par consulter la base de données des politiques de sécurité (SPD) pour savoir comment traiter ces données. Si cette base lui indique que le trafic doit se voir appliquer des mécanismes de sécurité, elle récupère les caractéristiques requises pour la SA correspondante et va consulter la base des SA (SAD). Si la SA nécessaire existe déjà, elle est utilisée pour traiter le trafic en question. Dans le cas contraire, IPsec fait appel à IKE pour établir une nouvelle SA avec les caractéristiques requises.
- **Trafic entrant :** Lorsque la couche IPsec reçoit un paquet en provenance du réseau, elle examine l'en-tête pour savoir si ce paquet s'est vu appliquer un ou plusieurs services IPsec et si oui quelles sont les références de la SA. Elle consulte alors la SAD pour connaître les paramètres à utiliser pour la vérification et/ou le déchiffrement du paquet. Une fois le paquet vérifié et/ou déchiffré, la SPD est consultée pour savoir si l'association de sécurité appliquée au paquet correspondait bien à celle requise par les politiques de sécurité. Dans le cas où le paquet reçu est un paquet IP classique, la SPD permet de savoir s'il a néanmoins le droit de passer. Par exemple, les paquets IKE sont une exception. Ils sont traités par IKE, qui peut envoyer des alertes administratives en cas de tentative de connexion infructueuse.

## II.7. Les quatre grandes catégories de VPN

Les VPN peuvent être classés dans les grandes catégories suivantes [18] :

- **Un VPN basé sur un pare-feu** : est un VPN équipé à la fois d'un pare-feu et d'un VPN. Ce type de VPN utilise les mécanismes de sécurité des pares-feux pour restreindre

l'accès à un réseau interne. Les caractéristiques qu'il offre sont la permutation d'adresse IP, l'authentification des utilisateurs et l'alerte en temps réel.

- **Un VPN matériel :** offre un débit réseau élevé, de meilleures performances et une meilleure qualité de service. Il offre également plus de fiabilité, puisqu'il n'y a pas de surcharge du processeur. Cependant, c'est beaucoup plus cher.
- **Un VPN logiciel :** offre la plus grande flexibilité dans la gestion du trafic. Ce type de VPN convient lorsque les terminaux VPN ne sont pas contrôlés par la même personne et lorsque différents pare-feu et routeurs sont utilisés. Il peut être utilisé avec des accélérateurs de chiffrement matériel pour améliorer ses performances.
- **Un VPN SSL :** permet aux utilisateurs de se connecter à des périphériques VPN à l'aide d'un navigateur Web. Le protocole SSL (Secure Sockets Layer) ou TLS (Transport Layer Security) est utilisé pour crypter le trafic entre le navigateur Web et le périphérique VPN SSL. L'un des avantages de l'utilisation des VPN SSL est sa facilité d'utilisation, car tous les navigateurs Web standard prennent en charge le protocole SSL. De ce fait, les utilisateurs n'ont pas besoin d'installer ou de configurer de logiciel.

## II.8. Avantages des VPN

Les réseaux privés virtuels offrent les avantages suivants :

- **Sécurité :** assure des communications sécurisées et chiffrées.
- **Simplicité :** utilise les circuits de télécommunication classiques.
- **Économie :** utilise Internet en tant que média principal de transport, ce qui évite les coûts liés à une ligne dédiée.
- **Évolutivité :** Les réseaux privés virtuels utilisent l'infrastructure Internet dont les FAI et les opérateurs, facilitant l'ajout de nouveaux utilisateurs pour les entreprises. Ces dernières, quelle que soit leur taille, peuvent augmenter leurs capacités sans élargir sensiblement leur infrastructure.

## Conclusion

Nous avons vu tout au long de ce chapitre que la technologie des VLANs repose sur des concepts principaux et essentiels tels que la limitation des domaines de broadcast, la mobilité des utilisateurs et sans oublier le point important de notre but c'est la sécurité, ainsi nous avons pu comprendre plus de détails sur la notion de VPN qui permet de sécuriser le tunnel de communication, pour cela nous avons détaillé les différentes catégories et possibilités pour le déploiement d'un VLAN et d'un VPN, leur rôle et leurs différents protocoles utilisés.

# Chapitre 3 : Etude de l'existant

## Introduction

Afin de nous familiariser avec l'environnement de l'entreprise NAFTAL Bitumes de la Wilaya de Bejaia, nous avons en premier lieu pris connaissance de celle-ci, des différents services, activités qui la constituent.

En second lieu, nous avons fait une présentation globale de l'infrastructure réseau de l'entreprise NAFTAL BITUMES sur laquelle nous réaliserons notre projet, ensuite nous verrons la problématique ainsi que l'objectif de notre projet et la solution proposée.

## I. Présentation de l'organisme d'accueil

### I.1. Historique de NAFTAL

L'entreprise NAFTAL est issue de la restructuration de la SONATRACH. Elle a été créée par le décret ministériel N° 80 /101 du 06 avril 1981. A l'origine, la commercialisation et la distribution des produits pétroliers est une activité de la direction du marché intérieur de la SONATRACH. Entrée en activité le 01 janvier 1982, l'ERDP (Entreprise de Raffinage et de Distribution des produits Pétroliers) a été chargée du raffinage des hydrocarbures, de la commercialisation et de la distribution des produits pétroliers sur le territoire national sous le sigle de NAFTAL. Suivant le décret N° 87/89 du 27 août 1987, l'activité raffinage est séparée de l'activité distribution. La raison sociale de la société a changé, suite à cette séparation des activités, NAFTAL est désormais chargée de la commercialisation et de la distribution des produits pétroliers et ces dérivés.

A partir du mois d'avril 1998, NAFTAL change le statut et devient société par actions filiale à 100% de la SONATRACH avec un capital de 6,65 millions DA. A compter du 01/01/2003, le capital de NAFTAL est passé à 15,650 millions de Dinars. Au début de l'année 2000, NAFTAL se divise principalement en deux districts :

- District CLPB (Carburant, lubrifiant, pneumatique, Bitumes)
- District GPL (Gaz propane, Gaz butane).

Actuellement NAFTAL opère avec trois (03) branches d'activités opérationnelles :

- La branche du carburant : Elle a pour mission l'approvisionnement et le ravitaillement en carburants des centres et des dépôts carburants terre - aviation et marine à partir des raffineries et la commercialisation des produits aviation et marine.

- La branche GPL : Elle a pour mission la satisfaction des besoins de la clientèle en GPL vrac et conditionné en tous lieux et en toutes circonstances.
- La branche commercialisation : Elle a pour mission la mise à la disposition de la clientèle l'ensemble des produits pétroliers à travers son réseau stations-service et par vente directe aux gros consommateurs sur tout le territoire national.

## I.2. La modernisation de NAFTAL

La modernisation de l'entreprise NAFTAL s'agit de :

- La réhabilitation de ses infrastructures de stockage.
- La mise en conformité de ses installations avec les normes de protection de l'environnement et de sécurité industrielle.
- La modernisation et l'extension de son réseau de stations-services.
- Le renouvellement de ses moyens de transport par route et de son matériel de manutention.
- L'augmentation de ses capacités de transport par pipe.
- La promotion de ses produits propre : GPL et essence sans plomb.
- Assurer une meilleure offre au marché.

## I.3. Organigramme de la direction générale de NAFTAL

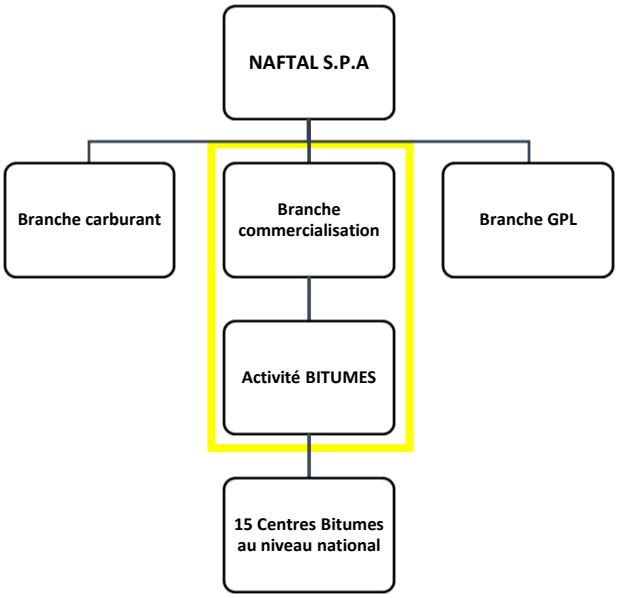


*Figure 22 : Organigramme de la direction générale de NAFTAL.*

## I.4. Présentation de l'activité BITUMES

Le bitume est un produit de raffinerie. Il constitue la fraction la plus lourde des pétroles. Et est obtenu par la distillation sous vide du résidu provenant de la distillation atmosphérique, suite à laquelle on obtient au fond de la colonne sous vide un résidu viscoélastique de couleur noire.

Le bitume est l'un des premiers matériaux thermoplastiques utilisés par l'homme.

D'une manière générale, c'est un produit organique, naturel, extrait du pétrole, un ciment viscoélastique, de couleur sombre, durable, imperméable…

### I.4.1. Caractéristiques des BITUMES

- De couleur marron à noire.
- Manipuler à chaud.
- Inflammable aux hautes températures.
- Matériaux d'étanchéité adhésive.
- Non volatile.
- Thermoplastique.
- Viscoélastique.
- Rigide à température ambiante.
- Durable.
- Immiscible avec l'eau et ne pollue pas.

### I.4.2. Commercialisation des BITUMES en Algérie par NAFTAL

La consommation des bitumes en Algérie vie actuellement un accroissement considérable, notamment avec les projets de renforcement d'entretien du réseau routier et de constructions nouvelles.

Le marché actuel des bitumes continu d'enregistrer une forte croissance, avec une quantité globale évaluée à 482126 tonnes dont NAFTAL se maintient à la hauteur de ce marché avec plus de 71% soit 346926 tonnes. Les bitumes utilisés en Algérie sont totalement importés comme nous l'avions mentionné précédemment, les pétroles algériens ne sont pas assez denses pour extraire du bitume.

Les classes de bitumes purs commercialisés par NAFTAL sont généralement le 40/50 et 80/10. Ils sont emportés soit sous forme de matière, brut réduit, raffiné au niveau des raffineries d'Arzew et de Skikda, soit sous forme de produits finis, bitumes purs.

### I.4.3. Répartitions géographiques des 15 centres BITUMES

Les centres bitumes sont repartis à quatre (4) régions sur le territoire national comme le montre la carte ci-dessous :

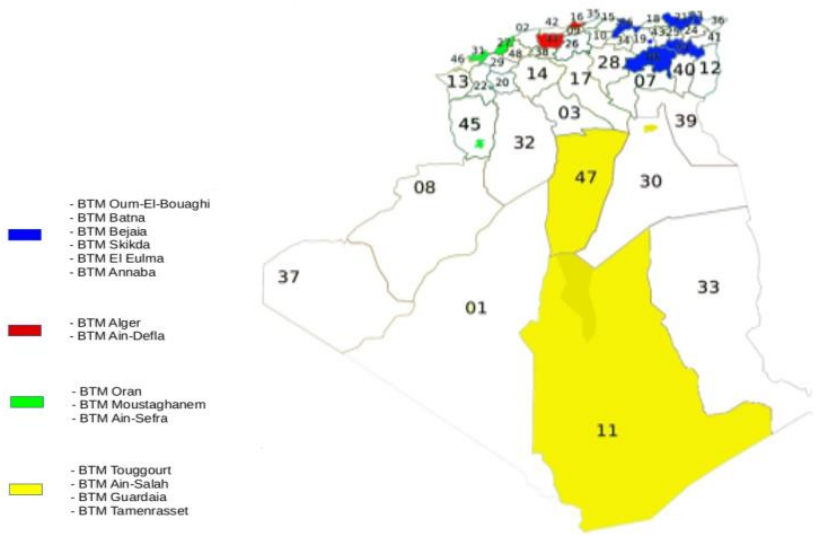


*Figure 23 : Répartitions géographiques des 15 centres BITUMES.*

## I.5. Création du centre bitume Bejaia

L'année de mise en service était en 1936 sur le nom SHELL, a pour mission commercialisation et ravitaillement du bitume pur ainsi que la vente des cut-backs et les émulsions.

Ce centre renferme un effectif de 38 agents composés comme suit :

- Chef de centre.
- Secrétaire du centre.
- Un cadre informatique.
- Dix agents administratifs et commerciaux.
- Onze agents à la section exploitation et maintenances.
- Quatre agents de sécurité.
- Un chef service commercial.
- Un chef service finances.
- Deux cadres techniques.
- Un chef de projet.
- Un inspecteur de sécurité.
- Quatre agents de sécurité industrielle.

- **Les équipements**
  - Un pipe-line de 320 M de longueur et 8 ’’ de diamètre.
  - Deux chaudières de marque WANSON de 3000 SC et 2000 SC à l’huile diathermique.
  - Deux postes de chargement.
  - Un pont bascule pour petits porteurs.
  - 03 bacs de stockage.

### I.5.1. Organigramme du centre BITUMES BEJAIA

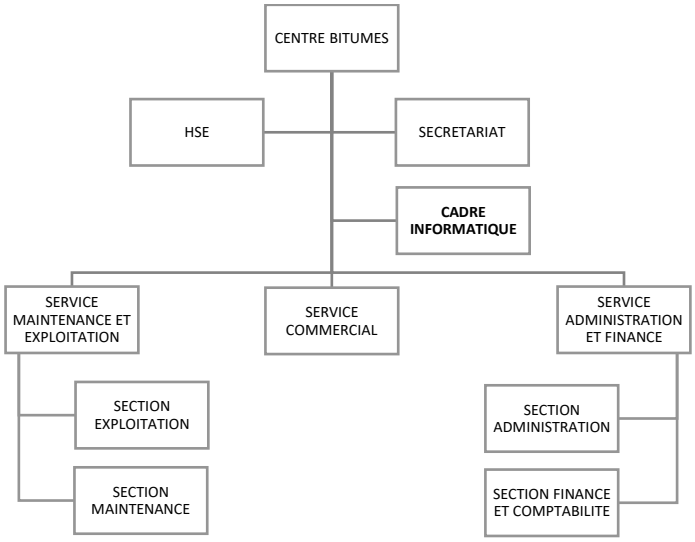


*Figure 24 : Organigramme du centre BITUMES BEJAIA.*

### I.5.2. Présentation du cadre informatique :

Le cadre informatique à sa dimension a un impact très important pour l’entreprise, car son apport est tellement présent et visible dans la communication des données et de l’information au sein du Bitumes de NAFTAL, dans l’administration et la maintenance du réseau informatique, etc.

### I.5.3. Rôle du cadre informatique du bitume

Le cadre informatique assure les tâches suivantes :

- La maintenance du matériel informatique.
- La maintenance des logiciels, systèmes et applications.
- Le suivi des différentes activités d’administration du réseau.
- Analyse des états.

- Veuille au recueil de l'information à partir des CDs (Centre de Stock).
- Participe à l'élaboration des plans de production de la zone, consolidé les plans élaborés par les structures de la zone.

## I.6. Architecture réseau de NAFTAL BITUMES

Une architecture réseau est un ensemble d'équipements matériel et logiciels interconnectés en réseau, afin de régir des activités informatiques collectives, en centralisant ou répartissant les ressources et les tâches à travers le système. C'est donc une façon d'interconnecter physiquement les différents éléments d'un réseau et de combiner son organisation logicielle, dans le but de communiquer et d'effectuer des opérations informatiques. L'entreprise NAFTAL dispose d'un grand réseau informatique réparti sur plusieurs wilayas, reliées par VPN basé sur Internet, le schéma ci-après illustre l'architecture réseau de NAFTAL BITUMES

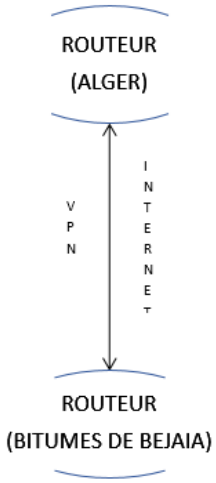


*Figure 25 : Architecture réseau de NAFTAL BITUMES.*

## II. Contexte du projet à réaliser

Dans cette partie de notre travail, nous allons en premier lieu présenter le projet à réaliser, suivi de la problématique associée au cahier de charges de l'organisme, en second lieu nous allons présenter notre proposition et améliorations de l'architecture réseau de cette entreprise.

## II.1. Diagnostic de la situation du réseau

Au cours de notre stage pratique à NAFTAL BITUMES de la Wilaya de Bejaia, nous avons constaté que le centre BITUMES est composé de trois services nécessaires, qui sont tous liés au même switch, donc un seul et unique domaine de diffusion ce qui implique une surcharge du réseau de l'entreprise et aussi l'absence de sécurité au niveau des ports des commutateurs du réseau local ce qui permet l'accès aux différents comptes utilisateurs sans control.

Notre étude au cœur de cette entreprise nous a permis aussi de remarquer que la communication entre ces différents centres repose sur un VPN site-à-site basé sur Internet, donc une simple coupure de celle-ci peut causer la perte des données envoyées, et comme aussi les transmissions peuvent être attaquées par un virus, ou les données peuvent êtres piratés par une autre personne hors NAFTAL. Donc on constate que le trafic inter-réseau était non sécurisé.

## II.2. Présentation du projet à réaliser

Le projet à réaliser s'intitule "Etude et amélioration de l'architecture et sécurité du réseau NAFTAL BITUMES de la Wilaya de BEJAIA", La mise en œuvre de ce projet permet d'apporter des améliorations au réseau de l'entreprise, en mettant l'accent sur l'administration et le partage du réseau tout en assurant la fluidité et une meilleure sécurité en utilisant les réseaux virtuels VLANs et des liaisons VPNs. L'objectif de ce projet consiste à garantir une bonne exploitation et segmentation du réseau, ainsi, assurer une communication sûre et confidentielle entre les utilisateurs au sein de l'entreprise.

En effet, proposer une segmentation sous laquelle les différents réseaux locaux des stations vont être organisés, ainsi de permettre la communication sûre, sécurisé et confidentielle.

## II.3. Solution proposée

Le but de notre projet est la sécurité du réseau Intranet de BITUME de la Wilaya de BEJAIA avec l'implémentation d'une solution basée sur les réseaux virtuels. Dans ce chapitre nous avons étudié et critiqué l'architecture existante du réseau de cette entreprise pour savoir comment procéder à une meilleure sécurisation.

Pour cela, nous avons constaté qu'on a besoin de la segmentation du réseau en plusieurs VLAN c'est-à-dire la configuration des Switch au niveau des armoires pour mettre en œuvre le réseau VLAN de l'entreprise. En effet, cette solution s'avère plus efficace en vue des avantages qu'elle offre, le plus avantageux est le fait de réaliser la réduction de la diffusion du trafic sur le réseau.

Ainsi nous avons opté pour la solution VPN site-à-site basé sur **ligne spécialisée** [1] qui consiste à mettre en place une liaison permanente, distante et sécurisée entre deux ou plusieurs sites de NAFTAL BITUMES, afin de résoudre les différentes préoccupations manifestées par les responsables informatiques de NAFTAL. De même pour pallier aux différents problèmes relevés au niveau de la critique de l'existant, et même pour mettre en avant le nombre d'utilisateurs potentiels du lien VPN, les applications concernées et le débit maximum à consommer. Il est néanmoins important de préciser que la solution retenue garantie la confidentialité, la sécurité, l'intégrité des données sur des canaux privés et un accès sécurisé.

## Conclusion

Ce chapitre nous a permet une bonne compréhension du réseau d'entreprise NAFTAL BITUMES de BEJAIA où nous avons suivi notre stage pratique, et nous a permet d'acquérir des nouvelles connaissances dans la mise en place et l'administration de réseau NAFTAL BITUMES, ce qui nous a conduit à voir ses lacunes et ses faiblesses. L'étude de ces dernières nous a aidé à proposer des solutions pour les paliers et pour bien améliorer le réseau.
Dans le chapitre qui suit nous allons présenter le simulateur Packet Tracer et décrire les étapes de la mise en œuvre des solutions proposées

[1] Appelée également liaison louée ou ligne louée est en informatique ou en télécommunication une liaison physique de niveau 2 connectée en permanence entre deux bâtiments distants ou deux sites différents.

# CHAPITRE 4 : Mise en œuvre du projet

## Introduction :

Chaque projet au travail, commence généralement par une étude théorique, et se termine par une étude pratique qui est la mise en œuvre de la solution ou bien la réalisation du projet.
Ce présent chapitre, consistera à mettre en œuvre la solution proposée pour la réalisation de notre projet, avec l'ensemble des configurations nécessaires à implémenter sur les LANs de l'entreprise NAFTAL.
Pour visualiser notre travail et mettre en évidence l'efficacité de notre solution, nous présenterons le logiciel utilisé et l'environnement de travail ainsi que les différentes configurations utilisées, enfin nous donnerons les résultats obtenus de la configuration.

## I. Présentation du simulateur « Cisco Packet Tracer »

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

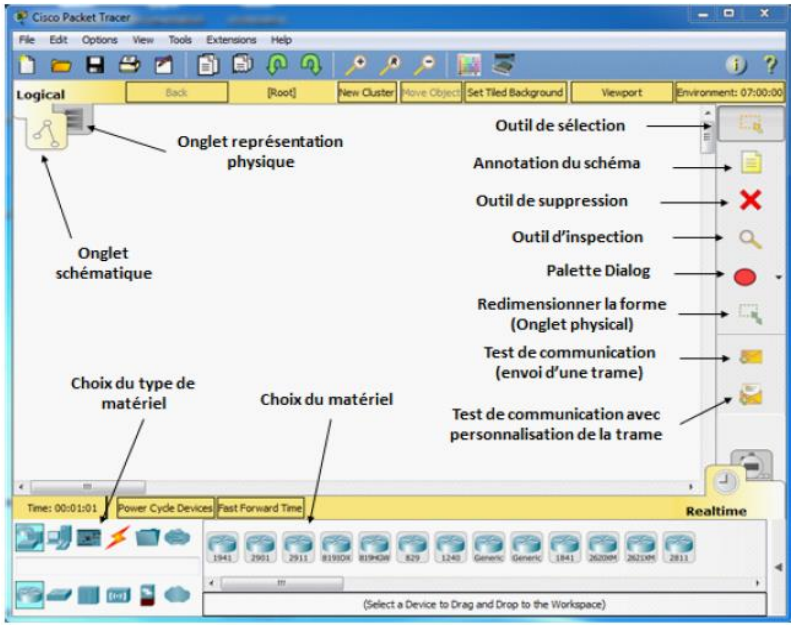


*Figure 26 : l'interface principale du simulateur Cisco Packet Tracer.*

## II. Interface commande de Packet Tracer

Toutes les configurations des équipements du réseau, sont réalisées au niveau de CLI (Command Language Interface). CLI est une interface de simulateur Packet Tracer qui permet la configuration des équipements du réseau à l'aide d'un langage de commandes. C'est-à-dire qu'à partir des commandes introduites par l'utilisateur du logiciel, que la configuration est faite. La Figure suivante montre l'interface CLI du Packet Tracer :

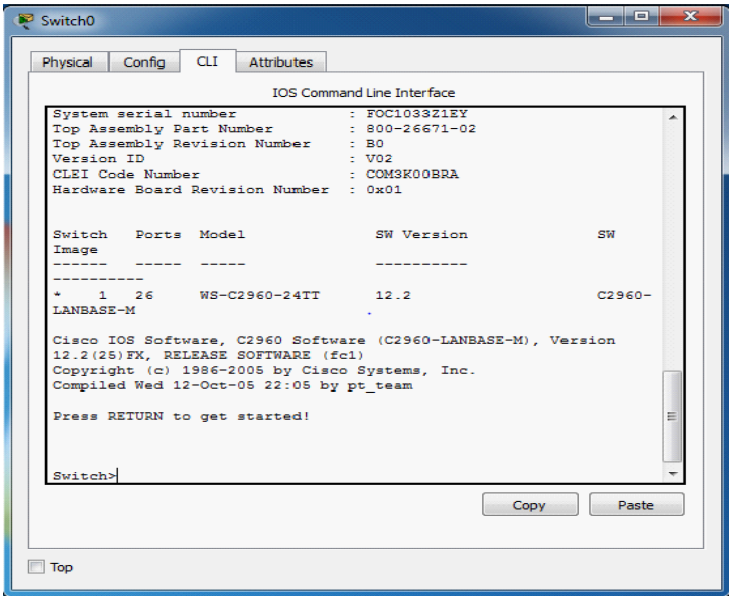


*Figure 27 : l'interface CLI du Packet Tracer.*

## III. Structure générale du réseau de l'entreprise NAFTAL :

La figure suivante illustre la topologie physique de l'entreprise NAFTAL captée sous le simulateur Packet Tracer.

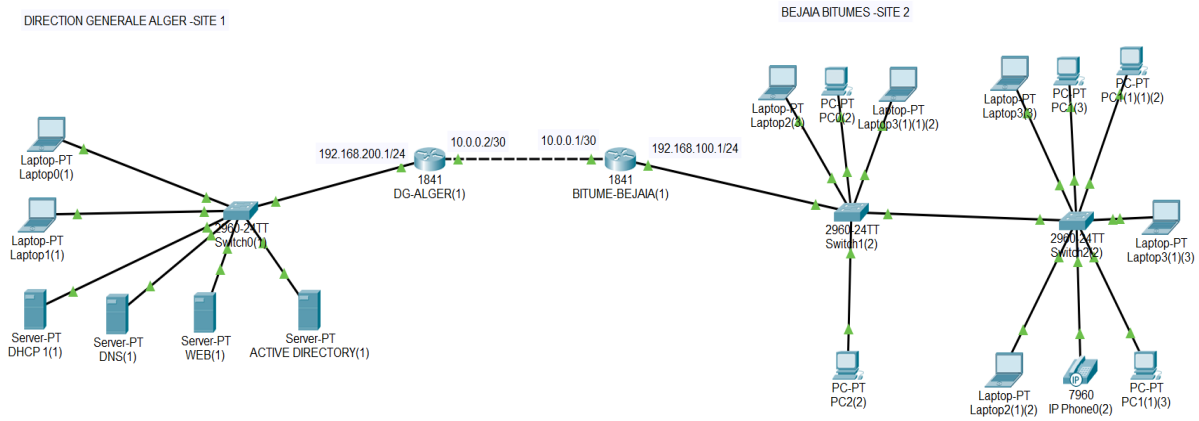


*Figure 28 : L'architecture du réseau NAFTAL BITUMES avant les améliorations.*

# IV. Solution adaptée

On a proposé en premier lieu, de segmenter le réseau local de l'entreprise de BEJAIA NAFTAL BITUMES en trois vlan selon leurs services qui sont les suivant :

- **Vlan 10** : maintenance_exploitation.
- **Vlan 20** : administration_finance.
- **Vlan 30** : commercial.

L'utilisation des VLANs pour la segmentation de réseau nous permettra de créer un ensemble logique isolé pour augmenter le niveau de la sécurité en isolant les utilisateurs accédant aux données sensibles. On découpe le LAN en plusieurs VLANs en utilisant la segmentation par sous-réseau, chaque service aurait son propre VLAN, ce qui permettra un échange d'informations plus sécurisé et augmentera la qualité de la bande passante.

En second lieu, on a mis en place un réseau VPN site-à-site (cas de NAFTAL BITUMES Bejaia) pour cela, nous avons opté pour un VPN WIMAX de **SLC** dans le but de :

- Permettre à NAFTAL d'échanger de manière fiable et sécurisée les informations entre ses différents réseaux à partir du serveur sur lequel les utilisateurs s'authentifieront.
- Permettre aux clients de NAFTAL ou aux clients VPN d'accéder au réseau internet de façon contrôlée.

- **La Société Smart Link Communication**

C'est l'opérateur télécoms de réseaux multiservices, SLC est un fournisseur majeur de solutions entreprises BWA (Broadband Wireless Access - *Accès à Internet large bande sans fil).*

L'offre de connexions Internet BWA de SLC se fait grâce à son propre réseau, backbone IP très fiable et à sa distribution WIMAX radio fréquence, qui couvre déjà une grande partie du territoire national. Le réseau backbone IP entièrement sécurisé et redondant, ainsi que la distribution cellulaire WIMAX de SLC permettent d'offrir aux administrations, aux collectivités locales et aux entreprises, notamment les PME et les Grands Comptes, les services suivants :

- Connexions Internet Large Bande Sans Fil (de 1 Mbps à 54 Mbps et plus) ;
- Interconnexions de sites d'entreprises ;
- Liaisons spécialisées sans fil.

Dans le cas pratique, en réalité il est évidemment impossible de connecter directement les 2 routeurs, puisque le but premier du VPN est justement de se passer d'une ligne spécialisée. Ce

lien sera donc créé grâce à un tunnel crypté, qui permettra aux 2 sites de communiquer entre eux de manière sécurisée. Pour cela, nous allons réaliser la configuration d'IPSec sur les deux routeurs : en mode automatique avec un secret pré-partagé via le protocole ISAKMP.

Les critères de configuration d'IPSec à mettre en place seront :

- Chiffrement et authentification avec le protocole ESP.
- Authentification avec le protocole AH.
- Mode tunnel.
- Les algorithmes de chiffrement et d'authentification sont AES et SHA.

Voici l'architecture après l'amélioration :

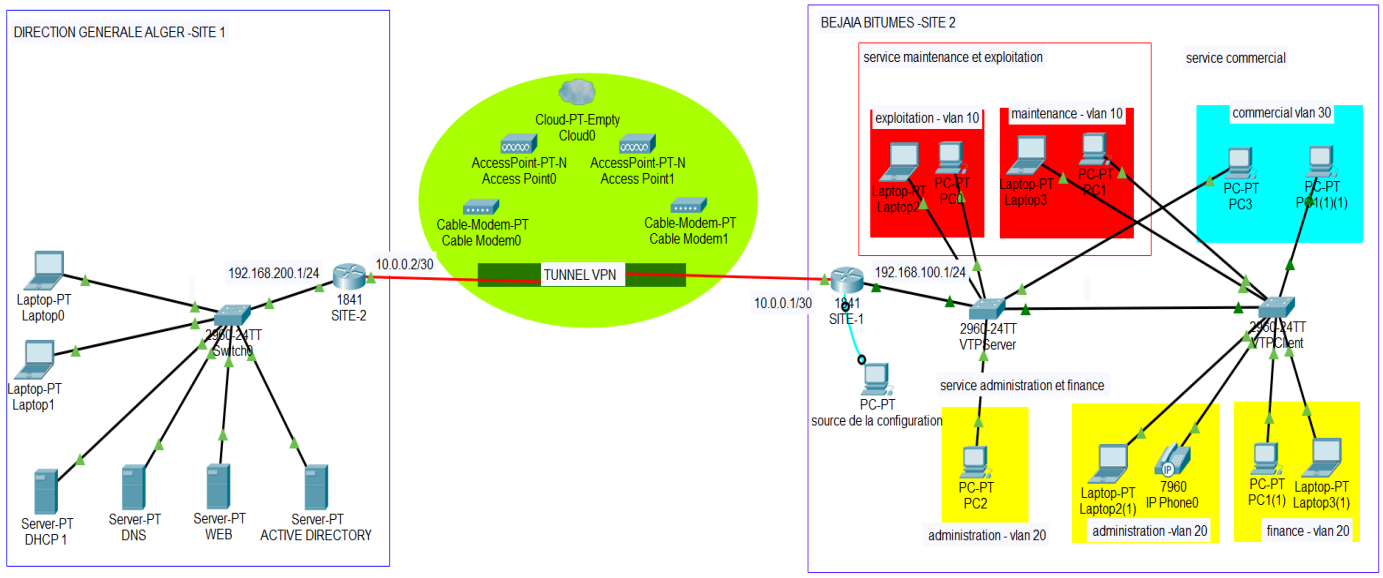


*Figure 29 : l'architecture améliorée du réseau BITUMES BEJAIA.*

## V. Mise en place de VLANs

Nous allons effectuer des configurations au niveau des switchs et des routeurs pour mettre en place les solutions proposées.

# V.1. Configuration de switch VTPServer

## V.1.1. Sécuriser l'accès aux périphériques

Il faut savoir qu'**ISO** [2] utilise des modes organisés hiérarchiquement pour faciliter la protection des périphériques. Dans le cadre de ces dispositifs de sécurité, ISO peut accepter plusieurs mots de passe, ce qui nous permet d'établir différents privilèges d'accès au périphérique.

La figure suivante illustre la Configuration initiale de switch VTPServer.

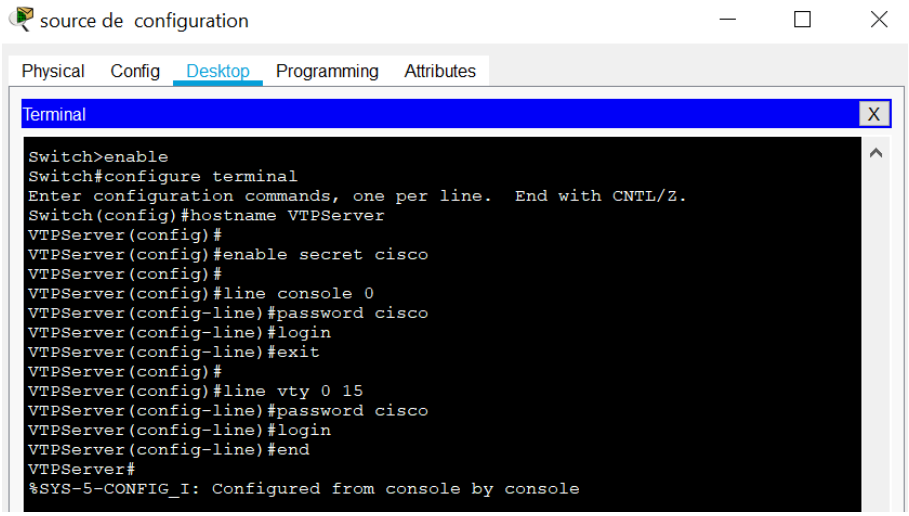


*Figure 30 : Configuration initiale de switch VTPServer.*

## V.1.2. Configuration des VLANs

La configuration des VLANs est faite au niveau des commutateurs, et dans notre cas on aura trois (03) VLANs différents qui seront configurés comme suit sur le switch VTPServer :

**Remarque** : la vérification des VLANs est faite à l'aide de la commande **do show vlan.**

[2] **ISO** est l'architecture logicielle qui est incorporée dans tous les routeurs CISCO. Ce système est muni d'une interface en ligne de commandes, propres aux équipements de CISCO Systems.

La figure ci-dessous montre la Configuration des VLANs sur le switch VTPServer :

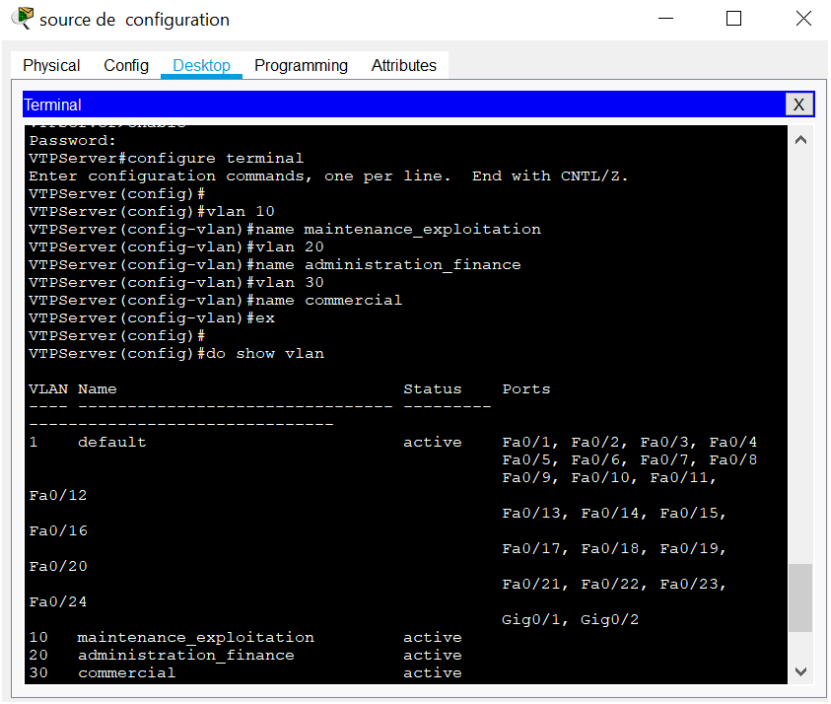


*Figure 31 : Configuration des VLANs sur le switch VTPServer.*

### V.1.3. Configuration des ports “Access”

Sur le switchs VTPServer, il faut se connecter sur chacune des interfaces, ensuite configurer le mode accès avec la commande « switchport mode access » et placer l’interface dans le vlan que l’on souhaite avec la commande « switchport access vlan » (figure 32)

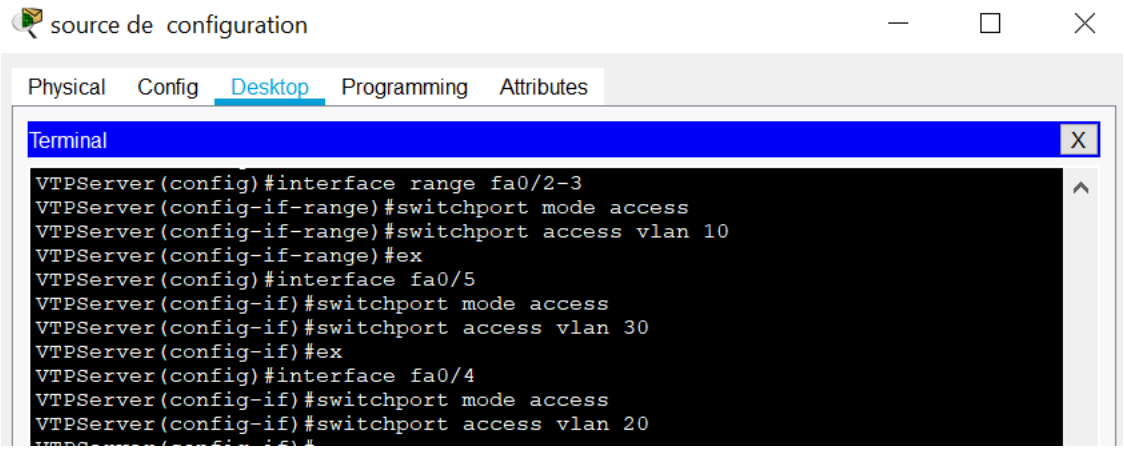


*Figure 32 : Affectation des ports aux vlan (mode ACCESS).*

### V.1.4. Configuration des ports “TRUNK ”

Les interfaces des équipements d’interconnexion à configurer en mode TRUNK existent entre l’ensemble des commutateurs ou entre le commutateur et le routeur. Le cas suivant représente l’interconnexion de deux commutateurs d’accès.

On va créer un lien « TRUNK » entre les deux switchs, afin de faire circuler les trames taguées d’un switch à l’autre.

La figure suivante représente la Configuration de port en mode TRUNK du switch VTPServer.

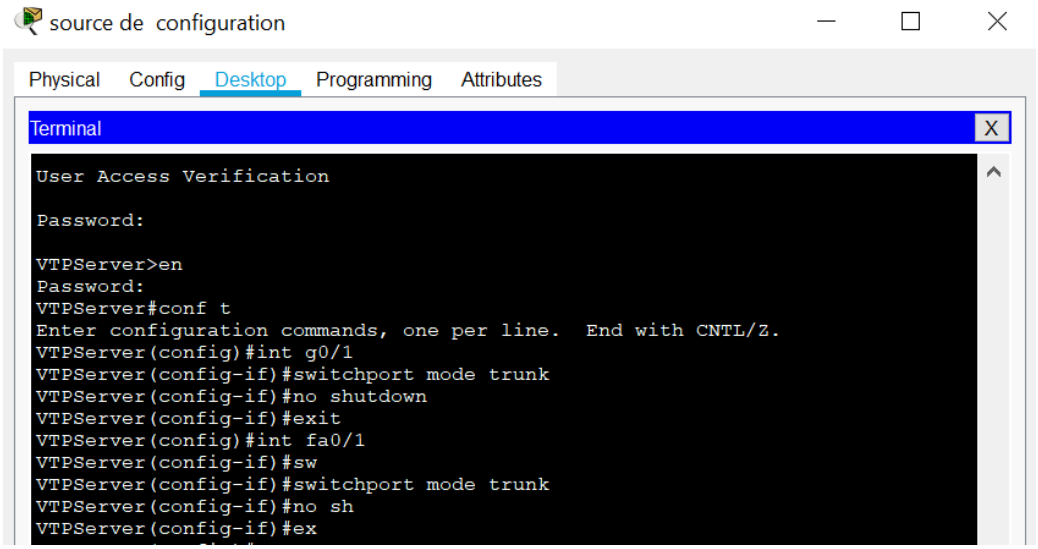


*Figure 33 : Configuration de port en mode TRUNK du switch VTPServer.*

### V.1.5. Configuration du protocole VTP (Vlan Transport Protocol) en mode Server

Le switch en mode Server permet à l’administrateur de faire toute modification sur les VLANs et de propager automatiquement ses modifications vers tous les switchs du réseau. La figure suivante nous permet de voir la configuration du mode VTP server :

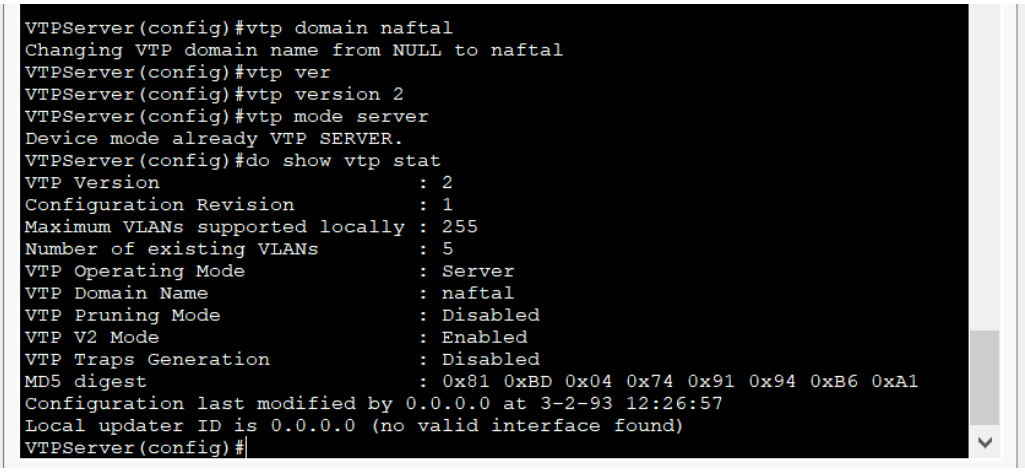


*Figure 34 : Configuration du VTP au niveau de switch VTPServer.*

# V.2. Configuration de switch VTPClient

## V.2.1. Sécuriser l'accès aux périphériques

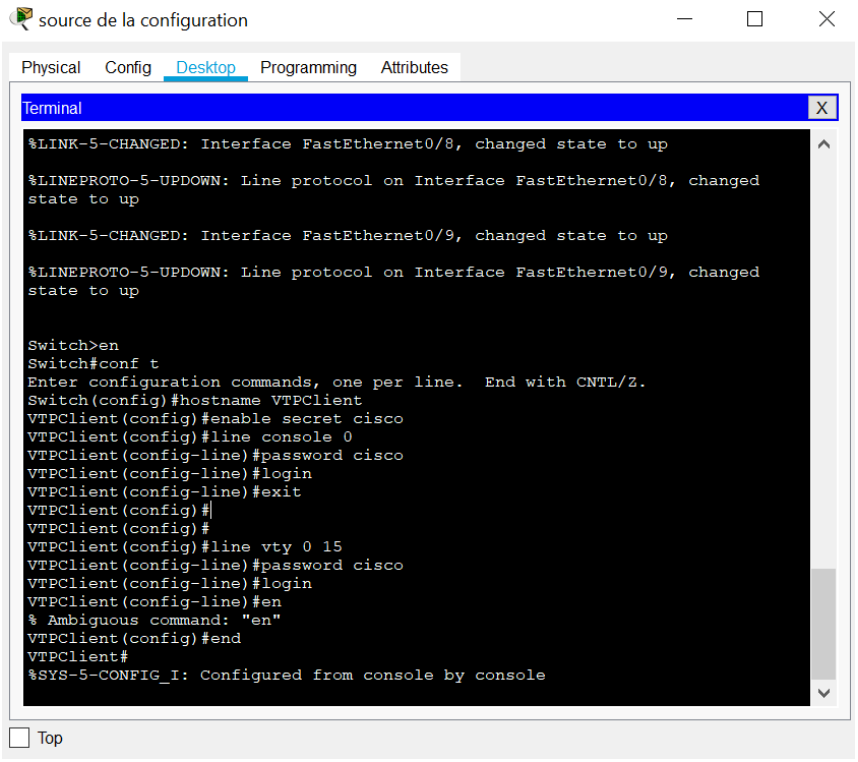


*Figure 35 : Configuration initiale de switch VTPClient.*

## V.2.2. Configuration de port en mode TRUNK

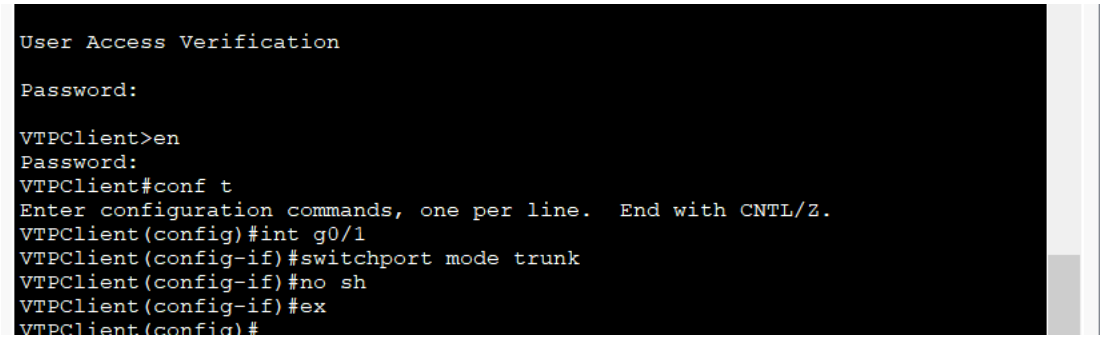


*Figure 36 : Configuration de port en mode TRUNK de switch VTPClient.*

### V.2.3. Configuration du protocole VTP en mode Client

Le protocole VTP permet la configuration automatique de VLANs entre des serveurs VTP et des clients sur un même domaine VTP.

Le mode client ne permet pas à l'administrateur de faire des modifications sur les VLANs. Vous recevez un message d'erreur quand vous essayez de créer un VLAN. La figure suivante nous permet de voir la configuration de switch en mode VTP client ;

La commande « show vtp status » permet de vérifier les paramètres de configuration VTP sur un commutateur à base de commandes Cisco IOS,voir la figure ci-après.

```
VTPClient(config)#vtp domain naftal
Changing VTP domain name from NULL to naftal
VTPClient(config)#vtp version 2
VTPClient(config)#vtp mode client
Setting device to VTP CLIENT mode.
VTPClient(config)#
VTPClient(config)#
VTPClient(config)#
VTPClient(config)#do show vtp stat
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : naftal
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x99 0x8D 0xA4 0xF8 0x7C 0xBF 0x60 0x1A
Configuration last modified by 0.0.0.0 at 3-2-93 12:54:16
```

*Figure 37 : Configuration du VTP au niveau de switch VTPClient.*

### V.2.4. Attribution des ports aux VLANs

```
VTPClient(config)#int ra
VTPClient(config)#int range fa0/4-5
VTPClient(config-if-range)#switchport mode access
VTPClient(config-if-range)#switchport access vlan 20
VTPClient(config-if-range)#ex
VTPClient(config)#int fa 0/2
VTPClient(config-if)#switchport mode access
VTPClient(config-if)#switchport access vlan 20
VTPClient(config-if)#
VTPClient(config-if)#
VTPClient(config-if)#ex
VTPClient(config)#int fa0/3
VTPClient(config-if)#switchport mode access
VTPClient(config-if)#switchport access vlan 20
VTPClient(config-if)#switchport voice vlan 20
VTPClient(config-if)#ex
VTPClient(config)#do wr
Building configuration...
[OK]
```

*Figure 38 : Attribution des ports au VLANs au niveau de switch VTPClient.*

## V.3. Configuration du routeur SITE-1

### V.3.1. Configuration des interfaces et le protocole de routage du routeur SITE-1

Nous allons configurer le routeur en indiquant les adresses IP des interfaces associés, ainsi que le protocole de routage utilisé par ce routeur.Le schéma suivant représente la Configuration des interfaces et le protocole de routage du routeur SITE-1.

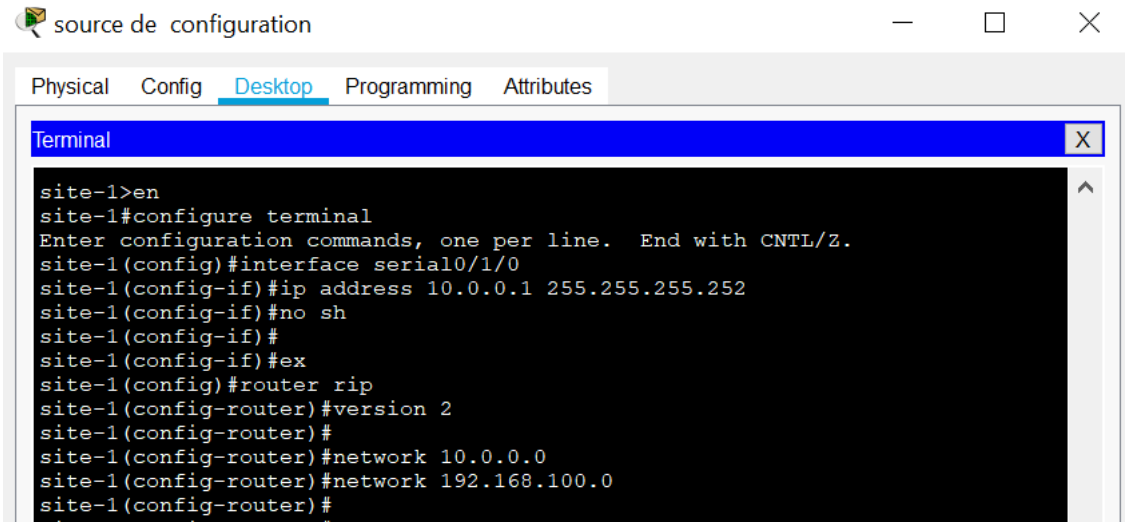


*Figure 39 : Configuration des interfaces et le protocole de routage du routeur SITE-1.*

### V.3.2. Configuration DHCP

Pour simplifier à l'administrateur la gestion et l'attribution des adresses IP, on utilise le protocole DHCP qui permet de configurer les paramètres réseaux client, au lieu de les configurer sur chaque ordinateur client.

La figure suivante illustre les commandes qui nous permettent de configurer ce protocole :

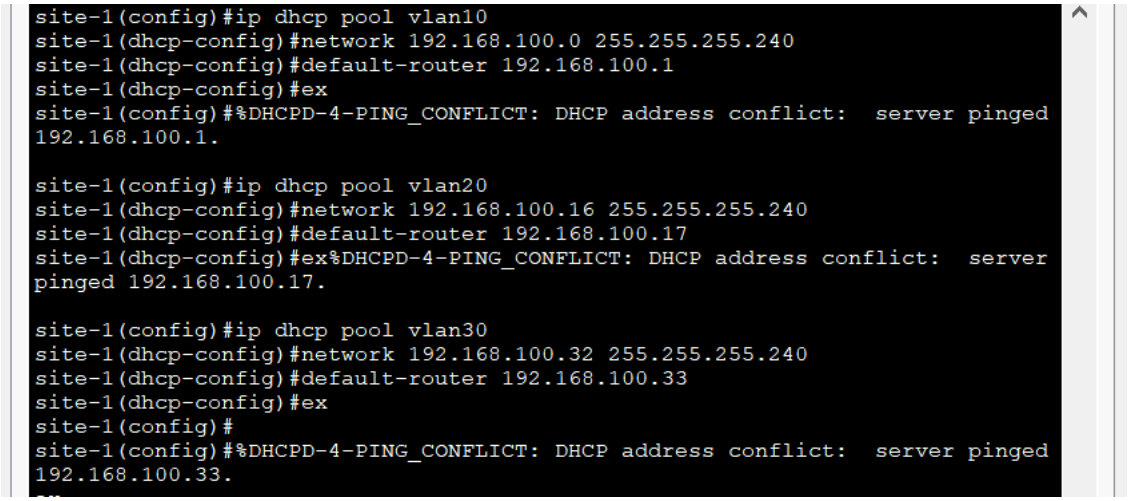


*Figure 40 : Configuration des interfaces et le protocole de routage du routeur SITE-1.*

### V.3.3. Vérification du protocole DHCP

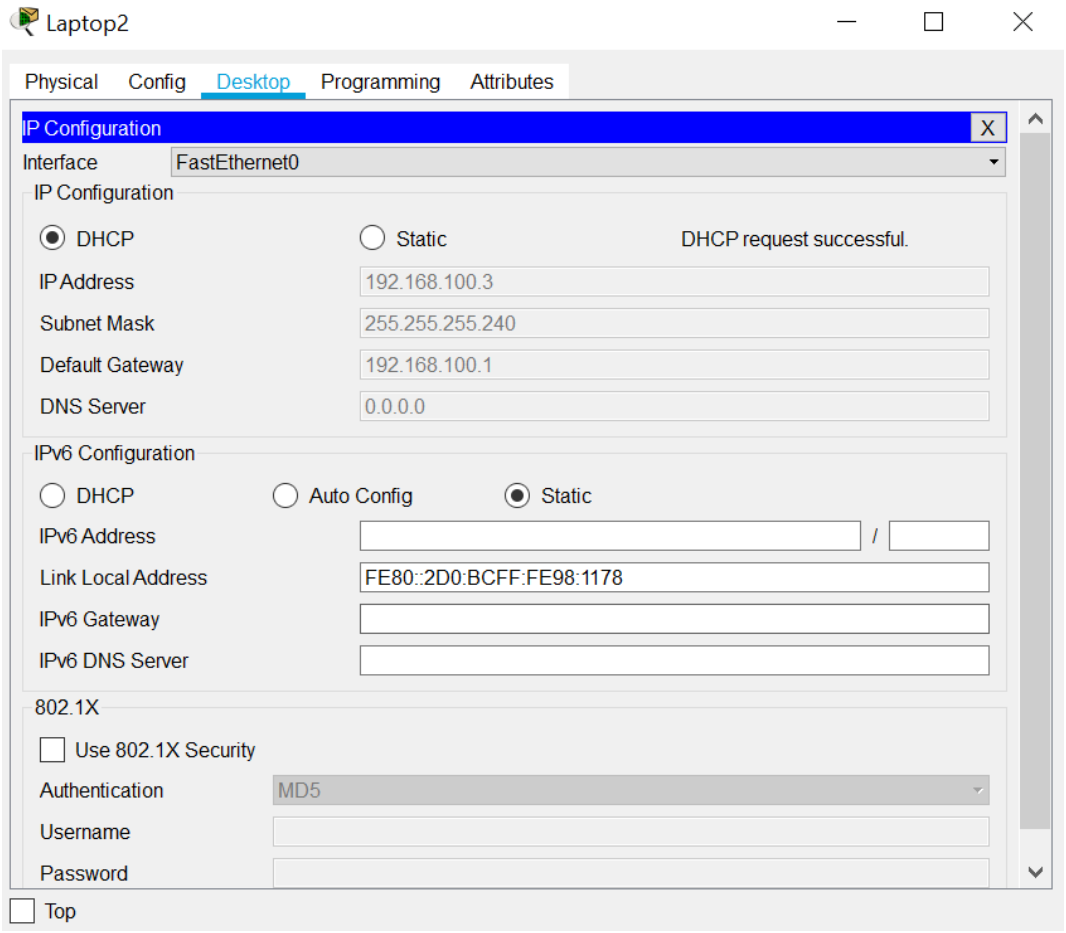


*Figure 41 : Attribution d'adresse IP avec le protocole DHCP*

### V.3.4. Routage inter-Vlan

Le routage inter-Vlans permet aux différents VLANs de communiquer, plusieurs VLANs peuvent avoir pour passerelle un même port physique du routeur qui sera "découpé" en plusieurs interfaces virtuelles. Nous pouvons en effet diviser un port du routeur selon les Vlans à router et ainsi créer une multitude de passerelles virtuelles avec des adresses IP différentes. La figure ci-dessous nous montre les commandes obligatoires pour réussir le routage :

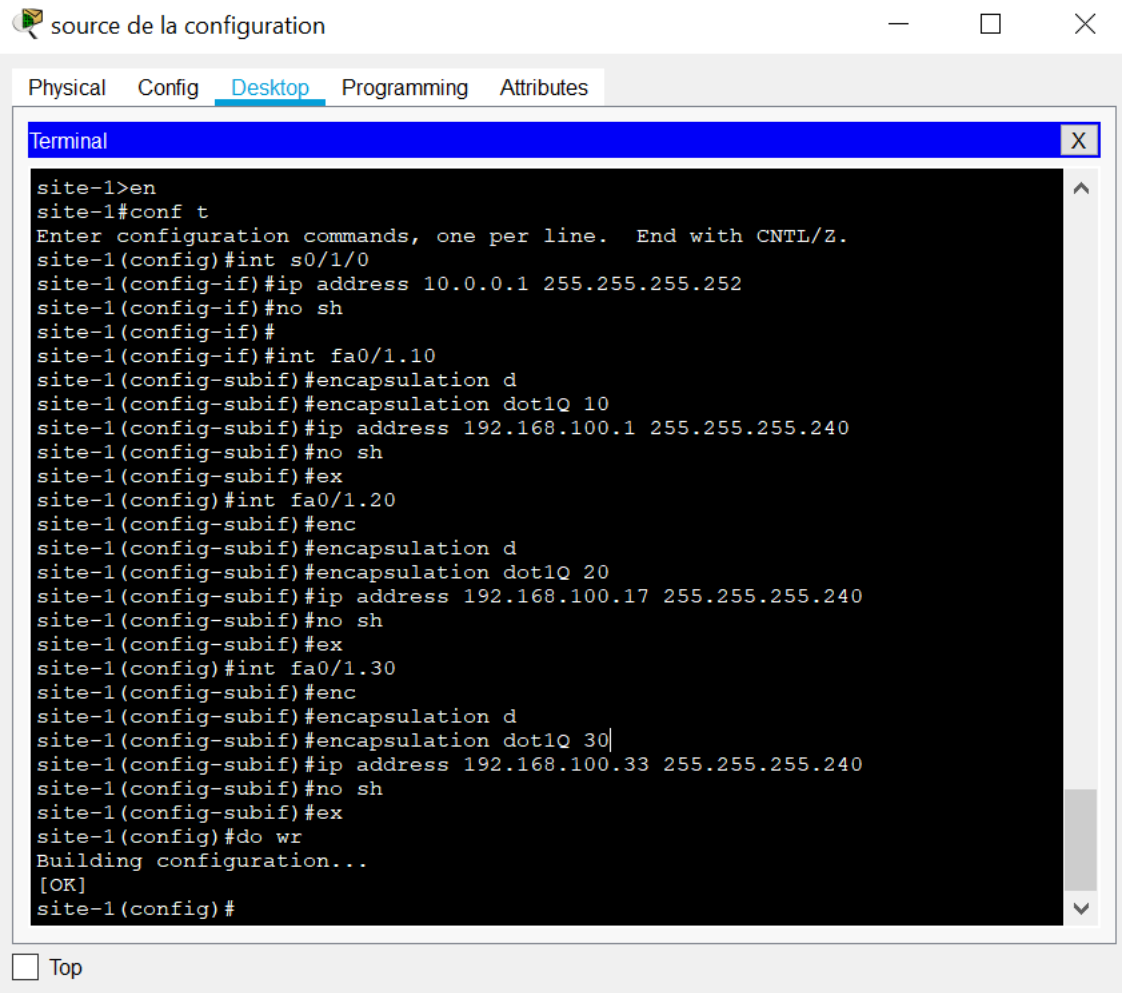


*Figure 42 : le routage inter-vlan sur le routeur SITE-1.*

### V.3.5. Vérification du routage inter-VLAN

Dans cette étape on vérifie la communication entres les VLANs crées au niveau de l'entreprise NAFTAL BITUMES de Bejaia, en utilisant la commande ping.

Ping entre VLAN 10 et VLAN 20 :

La figure suivante illustre la vérification de la communication entres les VLANs

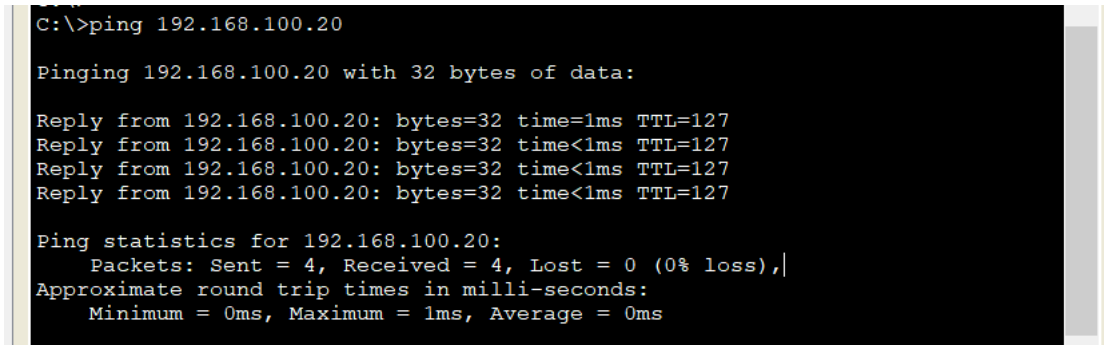


*Figure 43 : Vérification du routage inter-vlan sur le routeur SITE-1*

## V.4. Configuration du routeur SITE-2

### V.4.1. Configuration des interfaces et le protocole de routage du routeur SITE-2

Dans cette partie nous allons faire les configurations basiques du routeur de SITE-2 afin de faciliter les taches de la partie II.

La figure ci-dessous nous montre les différentes commandes utilisées :

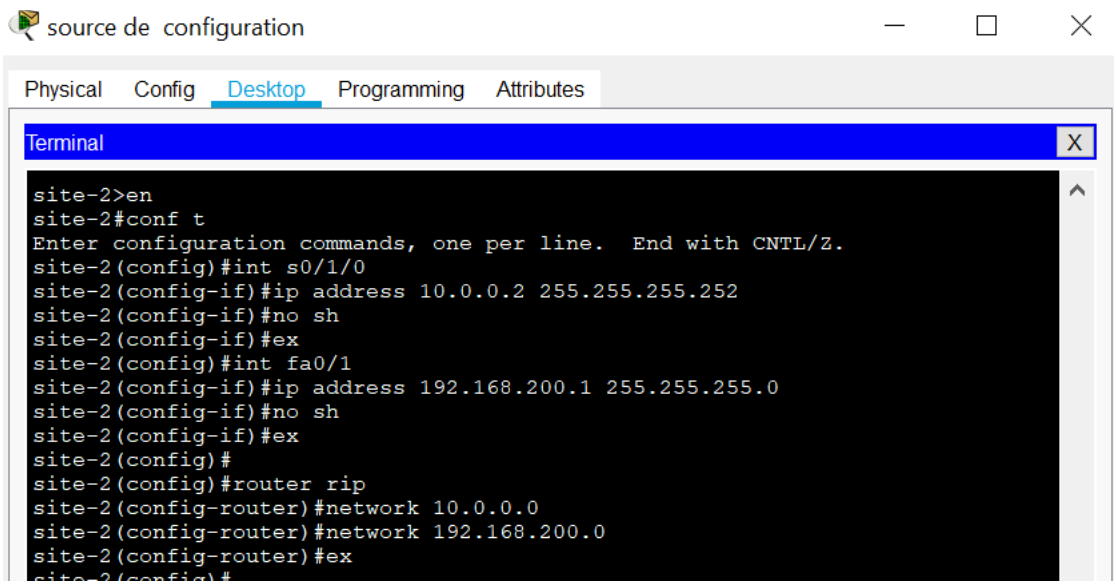


*Figure 44 : Configuration des interfaces et le protocole de routage du routeur SITE-2.*

## V.5. Test routage inter-VLAN

Une fois que nous avons mis les bonnes passerelles à nos postes, nous pouvons tester la communication inter-VLAN par l'intermédiaire d'un simple ping par exemple du poste 192.168.100.3 vers 192.168.100.17.

La figure suivante illustre la vérification de la communication inter-VLANs

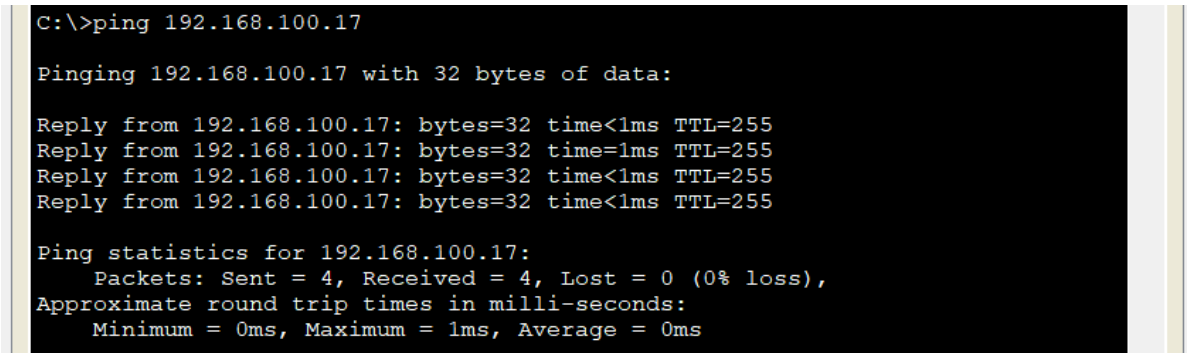


*Figure 45 : Test routage inter-VLAN.*

# VI. Mise en place de VPN

IPSec VPN est une fonctionnalité de sécurité qui nous permet de créer un lien de communication sécurisé (également appelé tunnel VPN) entre deux réseaux différents situés sur des sites différents. Les routeurs Cisco IOS peuvent être utilisés pour configurer un tunnel VPN entre deux sites. Le trafic tels que les données, voix, vidéo, etc. peut être transmis de manière sécurisée via le tunnel VPN. Dans ce qui suit, on va montrer les étapes à suivre pour configurer le tunnel VPN IPSec de site à site dans le routeur Cisco IOS.

La configuration d'IPSec s'effectue généralement en suivant les étapes ci-dessous :

1. Configuration de la politique d'ISAKMP : algorithmes, clés, durée de vie du tunnel ISAKMP qui se trouveront à la suite de la ligne de configuration commençant par crypto ISAKMP.
2. Configuration de la SA IPSec (protocoles AH/ESP, algorithmes, durée de vie du tunnel IPSec) se trouveront à la suite de la ligne de configuration commençant par crypto IPSec.
3. Description d'une carte de cryptage (crypto map) rassemblant les paramètres des deux phases, l'extrémité du tunnel et la définition du trafic à sécuriser se trouvera à la suite de la ligne de configuration commençant par crypto map.

Il est très important de faire attention à ce que les configurations des deux routeurs soient cohérentes et symétriques, l'une par rapport à l'autre.

## VI.1. Configuration du VPN au niveau du routeur SITE-1

### VI.1.1. Configuration d'IPSec (stratégie ISAKMP)

Dans cette étape nous allons activer et créer une politique ISAKMP sur chaque routeur, cette politique se définit par une combinaison des paramètres de sécurité à employer. La figure suivante nous montre les différentes commandes utilisées :

```
site-1>
site-1>EN
site-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
site-1(config)#crypto isakmp enable
site-1(config)#crypto isakmp policy 10
site-1(config-isakmp)#auth
site-1(config-isakmp)#authentication p
site-1(config-isakmp)#authentication pre-share
site-1(config-isakmp)#encryption 3des
site-1(config-isakmp)#hash md5
site-1(config-isakmp)#group5
                      ^
% Invalid input detected at '^' marker.

site-1(config-isakmp)#group 5
site-1(config-isakmp)#lifetime 60
site-1(config-isakmp)#ex
site-1(config)#
```

*Figure 46 : Activation du protocole ISAKMP pour le routeur de SITE-1.*

### VI.1.2. Configuration de l'authentification par clé pré-partagée

Dans cette étape nous allons configurer les clés pré-partagées que doit utiliser chaque hôte IPSec dans sa politique d'IKE en mode de configuration globale. La figure suivante nous montre la commande utilisée :

```
site-1(config)#crypto isakmp key cisco address 10.0.0.2
site-1(config)#
```

*Figure 47 : Configuration de l'authentification par clé pré-partagée pour le routeur de SITE-1.*

### VI.1.3. Configuration d'IPSec (transform-set)

Dans cette phase, il s'agit de définir une transformation qui explicite les algorithmes IPSec (AH et/ou ESP) nécessaires pour la mise en œuvre du tunnel IPSec. Pour la mise en place de notre transformation, nous allons taper la commande suivante sur le routeur BEJAIA BITUMES :

```
site-1(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
site-1(config)#crypto ipsec se
site-1(config)#crypto ipsec security-association lifetime seconds 120
site-1(config)#
```

*Figure 48 : Configuration d'IPSec (transform-set) pour le routeur de SITE-1.*

### VI.1.4. Configuration de la liste de contrôle d'accès étendue pour un trafic intéressant

Cette ACL définit le trafic intéressant qui doit passer par le tunnel VPN. Ici, le trafic en provenance du réseau 192.168.100.0 vers le réseau 192.168.200.0 sera acheminé via un tunnel VPN. Cette ACL sera utilisée dans l'étape suivante. La figure suivante nous montre la commande utilisée :

```
site-1(config)#access-list 100 permit ip 192.168.100.0 0.0.0.255
192.168.200.0 0.0.0.255
```

*Figure 49 : configuration des ACLs pour le routeur de SITE-1.*

### VI.1.5. Configuration de la carte de cryptage (crypto map)

La carte de cryptage (ou crypto map) permet de lier les SA (Security Association) négociées et la politique de sécurité (SP : *Security Policy*). En d'autres termes, elle permet de renseigner :

- Quel trafic devrait être protégé par IPSec.
- L'autre extrémité du tunnel vers lequel le trafic IPSec devrait être envoyé.
- Quelle sécurité d'IPSec devrait être appliquée à ce trafic (transform-set).

La figure suivante illustre la Configuration de la carte de cryptage pour le routeur de SITE-1:

```
site-1(config)#crypto map VPN_NAFTAL 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
site-1(config-crypto-map)#
site-1(config-crypto-map)#set peer 10.0.0.2
site-1(config-crypto-map)#set transform-set 50
site-1(config-crypto-map)#set se
site-1(config-crypto-map)#set security-association lifetime seconds 120
site-1(config-crypto-map)#match address 100
site-1(config-crypto-map)#ex
site-1(config)#
```

*Figure 50 : Configuration de la carte de cryptage pour le routeur de SITE-1.*

### VI.1.6. Application des crypto map à l'interface

Il faut lier la crypto map à une interface du routeur par laquelle le trafic d'IPSec passera. Tout trafic arrivant ou sortant de cette interface est comparé avec le trafic à sécuriser défini dans une liste d'accès : s'il y a correspondance ce dernier est chiffré. La figure ci-dessous nous montre les commandes :

```
site-1(config)#
site-1(config)#int s0/1/0
site-1(config-if)#crypto map VPN_NAFTAL
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
site-1(config-if)#EX
site-1(config)#DO WR
Building configuration...
[OK]
site-1(config)#
```

*Figure 51 : Application des crypto map a l'interface pour le routeur de SITE-1.*

# VI.2. Configuration du VPN au niveau du routeur SITE-2

## VI.2.1. Configuration d'IPSec (stratégie ISAKMP)

```
site-2(config)#crypto isakmp enable
site-2(config)#crypto isakmp policy 10
site-2(config-isakmp)#au
site-2(config-isakmp)#authentication pr
site-2(config-isakmp)#authentication pre-share
site-2(config-isakmp)#
site-2(config-isakmp)#enc
site-2(config-isakmp)#encryption 3de
site-2(config-isakmp)#encryption 3des
site-2(config-isakmp)#ha
site-2(config-isakmp)#hash md
site-2(config-isakmp)#hash md5
site-2(config-isakmp)#group 5
site-2(config-isakmp)#lif
site-2(config-isakmp)#lifetime 60
site-2(config-isakmp)#ex
site-2(config)#
```

*Figure 52 : Activation du protocole ISAKMP pour le routeur de SITE-2.*

## VI.2.2. Configuration de l'authentification par clé pré-partagée

```
site-2(config)#crypto isakmp key cisco address 10.0.0.1
```

*Figure 53 : Configuration de l'authentification par clé pré-partagée pour le routeur de SITE-2.*

## VI.2.3. Configuration d'IPSec (transform-set)

```
site-2(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
site-2(config)#crypto ipsec security-association lifetime seconds 120
site-2(config)#
```

*Figure 54 : Configuration d'IPSec (transform-set) pour le routeur de SITE-2.*

## VI.2.4. Configuration des ACLs

```
site-2(config)#access-list 100 permit ip 192.168.200.0 0.0.0.255
192.168.100.0 0.0.0.255
```

*Figure 55 : Configuration des ACLs pour le routeur de SITE-2.*

## VI.2.5. Configuration de la carte de cryptage (crypto map)

```
site-2(config)#crypto map VPN_NAFTAL 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
site-2(config-crypto-map)#set peer 10.0.0.1
site-2(config-crypto-map)#set transform-set 50
site-2(config-crypto-map)#set se
site-2(config-crypto-map)#set security-association lifetime seconds 120
site-2(config-crypto-map)#match address 100
site-2(config-crypto-map)#ex
site-2(config)#
```

*Figure 56 : Configuration de la carte de cryptage pour le routeur de SITE-2.*

### VI.2.6. Application des crypto map à l'interface

```
site-2(config)#
site-2(config)#int s0/1/0
site-2(config-if)#crypto map VPN_NAFTAL
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
site-2(config-if)#
```

*Figure 57 : Application des crypto map a l'interface pour le routeur de SITE-2.*

## VI.3. Vérification et Tests de fonctionnement du VPNs

Pour tester la connexion VPN, Nous allons faire un ping entre le PC de Bejaia vers le PC de Alger comme suit :

```
C:\>ping 192.168.200.6

Pinging 192.168.200.6 with 32 bytes of data:

Reply from 192.168.200.6: bytes=32 time=1ms TTL=126
Reply from 192.168.200.6: bytes=32 time=15ms TTL=126
Reply from 192.168.200.6: bytes=32 time=4ms TTL=126
Reply from 192.168.200.6: bytes=32 time=15ms TTL=126

Ping statistics for 192.168.200.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 15ms, Average = 8ms
```

*Figure 58 : Vérification connexion VPN par ping BEJAIA vers ALGER.*

- **Vérification de bon fonctionnement des VPNs**

Afin de vérifier le bon fonctionnement du VPN, plusieurs commandes sont à notre disposition.

La commande "show crypto isakmp sa" fourni des informations sur l'association de sécurité d'ISAKMP. La figure ci-dessous nous montre la Vérification de connexion d'IPSec « ISAKMP » :

```
site-1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.0.0.2        10.0.0.1        QM_IDLE           1090    0 ACTIVE


IPv6 Crypto ISAKMP SA


site-1#
```

*Figure 59 : Vérification de connexion d'IPSec "ISAKMP".*

La commande "show crypto ipsec transform-set" nous permet de voir les différents types d'encodage actifs (la figure 60).

```
site-1#show crypto ipsec transform-set
Transform set 50: {     { esp-3des esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

*Figure 60 : Vérification de connexion d'IPSec "Transform-Set".*

La commande "show crypto ipsec sa" fourni une version plus détaillée que les deux commandes citées plus haut, voir la figure 61.

```
site-1#show crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: VPN_NAFTAL, local addr 10.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
   current_peer 10.0.0.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 22, #pkts encrypt: 22, #pkts digest: 0
   #pkts decaps: 21, #pkts decrypt: 21, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 10.0.0.1, remote crypto endpt.:10.0.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
     current outbound spi: 0x3EDA331F(1054487327)

     inbound esp sas:
      spi: 0x6A987546(1788376390)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2007, flow_id: FPGA:1, crypto map: VPN_NAFTAL
        sa timing: remaining key lifetime (k/sec): (4525504/106)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE
```

*Figure 61 : Vérification de connexion d'IPSec plus détaillée.*

La commande "show crypto map" nous permet de visionner des informations relatives aux cartes de cryptage crées (la figure 62).

```
site-1#show crypto map
Crypto Map VPN_NAFTAL 10 ipsec-isakmp
        Peer = 10.0.0.2
        Extended IP access list 100
            access-list 100 permit ip 192.168.100.0 0.0.0.255 192.168.200.0
0.0.0.255
        Current peer: 10.0.0.2
        Security association lifetime: 4608000 kilobytes/120 seconds
        PFS (Y/N): N
        Transform sets={
                50,
        }
        Interfaces using crypto map VPN_NAFTAL:
                Serial0/1/0
```

*Figure 62 : Vérification de la carte de cryptage.*

## VII. Conclusion

Dans ce chapitre, nous nous sommes focalisés sur l'aspect pratique de notre projet, tout en détaillant les étapes de mise en place de notre solution.

Nous avons commencé par présenter le simulateur Packet tracer, ensuite on a présenté l'architecture de l'entreprise avant l'amélioration, puis on a entamé la partie pratique qui a débuté par l'amélioration de l'architecture de l'entreprise basée sur les principes de sécurité VLANs ainsi que les VPNs. On a commencé par la configuration des VLANs au niveau des switchs ensuite au niveau de la configuration des routeurs nous avons effectué le routage inter-Vlan puis nous avons opté pour un VPN WIMAX de SLC, et bien sûr on a finalisé ces configurations par des vérifications et des tests pour la solution proposée

# Conclusion générale

Le domaine de la sécurité informatique est considéré comme difficile pour sa complexité de mettre en œuvre une solution durable qui répond parfaitement aux besoins et exigences ressentis dans une entreprise, ce qui pousse les ingénieurs réseau à travailler sans relâche à fin d'arriver à une solution permettant l'amélioration de la sécurité de leur réseau. De ce fait, nous avons effectué la mise en place d'une segmentation en VLAN et l'implémentation des VPN pour une sécurisation externe.

Pour mener à bien notre projet, nous avons parcouru notre thème sous deux parties l'un théorique, l'autre pratique. À savoir l'approche théorique qui était subdivisé en deux chapitres le premier a porté sur les Généralités sur les réseaux et la sécurité informatique, le second a porté sur les réseaux virtuels où nous sommes basés de façon claire sur les notions, les fonctionnements ainsi que les différents protocoles utilisés pour la mise en œuvre des réseaux virtuels.

Quant à la deuxième partie, elle est consacrée à la finalisation du projet, qui était aussi subdivisé en deux chapitres dont le premier nous avons présenté l'étude de l'existant dans laquelle nous avons présenté l'entreprise et exposé la problématique, laquelle nous avons solutionné par une solution VPN site-à-site qui consiste à mettre au point une liaison permanente, distante et sécurisée entre sites du Bejaia et Alger basée sur les WIMAX et aussi on a segmenté le réseau local en plusieurs VLANs , pour réduire les domaines de collisions et éviter les congestions, ce qui permet de renforcer la sécurité au niveau du réseau local.

Le deuxième chapitre de cette seconde partie a été consacré à la réalisation du projet, où nous avons introduit l'outils packet tracer qui a servis à l'élaboration du projet en expliquant les différentes configurations.

Ce travail a fait l'objet d'une expérience intéressante, qui nous a permis d'améliorer nos connaissances et nos compétences dans les domaines des réseaux informatiques. En définitive, comme tout travail scientifique, nous n'avons pas la prétention de réaliser un travail sans critique et suggestion de la part de tout lecteur afin de le rendre meilleur.

En guise de perspectives, on aimera implémenter la TOIP (Téléphonie sur IP) dans cette entreprise, étant donné que NAFTAL possède une infrastructure réseau solide composé de routeurs et switch CISCO il serait très bénéfique d'exploité ce matériels pour l'intégration de la téléphonie IP.

# Bibliographies


[1] T. DEAN, Réseaux Informatique, 2ème édition. Les Editions RYNALD GOULET, 972 pages, 2001.

[3] P. ATELIN, Réseaux informatiques Notions fondamentales (Normes, Architecture, Modèle OSI, TCP/IP, Ethernet, Wi-Fi, ...). Editions ENI, 407 pages, 2009.

[4] P. ATELIN and J. DORDOIGNE, TCP/IP et les protocoles Internet. Editions ENI, 190 pages, 2008.

[6] C. LLORENS, « Mesure de la sécurité logique d'un réseau d'un opérateur de télécommunications », thèse de doctorat en informatique et réseaux, ENST, pages 142, 2005.

[7] D. GODART, Sécurité informatique : risques, stratégies et solutions. Edition Edipro, 471 pages, 2002.

[10] S. GHERNAOUTI-HELIE, Sécurité informatique et réseaux, Edition DUNOD, 368 pages, 2011

[11] F. NOLOT, les Virtual LAN, cours, Université de Reims Champagne. Ardenne, 69 pages, 2009.

[12] R. SANCHEZ, Les réseaux locaux virtuels (VLAN) CERTA, 24 pages, janvier 2006.

[13] J. ARCHIER, LES VPN fonctionnement, mise en œuvre et maintenance des VPNs, Edition ENI, 684 pages, décembre 2013.

[15] E. GALLET DE SANTERRE, Protocole l2tp, Techniques de l'ingénieur, Télécoms, (TE7579), 2006.

[17] G. LABOURET, IPSEC : présentation technique, 47 pages, version du 16 juin 2000.

[18] V. REMAZEILLES, La sécurité des réseaux avec Cisco. Editions ENI, 600 pages, février 2009.

# Webographie


[2] https://www.algerietelecom.dz/fr/entreprises/wimax-prod22

[5] http://www.intrapole.com/spip.php?article18

[8] https://www.commentcamarche.net/contents/992-firewall-pare-feu,

[9] https://static-course-assets.s3.amazonaws.com/RSE6/fr/index.html#7.0.1.1. « Formation CCNA R&S: Routing and Switching Essentials ».

[14] http: //perso.modulonet.fr/ placurie/Ressources/BTS2-AMSI/Chap-8-Les20VPN.pdf

[16] https://desgeeksetdeslettres.com/vpn/les-differents-types-de-vpn

# Résumé

De nos jours, la sécurité informatique est quasi-indispensable pour le bon fonctionnement de n'importe quel réseau informatique. C'est pour cette raison que les entreprises implémentent des mécanismes et des protocoles de gestion, de sécurité plus robustes et efficaces afin de protéger leurs réseaux. L'objectif de notre travail accompli est de réussir à mettre en œuvre une amélioration de l'architecture de réseau de l'entreprise NAFTAL BITUME de la Wilaya de BEJAIA afin de gérer et sécuriser d'une bonne manière sûre le transfert interne et externe des données, en utilisant les liaisons virtuelles VLANs afin de segmenter et sécuriser le réseau intranet de l'entreprise et pour augmenter la sécurité externe en créant des réseaux privés virtuels VPNs, associé au protocole de tunneling IPSEC et basé sur les WIMAX (Worldwide Interoperability for Microwave Access).

**Mots clés :** VLANs, VPNs, IPSEC, WiMax.

# Abstract

Nowadays, computer security is almost indispensable for the proper functioning of any computer network. For this reason, companies are implementing more robust and effective management, security mechanisms and protocols to protect their networks.
The objective of our accomplished work is to successfully implement an improvement of the network architecture of the company NAFTAL BITUME of the wilaya of BEJAIA in order to manage and secure in a good way the internal and external transfer of data, Using VLANs virtual links to segment and secure the company's intranet network and to increase external security by creating VPNs (virtual private networks) associated with the IPSEC tunneling protocol, and WIMAX (Worldwide Interoperability for Microwave Access).

**Keywords**: VLANs, VPNs, IPSEC, WiMax