République Algérienne Démocratique Populaire
Ministère de l'Enseignement Supérieure et de la Recherche Scientifique
Université Abderrahmane Mira De Bejaïa
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

Solution de sécurité basée sur les VLANs et les VPNs

Cas d'étude : Entreprise SCS (Soummam Computer System)

Présenté par :

M[lle] BENAYACHE Afifa

M[lle] NAIT TAHAR Soria

Devant le jury composé de :

Président : M[r] TOUAZI Djoudi

Examinateur 1 : M[r] SALHI Nadir

Examinatrice 2 : M[me] AITHATRIT Fatima

Encadreur : M[r] BAADACHE Abderrahmane

Promotion 2017/2018

Remerciements

Nous tenons dans un premier temps à remercier et rendons grâce au bon Dieu le tout puissant, qui nous a donné le courage et la volonté pour mener à bien ce modeste travail.

Nous exprimons notre reconnaissance à Monsieur ***BAADACHE Abderrahmane*** *d'avoir joué pleinement son rôle de promoteur en étant à nos côtés tout au long de l'étude de notre projet, ses conseils et orientations nous a guidé jusqu'à l'aboutissement de ce travail.*

Nous remercions aussi Monsieur ***TOUAZI Djoudi*** *d'avoir accepté de présider le jury de notre soutenance. Ainsi qu'aux membres de jury constitué de : Monsieur* ***SALHI Nadir*** *et Madame* ***AITHATRIT Fatima*** *d'avoir accepté de juger ce modeste travail.*

Nos sincères remerciements s'adressent à nos parents, nos frères, nos sœurs ainsi qu'à toute la famille pour leur encouragement inconditionnels et surtout pour la confiance qu'ils nous accordent.

Enfin, Nous remercions tous ceux qui ont contribué de près ou de loin à l'élaboration de notre travail, en particulier tous nos ami(e)s pour leur soutien et leur présence à nos côtés.

Dédicace

Je dédie mon travail à mes parents surtout ma chère mère qui m'a soutenu tout en long de ma vie
À la mémoire de mes grands-parents, que Dieu les accueils en son vaste paradis
À mes chers frères et sœurs
À mes oncles et leurs familles sans exception
À mes cousins et cousines, oncles et tantes
À mes ami(e)s et collègues,
À toute personne qui m'a aidé et encouragé de prêt ou de loin tout au long de mes études

Afifa

Dédicace

Je dédie ce modeste travail :

A ma grande mère Baya

A ma mère et à mon père

A mes oncles et leur famille

A mes chères sœurs et frères

A mon promoteur M^r A.BAADACHE pour son soutien et ses conseils les plus précieux

A mes chères amies

Soria

Table des matières

Liste des figures

Liste des tableaux

Liste des abréviations

ACL: Access Control List

CLI: Command Language Interface

DHCP: Dynamic Host Configuration Protocol

DMZ: Demilitarized Zone

DOS: Denial Of Service

FTP: File Transfer Protocol

HTTP: Hypertext Transfer Protocol

HTTPS: HyperText Transfer Protocol Secure

ID: Identifier

IEEE: Institute of Electrical and Electronics Engineers

IOS : Internetwork Operating System

IPSec: Internet Protocol Security

ISL: Inter Switch Link Protocol

ISO: International Standards Organisation

LAN: Local Area Network

L2TP: Layer Two Tunneling Protocol

MAC: Media Access Control

MAN: Metropolitan Area Network

OSI: Open Systems Interconnection

PAN: Personal Area Network

PC: Personnel computer

POP3: Post Office Protocol

RFC: Request For Comments

RTC: Réseau Téléphonique Commuté

SCS: Sommam Computer System

TCP/IP: Transmission Control Protocol /Internet Protocol

VLAN: Virtual Local Area Network

VPN: Virtuel Private Network

VTP: Vlan Trunking Protocol

VTY: Virtual Teletype

WAN: Wide Area Network

Introduction générale

Introduction générale

Depuis la découverte de l'informatique, de nombreuses activités de la vie courante ont été simplifiés. Actuellement, les individus peuvent facilement traiter des informations en se servant de réseau informatique. Ce dernier devient de plus en plus indispensable pour la modernisation et le développement d'une entreprise ; son principal objectif est de gérer les données, limiter les impressions papiers pour le transfert d'informations et de travailler en équipe de manière productive pour faciliter l'échange de données et éviter le déplacement inutile du personnel. Aucune entreprise ne pourra être fiable si ses données ne sont pas protégées vu que ces dernières constituent un véritable patrimoine essentiel à sa pérennité. En effet, la perte ou la violation de ces informations peuvent mettre l'activité d'une entreprise en péril ou à la paralysie. Tous ces facteurs ont généré le problème de la sécurité au niveau local ou à distance.

Dans le cadre de notre travail, nous avons effectué un stage au sein de l'entreprise SCS (Sommam computer system). Au cours de ce stage, nous avons pu aborder tous ce qui concerne la sécurité de l'information qui circule à l'intérieur de l'entreprise ou vers l'extérieur. Dans ce contexte, nous avons utilisé, d'une part, la solution VLANs qui permet la séparation des flux entre les différents utilisateurs, ce qui renforce la sécurité au niveau du réseau local ; d'autre part, la solution VPNs qui met en œuvre un mécanisme d'authentification et de chiffrement des données protégeant les connexions distantes.

Afin d'atteindre les objectifs sollicités, nous avons structuré ce travail en quatre chapitres :

Le premier chapitre donnera un aperçu général sur les réseaux informatiques. Il a pour objectifs de définir les principaux concepts pour la compréhension des réseaux informatiques. Le deuxième chapitre sera consacré à la présentation de quelques notions de base sur la sécurité des réseaux informatique qui nous serviront dans la partie pratique. Et dans le troisième chapitre, nous étudierons en profondeur la sécurité et plus particulièrement la solution VLANs et VPNs.

Le dernier chapitre sera devisé en deux parties ; la première portera sur la présentation de l'entreprise qui nous a accueillis pendant notre stage, ainsi que sur la problématique rencontré, la deuxième partie sera consacrée à la réalisation de notre travail portant sur l'implémentation et la simulation des VLANs et des VPNs.

Notre travail s’achève par une conclusion générale qui récapitule tous les éléments essentiels abordés dans ce mémoire.

Chapitre I : *Généralités sur les réseaux informatiques*

1. Introduction

Les réseaux informatiques qui permettaient à leur origine de relier des terminaux passifs à de gros ordinateurs centraux, autorisent à l'heure actuelle l'interconnexion de tous types d'ordinateurs, que ce soit de gros serveurs, des stations de travail, des ordinateurs personnels ou de simples terminaux graphiques. Les services qu'ils offrent font partie de la vie courante des entreprises et des administrations (banques, gestion, commerce, bases de données, recherche, etc.) et des particuliers (messagerie, loisirs, services d'informations par minitel et Internet...).

L'objectif de ce chapitre est de présenter quelques concepts de base sur les réseaux informatiques pour mieux comprendre leur fonctionnement. Toutes les notions nécessaires seront présentées, tirant exemple de la classification des réseaux selon plusieurs critères, les réseaux locaux, les périphériques réseaux ainsi le modèle OSI et TCP/IP.

2. Réseaux informatiques

2.1 Définition

La technologie des réseaux informatiques constitue l'ensemble des outils qui permettent à des ordinateurs de partager des informations et des ressources, il est constitué d'équipements appelés nœuds qui peuvent communiquer entre eux, en utilisant des protocoles, ou langages compréhensibles par tous. Ces réseaux sont catégorisés en fonction de leur étendue et de leur domaine d'application [1].

2.2 Classification des réseaux

Les caractéristiques principales qui vont permettre de différencier les grandes familles de réseaux sont la taille (voir figure I.1), le mode de connexion, le type de connexion, la topologie et le mode de commutation [2] :

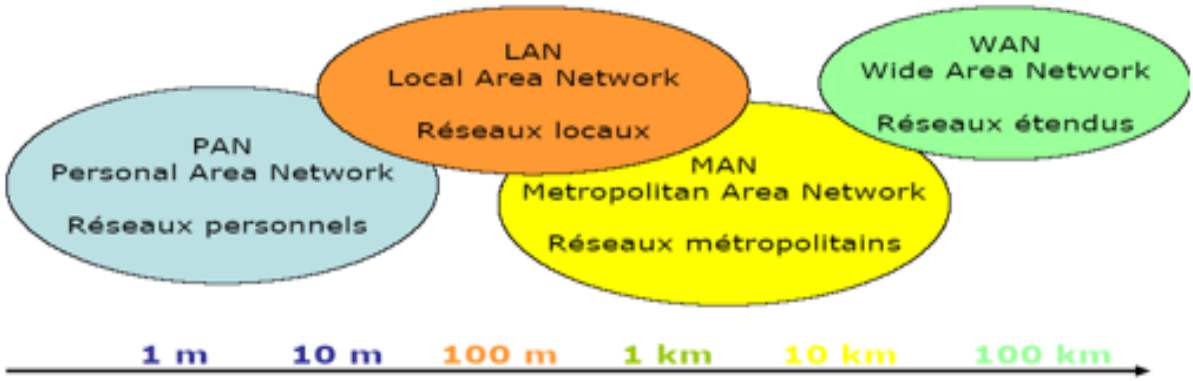

Figure I.1 : Classification des réseaux selon l'étendue [2].

- **Selon la taille**

✓ **Réseaux personnels**

Le réseau PAN (Personal Area Network**)** désigne un réseau restreint d'équipements informatiques habituellement utilisés dans le cadre d'une utilisation personnelle. Les bus utilisés les plus courants sont l'USB (Universal Serial Bus), les technologies sans fil telles que Bluetooth, l'IR (Infrarouge). Ces réseaux interconnectent sur quelques mètres les équipements personnels tels que des téléphones mobiles, des téléphones portables, etc.

✓ **Réseaux locaux**

Le réseau LAN (Local Area Network) est un réseau informatique à une échelle géographique relativement restreinte, par exemple une salle informatique, une habitation particulière, un bâtiment ou un site d'entreprise. Dans le cas d'un réseau d'entreprise, on utilise souvent le terme RLE pour Réseau Local d'Entreprise. Car il présente les caractéristiques suivantes :

- Il occupe un emplacement physique et un seul, comme le suggère le mot «local».
- Leur vitesse de transfert de données est élevée, de 10 à 1000 Mbit/s.
- Toutes les données circulent sur le câblage local.

✓ **Réseaux métropolitains**

Les réseaux MAN (Metropolitan Area Network) sont à mi-chemin entre les réseaux locaux et les réseaux étendus. Un réseau métropolitain est un réseau qui dessert une ville entière, mais qui utilise la technologie des réseaux locaux. Les MAN interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi il permet à deux nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local.

Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique). Ils s'étendent à des distances allant de deux kilomètres jusqu'à une dizaine de kilomètre et ne dépassant pas les 200 kilomètres. Ces réseaux doivent être tolérants aux pannes, car vus les étendus couvertes, la coupure d'un câble ne doit pas paralyser les entreprises.

✓ **Réseaux étendus**

Le réseau WAN (Wide Area Network) permet l'interconnexion de plusieurs LANs ou MANs sur de grandes distances géographiques, à l'échelle d'un pays ou mondiale. A la différence du LAN qui est un réseau privé, le WAN emprunte les infrastructures publiques telles Internet, ou celles d'un opérateur. Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles. Le plus grand WAN est le réseau Internet.

- **Selon la topologie**

Un réseau informatique est constitué d'ordinateurs reliés entre eux. L'arrangement physique (type de câblage) de ces éléments est appelé topologie physique. Il en existe généralement [2] :

✓ **Topologie en bus**

Une topologie en bus (voir figure I.2) est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Les connecteurs utilisés sont de types : connecteur en T ou Vampire. Le mot « bus» désigne la ligne physique qui relie les machines du réseau. Une seule station émet sur le bus. Lorsque celle-ci émet, la trame parcourt tout le bus jusqu'à ce qu'elle arrive au destinataire. L'exemple le plus courant de ce type de réseau est le réseau Ethernet.

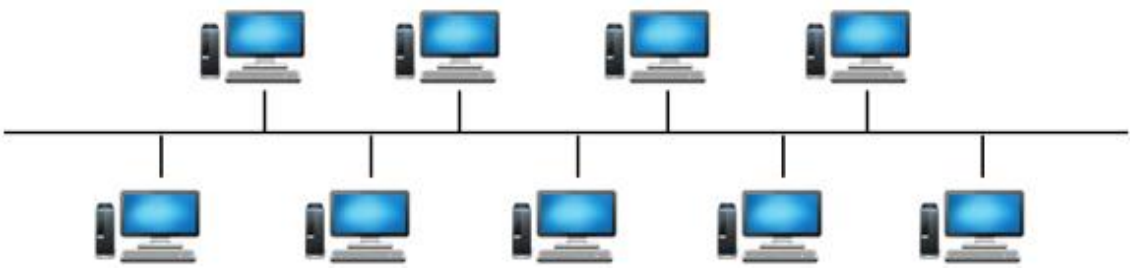

Figure I.2 : Topologie en bus [2].

✓ **Topologie en anneau**

Comme illustré dans la figure I.3, il s'agit d'un réseau local dans lequel les nœuds sont reliés à un répartiteur appelé MAU (Multi station Access Unit), les données circulent sur un anneau (qui n'est souvent que virtuel) d'un nœud à l'autre. A un instant donné, un seul

nœud peut émettre sur le réseau. Il ne peut donc pas se produire de collision entre deux messages contrairement au cas du réseau de type bus. Un jeton (qui est en fait une trame de donnée) circule en permanence le long de la boucle. Lorsqu' aucun nœud n'émet de message, le jeton est dans un état libre (trame vide). Seul le nœud qui a envoyé le message est en attente d'un accusé de réception. Les autres nœuds n'étant pas en alerte, se contentent de retransmettre l'accusé de réception sans le lire. Lorsque le jeton arrive à la station émettrice celle-ci vérifie l'accusé de réception, retire son message et rend le jeton libre et ainsi de suite… Cette topologie est utilisée par les réseaux Token Ring et FDDI.

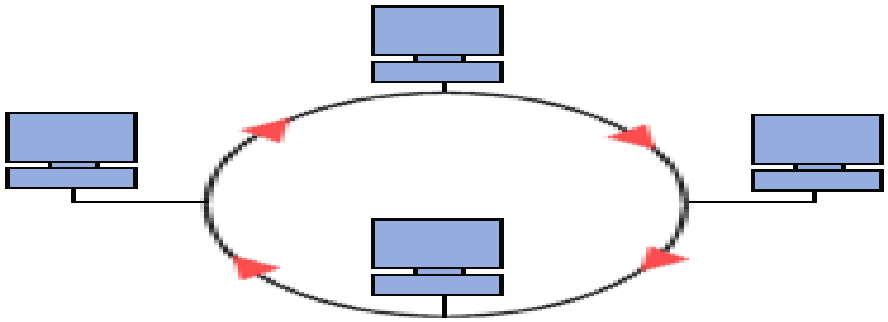

Figure I.3 : Topologie en anneau [2].

- ✓ **Topologie en étoile**

Dans un réseau en étoile (voir figure I.4), chaque nœud du réseau est relié à un nœud central (Switch ou hub). Ce nœud est un appareil qui recevant un signal de données par une de ses entrées, va retransmettre ce signal à chacune des autres entrées sur lesquelles sont connectés des ordinateurs ou périphériques.

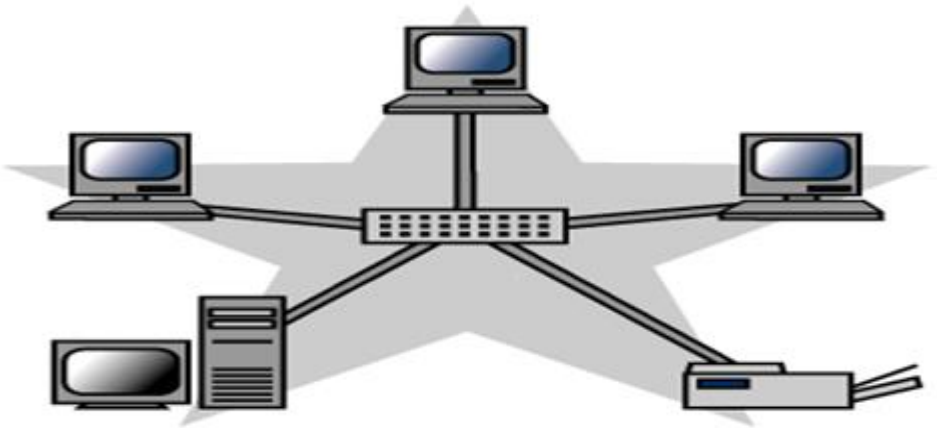

Figure I.4 : Topologie en étoile [2].

✓ **Topologie en arbre**

Aussi connue sous le nom de hiérarchique. Le sommet, de haut niveau, est connecté à plusieurs nœuds de niveau inférieur dans la hiérarchie. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le tout dessine alors un arbre, ou une arborescence (voir figure I.5). Le point faible de ce type de topologie réside dans l'ordinateur "père" de la hiérarchie qui, s'il tombe en panne, paralyse le réseau.

Figure I.5 : Topologie en arbre [2].

✓ **Topologie maillée**

La plupart des réseaux étendus adoptent une topologie maillée. Une topologie maillée correspond à plusieurs liaisons point à point (voir figure I.6). Une unité réseau peut avoir (1, N) connexions point à point vers plusieurs autres unités. L'inconvénient est le nombre de liaisons nécessaires qui devient très élevé lorsque le nombre de terminaux l'est : s'il y a N terminaux, les nombres de liaisons nécessaires est de N. (N-1)/2. Cette topologie se rencontre dans les grands réseaux de distribution (Exemple : Internet).

Figure I.6 : Topologie maillée [2].

L'information peut parcourir le réseau suivant des itinéraires divers à l'aide des routeurs par exemple.

- **Selon le type de connexion (ou mode de diffusion)**

On distingue deux classes de réseau [2] :

✓ **Réseaux point à point**

Ces réseaux sont caractérisés par un canal de communication qui ne relie que deux machines (liaison point à point), c'est-à-dire que pour arriver à sa destination, un message doit transiter par plusieurs machines intermédiaires.

✓ **Réseaux à diffusion**

Ces réseaux sont caractérisés par un canal de communication partagé par un ensemble de machines (liaison multipoint). Toutes les machines se partagent un seul et unique canal de communication. Lorsqu'une machine émet un message sur ce réseau, toutes les autres machines, sans exception, le reçoivent également.

- **Selon le mode de connexion**

Quelle que soit l'architecture physique d'un réseau on trouve deux modes de fonctionnement différents [2] :

✓ **Avec connexion**

Dans ce mode toute communication entre deux équipements suit le processus suivant :

1. L'émetteur demande l'établissement d'une connexion par l'envoi d'un bloc de données spécial.
2. Si le récepteur refuse cette connexion la communication n'a pas lieu.
3. Si la connexion est acceptée, elle est établie par mise en place d'un circuit virtuel dans le réseau reliant l'émetteur au récepteur.
4. Les données sont ensuite transférées d'un point à l'autre.
5. La connexion est libérée.

✓ **Sans connexion**

Dans le mode sans connexion les blocs de données, appelés datagrammes, sont émis sans vérifier à l'avance si l'équipement à atteindre, ainsi que les nœuds intermédiaires éventuels, sont bien actifs. Ce service est celui du courrier postal classique et suit les principes généraux suivants :

- Le client poste une lettre dans une boîte aux lettres.

- Chaque lettre porte le nom et l'adresse du destinataire.
- Chaque client a une adresse propre et une boîte aux lettres.
- Le contenu de l'information reste inconnu du prestataire de service.
- Les supports du transport sont inconnus de l'utilisateur du service.

- **Selon le mode de commutation** [3]

✓ **Commutation de circuit**

Ce type de commutation établit une liaison physique temporaire, pendant toute la durée de la communication. Cette commutation de circuit est utilisée par le RTC (Réseau Téléphonique Commuté).

✓ **Commutation de messages**

Ici, il n'est pas nécessaire d'établir un chemin dédié entre les deux stations qui communiquent. En fait, lorsqu'une station envoie un message, l'adresse du destinataire est ajoutée au paquet. Le message est alors transmis en un seul bloc, de nœud en nœud. Chaque nœud reçoit le message en entier, le stocke brièvement, puis le transmit au suivant : on parle alors de store and forward.

✓ **Commutation de paquets**

La commutation de paquets combine celle de messages et celle de circuits. Deux techniques sont couramment utilisées. Dans les deux cas, un message est décomposé en paquets, chacun contenant les adresses source et destination.

2.3 Rôle des réseaux informatique

Il peut être intéressant de mettre en place un réseau, local ou longue distance, pour des raisons techniques d'une part, et orientées vers l'utilisateur d'autre part [4] :

- **Objectifs techniques**

L'une des raisons justifiant très souvent l'installation d'un réseau est le partage des ressources entre plusieurs utilisateurs. Il est en effet particulièrement intéressant d'accéder à des données à distance et de réaliser sur ces dernières toutes les opérations qui seraient disponibles en travaillant réellement sur l'ordinateur distant.

- **Objectifs utilisateurs**

La communication est sans nul doute l'aspect le plus intéressant pour un utilisateur. Elle peut prendre la forme de courrier électronique, de vidéoconférence, de téléphonie mobile, de groupes d'intérêts. Un certain nombre de services sont proposés aux particuliers via réseau. L'accès à l'information est de loin le plus utilisé. Cette

information peut être de type financier (banques, bourse…), des journaux électroniques, des bibliothèques en ligne. La toile WWW (World Wide Web) est aujourd'hui une source mondiale d'informations de tous types directement utilisables par chaque utilisateur, et basée sur l'interconnexion physique d'un très grand nombre de réseaux locaux.

3. Réseaux locaux

3.1 Définition

Le réseau local, apparu dans les années 1970, représente un système de communication locale reliant plusieurs ordinateurs (Serveurs, stations de travail et périphériques) dans un rayon de quelques kilomètres. Ces réseaux permettent de transférer des données à des vitesses élevées, sur des courtes distances et dans les limites d'une enceinte privée [5].

3.2 Utilité des réseaux locaux

Le réseau local a pour but de [5] :

- Mettre en commun des données communes à plusieurs utilisateurs (fichiers comptables par exemple...).
- Partager des périphériques (FAX, MODEM, imprimantes, lecteur de CD ROM...).
- Partager un accès à internet.
- Partager des applications.
- Partager des documents (classeur Excel, textes Word, base de données).
- Accéder à un site Intranet.

4. Modèles de réseaux

4.1 Modèle OSI

Pour faciliter l'interconnexion des systèmes, un modèle dit d'interconnexion des systèmes ouverts, appelé encore OSI (Open Systems Interconnection) élaboré par ISO (International Standards Organisation). Le modèle OSI comme illustré dans la figure I.7, constitue un cadre de référence qui nous permet de comprendre comment les informations circulent dans un réseau. C'est aussi un modèle conceptuel d'architecture de réseau qui facilite la compréhension théorique du fonctionnement des réseaux. Il est constitué de sept couches, chacune définissant des fonctions particulières du réseau [6].

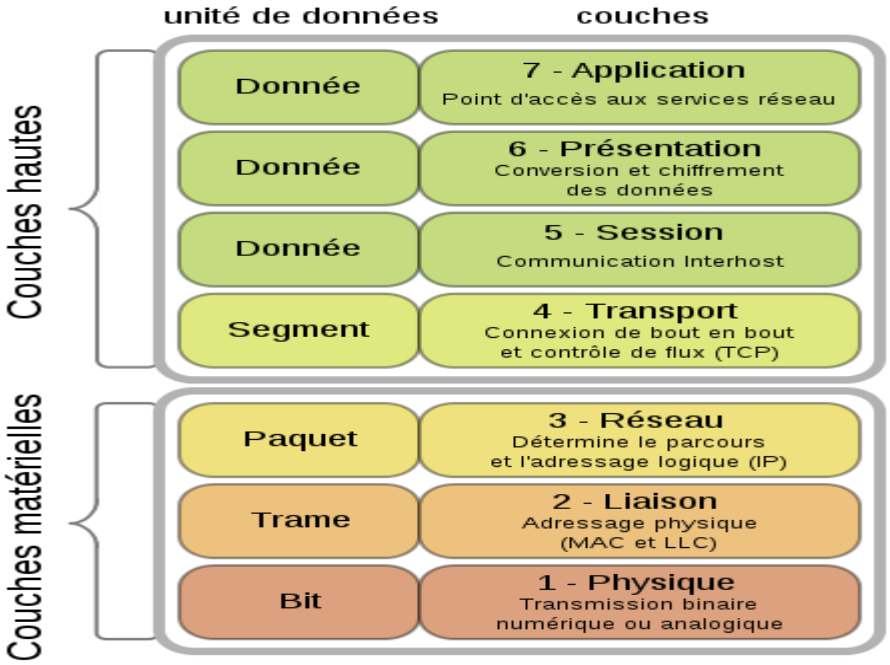

Figure I.7 : Modèle OSI [7].

Couche physique : La couche physique contient les règles et procédures à mettre en œuvre pour acheminer les éléments binaires sur le médium physique, elle possède des équipements réseau qui traitent l'élément binaire, comme les modems, concentrateurs, ponts, hubs, etc.

Couche liaison : La trame est l'entité transportée sur les lignes physiques, elle contient un certain nombre d'octets transportés simultanément.

Couche réseau : La couche réseau ou niveau paquet permet l'acheminement correcte des paquets d'information jusqu'à l'utilisateur final. Pour aller de l'émetteur au récepteur, il faut passer par des nœuds de transfert intermédiaires ou par des passerelles, qui interconnectent deux ou plusieurs réseaux.

Couche transport : La couche transport prend en charge le transport du message de l'utilisateur d'une extrémité à une autre du réseau.

Couche session : Le rôle du niveau session est de fournir aux entités de présentation les moyens nécessaires à l'organisation et à la synchronisation de leur dialogue, de fournir les services permettant l'établissement d'une connexion, son maintien et sa libération, ainsi que ceux permettant de contrôler les interactions entre les entités de présentation.

Couche présentation : Le niveau présentation se charge de la syntaxe des informations que les entités d'application se communiquent.

Couche application : Le niveau application est le dernier du modèle de référence. Il fournit aux processus applicatifs le moyen d'accéder à l'environnement réseau. Ces processus échangent leurs informations par l'intermédiaire des entités d'application.

4.2 Modèle TCP/IP

Le modèle TCP/IP comme illustré dans la figure I.8, définit une architecture de référence en quatre couches : la couche application, la couche transport, la couche Internet et la couche d'accès au réseau, permettant aux diverses applications réseau d'accéder à un support de transmission, en faisant appel aux services proposés par deux couches intermédiaires [4].

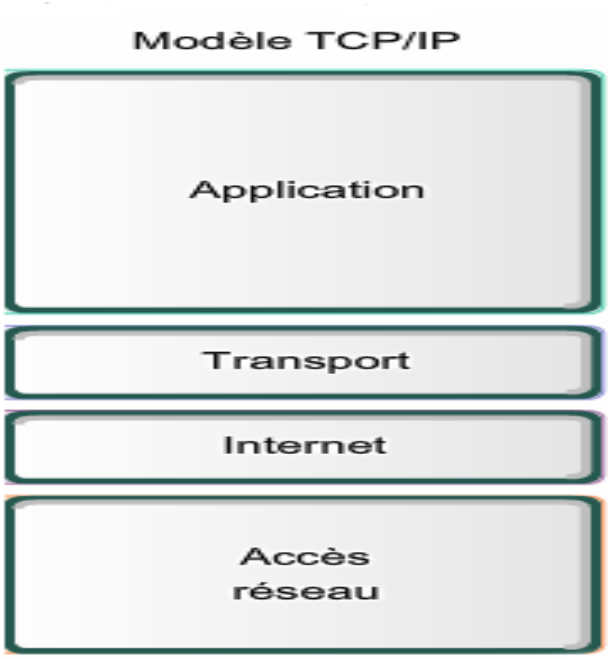

Figure I.8 : Modèle TCP/IP [7].

Couche Application : Les concepteurs du modèle TCP/IP estimaient que les protocoles de niveau supérieur devaient inclure les détails des couches session et présentation. Ils ont donc simplement créé une couche application qui gère les protocoles de haut niveau, les 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 [8].

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 [8].

Couche Réseau : 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 Protocole) [8].

Couche d'accès au réseau : Le nom de cette couche a un sens très large et peut parfois prêter à confusion. On lui donne également le nom de couche hôte-réseau. Cette couche se charge de tout ce dont un paquet IP a besoin pour établir une liaison physique avec l'hôte de destination [8].

5. Equipements de base d'un réseau informatique [9]

- **Le concentrateur**

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

- **Le répéteur**

  Le répéteur (appelé Repeater en anglais) est un équipement utilisé pour régénérer le signal entre deux nœuds du réseau, afin d'étendre la distance du réseau.

- **Le pont**

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

- **Le commutateur**

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

- **La passerelle**

  La passerelle est un système matériel et logiciel permettant de relier deux réseaux et servant d'interfaces entre deux protocoles différents.

- **Le routeur**

  C'est un matériel de communication de réseau informatique qui permet de choisir le chemin qu'un message va emprunter. Il est utilisé pour relier des réseaux locaux de technologie différente.

6. L'adressage IP

Dans un réseau IP (Internet Protocol), toutes les machines, postes client ou serveur, possèdent un adresse qui permet de les identifier. Ainsi, il est possible de déterminer qui est l'émetteur d'un message et qui est son destinataire. Dans le protocole IP actuel (version 4), une adresse IP est codée sur 4 octets, ce qui correspond à une adresse de 32 bits. L'adresse IP est généralement présentée sous forme décimal [10].

6.1 L'adresse IP

Chacun des éléments d'un réseau travaillant avec le protocole IP doit posséder une adresse unique sur le réseau : adresse IP. Ce label numérique est employé d'une part pour identifier chaque équipement et d'autre part pour réaliser le routage des datagrammes IP dans le réseau. Toute adresse IP est composée de deux parties distinctes : une partie nommée identificateur réseau (Net-ID) qui désigne le réseau contenant les ordinateurs et une partie nommée identificateur de l'hôte (Host-ID**)** qui désigne les ordinateurs de ce réseau.

Il existe des adresses IP de version 4 (sur 32 bits, soit 4 octets) et de version 6 (sur 128 bits, soit 16 octets). La version 4 est actuellement la plus utilisée : elle est généralement représentée en notation décimale avec quatre nombres compris entre 0 et 255, séparés par des points [4].

6.2 Le sous réseau

Un sous-réseau est une subdivision logique d'un réseau de taille plus importante. Le masque de sous-réseau permet de distinguer la partie de l'adresse utilisée pour le routage et celle utilisable pour numéroter des interfaces. Un sous-réseau correspond typiquement à un réseau local. Diviser la partie "host number" d'une adresse réseau permet de créer un sous-réseau Historiquement, on appelle également sous-réseau chacun des réseaux connectés à Internet [11].

6.3 Masque de sous-réseau

Les adresses IPv4 sont composées de deux parties : le sous-réseau et l'hôte. On considérait autrefois que l'adresse du réseau était définie par sa classe, et obtenue en

appliquant l'opérateur booléen ET bit à bit entre le masque par défaut associé et l'adresse IPv4. Un masque de sous-réseau est un masque indiquant le nombre de bits d'une adresse IPv4 utilisés pour identifier le sous-réseau et le nombre de bits caractérisant les hôtes (ce qui indique aussi le nombre d'hôtes possibles dans ce sous-réseau).

L'adresse du sous-réseau est obtenue en appliquant l'opérateur ET binaire entre l'adresse IPv4 et le masque de sous-réseau. L'adresse de l'hôte à l'intérieur du sous-réseau est quant à elle obtenue en appliquant l'opérateur ET entre l'adresse

IPv4 et le complément à un du masque.

Les masques de sous-réseau utilisent la même représentation que celles des adresses IPv4 [11].

6.4 Les classes d'adresses IP

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

Il existe cinq classes d'adresses dénommées A, B, C, D et E (voir figure I.9) telle que, chaque classe a un format spécial de son adresse IP [11].

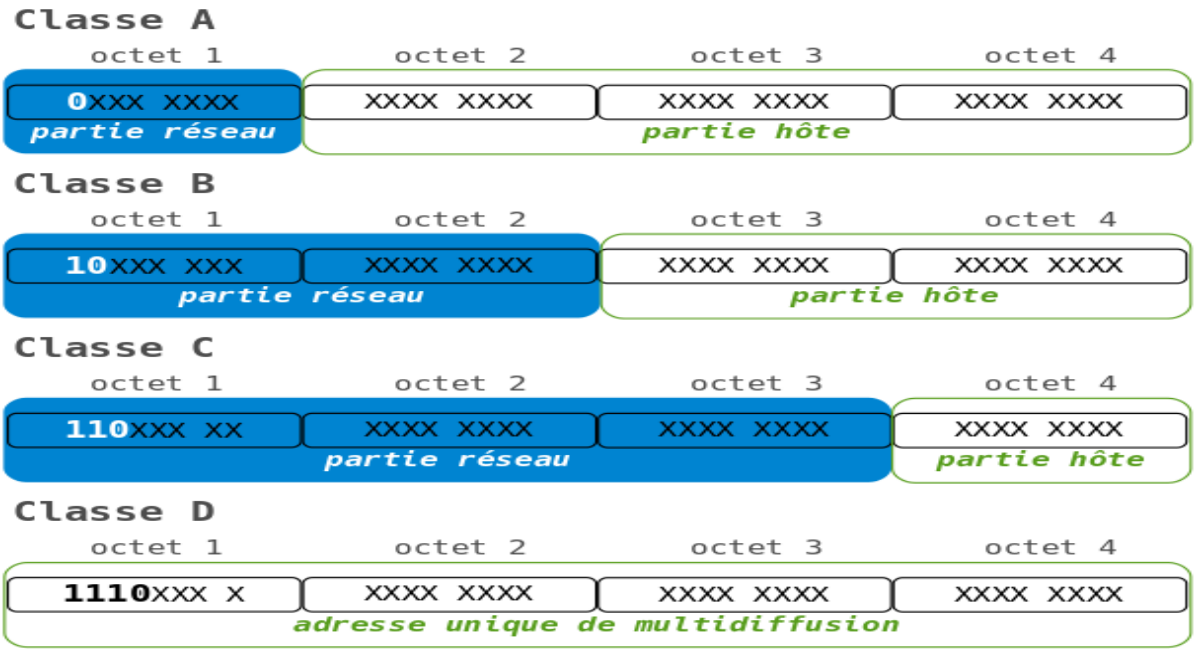

Figure I.9 : Caractéristiques des classes des adresses IP [12].

Classe A : Les adresses de classe A sont affectées aux réseaux qui comprennent de très nombreux hôtes. Le bit de plus fort poids d'une adresse de classe A vaut toujours 0. Les 7 bits suivants, qui complètent le premier octet, forment avec celui-ci l'identificateur d'hôte. Une telle adresse peut donc définir 126 réseaux avec 16 777 214 hôtes par réseau.

Classe B : Les adresses de la classe B sont employées dans les réseaux de taille moyenne ou grande. Les 2 bits de poids fort sont toujours 10. Les 14 bits suivants, qui complètent les 2 premiers octets, forment avec les deux premiers l'indicateur de réseau. Les 2 derniers octets représentent l'indicateur d'hôte. Cette structure permet de définir 16 384 réseaux et 65 534 hôtes par réseau.

Classe C : Les adresses de classe C sont utilisées par les petits réseaux. Les 3 bits de poids fort d'une adresse de classe C sont toujours 110. Les 21 bits suivants, qui complètent les 3 premiers octets, forment avec les trois premiers l'identificateur de réseau. L'octet restant constitue l'identificateur d'hôte. Cette structure permet de définir 2097 152 réseaux et 254 hôtes par réseau.

Classe D : Les adresses de la classe D sont réservées aux adresses de multidiffusion IP. Les 4 bits de poids fort d'une adresse de la classe D valent toujours 1110. Les bits restants constituent l'adresse reconnue par les hôtes intéressés.

Classe E : La classe E est une classe d'adresses expérimentales réservées à un usage futur. Les 4 bits de poids fort d'une adresse de classe E valent toujours 1111.

7. Conclusion

Au cours de ce chapitre, nous avons défini les réseaux informatiques, leurs importances et leurs différents composants. Par la suite, nous avons présenté la manière dont les données sont transmises à travers les couches des deux modèles OSI et TCP/IP, en passant par les services offerts par ces derniers ainsi que l'adressage et ses classes.

Le chapitre suivant va porter sur la sécurité des réseaux informatiques qui est devenue un sérieux problème et que la majorité des entreprises ne peuvent plus l'ignorer.

Chapitre II *: Sécurité des réseaux informatiques*

1. Introduction

La sécurité informatique est devenue de nos jours un problème majeur dans la gestion des réseaux d'entreprise ainsi que pour les particuliers toujours plus nombreux à se connecter à Internet. La transmission d'informations sensibles et le désir d'assurer la confidentialité de celles-ci est devenue un point primordial dans la mise en place de réseaux informatiques. La sécurité informatique est la mise en œuvre de techniques et méthodes logique ou physique pour minimiser la vulnérabilité d'un système contre des menaces. D'une manière générale, elle consiste à assurer que les ressources matérielles ou logiciels d'une organisation soient uniquement utilisées dans le cadre prévu.

Ce chapitre a pour but de définir quelques notions sur la sécurité informatique, ses termes et ses objectifs, pour ensuite exposer les vulnérabilités et les dangers. Enfin passerons à l'élaboration de dispositif de sécurité afin de se protéger des attaques et des faiblesses du réseau.

2. Sécurité informatique

La sécurité est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système informatique contre les menaces accidentelles ou intentionnelles auxquelles il peut être confronté. En d'autres mots, c'est l'ensemble des techniques qui assurent que les ressources du système d'information (matérielles ou logicielles) d'une organisation sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient [13].

3. Objectifs de la sécurité informatique

La sécurité d'un réseau informatique d'une manière générale, vise les objectifs suivants [14] :

- **Authentification**

  L'authentification permet de vérifier l'identité annoncée et s'assurer de la non-usurpation de l'identité d'une entité. Pour cela, l'entité devra produire une information spécifique telle que par exemple un mot de passe (un code, une empreinte biométrique, etc.).

- **Confidentialité**

  La confidentialité est la protection des données contre une divulgation non autorisée.

- **Intégrité**

  Le critère d'intégrité est relatif au fait que des ressources, données, traitements, transactions ou services n'ont pas été modifiés, altérés ou détruits tant de façon intentionnelle qu'accidentelle.

- **Disponibilité**

  Pour un utilisateur, la disponibilité d'une ressource est la probabilité de pouvoir mener correctement à terme une session de travail.

- **Non-répudiation**

  La non-répudiation est le fait de ne pouvoir nier ou rejeter qu'un évènement (action, transaction) a eu lieu.

4. Terminologie de la sécurité informatique

4.1 Vulnérabilité

Une vulnérabilité ou faille est une faiblesse dans un système informatique, permettant à un attaquant de porter atteinte à la sécurité de ce système [13].

4.2 Risque

Un risque permet de mesurer les possibilités de l'occurrence d'un événement associé à une situation ou une activité, de l'autre côté, un enjeu est grossièrement ce que l'on peut gagner ou perdre en posant un acte. Dans le cas de la sécurité informatique en entreprise, il s'agit plutôt de ce que l'on peut perdre, en l'absence de moyens adéquat de sécurisation. Lorsque l'on évoque les risques susceptibles d'engendrer un incident informatique sur le Système d'Information d'une entreprise [13].

4.3 Attaque

C'est l'ensemble des actions malveillantes qui constituent la plus grosse partie du risque, elles font principalement l'objet de mesures de protection. Parmi elles, on compte [15] :

- **Attaque par force brute**

  On appelle attaque par force brute le cassage d'un mot de passe en testant les mots de passe possibles. Cette méthode est en général considérée comme la plus simple concevable.

- **Attaque par déni de service**

Une attaque par déni de service (DOS, Denial Of Service) est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou ressources d'un réseau. On distingue habituellement deux types de dénis de service :

- ✓ **Les dénis de service par saturation :** Consistant à submerger une machine de requêtes, afin qu'elle ne soit plus capable de répondre aux requêtes réelles.
- ✓ **Les dénis de service par exploitation de vulnérabilité :** Consistant à exploiter une faille du système distant, afin de le rendre inutilisable.

- **Attaque « man in the middle »**

Une attaque man in the middle est un scénario d'attaque dans lequel un pirate écoute une communication entre deux interlocuteurs et falsifie les échanges afin de se faire passer pour l'une des parties.

- ✓ **Attaque par rejeu :** les attaques par rejeu (replay attaque) sont des attaques de type man in the middle consistant à intercepter des paquets de données et à les rejouer, c'est-à-dire les retransmettre tels quel (sans aucun déchiffrement) au serveur destinataire.
- ✓ **Détournement de session TCP :** le vol de session TCP est une technique consistant à intercepter une session TCP initiée entre deux machines afin de la détourner.
- ✓ **Attaque de protocole ARP :** une des attaques man in the middle les plus célèbres consiste à exploiter une faiblesse du protocole ARP (Address Resolution Protocol) dont l'objectif est de permettre de retrouver l'adresse IP d'une machine connaissant l'adresse physique (adresse MAC) de sa carte réseau.

- **Spoofing IP**

L'usurpation d'adresse IP est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine. Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement. Il ne s'agit pas pour autant d'un changement d'adresse IP, mais d'une mascarade de l'adresse IP au niveau des paquets émis.

5. Logiciels malveillants

La sécurité a pour but de s'assurer de l'intégrité des données stockées dans les machines informatiques et de les protéger des risques pouvant les altérer. Ceux-ci peuvent prendre plusieurs formes [16] :

- **Virus**

  Un virus est un logiciel capable de s'installer sur un ordinateur à l'insu de son utilisateur légitime. Le terme virus est réservé aux logiciels qui se comportent ainsi avec un but malveillant.

- **Ver**

  Un ver (Worm) est logiciel malveillant qui s'autoréplique et qui se propage via le réseau comme internet par exemple**.** Ce ver se répand de système en système en exploitant des failles informatiques et humaines, il va donc essayer de se répandre sur un maximum d'ordinateurs, pour le but de voler des données, chiffrer des fichiers, l'accès à distance (backdoor)…etc.

- **Cheval de troie**

  Un cheval de Troie (Trojan horse) est un logiciel qui se présente sous un jour honnête, utile ou agréable, et qui, une fois installé sur un ordinateur y effectue des actions cachées et pernicieuses.

- **Porte dérobée**

  Une porte dérobée (backdoor) est un logiciel de communication caché, installé par exemple par un virus ou par un cheval de Troie, qui donne à un agresseur extérieur accès à l'ordinateur victime, par le réseau.

- **Bombe logique**

  Une bombe logique est une fonction cachée dans un programme en apparence honnête, utile ou agréable, qui se déclenchera à retardement, lorsque sera atteinte une certaine date, ou lorsque surviendra un certain événement. Cette fonction produira alors des actions indésirées.

- **Logiciel espion**

  Un logiciel espion, comme son nom l'indique, collecte à l'insu de l'utilisateur légitime des informations au sein du système où il est installé, et les communique à un agent extérieur, par exemple au moyen d'une porte dérobée.

Une variété particulièrement toxique de logiciels espion est le keylogger (espion dactylographique), qui enregistre fidèlement tout ce que l'utilisateur tape sur son clavier et le transmet à son honorable correspondant.

- **Courrier électronique non sollicité (spam)**

Le spam, que l'on appelle en français courrier indésirable ou pourriel, est une forme de communication électronique non sollicitée, à des fins plus souvent publicitaires ou malhonnêtes. Ciblant principalement les messageries, le spam est diffusé de façon massive et automatisée.

6. Mécanismes de sécurité

De nombreuses solutions existent pour améliorer la protection et la sécurité d'un ordinateur personnel ou d'un réseau contre les menaces extérieures sans pour autant nécessiter un niveau de connaissance élevé de la part des utilisateurs. Les moyens de protection les plus connus et utilisés sont :

a. Anti-virus à jour

L'objectif principal est de limiter la prolifération virale dans le cas ou au moins une machine est infectée. Trois solutions complémentaires existent :

- Un logiciel d'antivirus disposé sur la passerelle d'accès à internet. cette solution consiste à réaliser un filtrage applicatif sur l'ensemble des flux qui transitent par cette passerelle.
- Un logiciel antivirus installé et opérationnel sur le serveur messagerie.
- Un logiciel antivirus installé et opérationnel sur tous les postes de travail et tous les serveurs présents dans le système d'information [17].

b. Cryptographie

La cryptographie est une science très ancienne. Elle a été utilisée exclusivement à des fins militaires. Aujourd'hui, les réseaux informatiques exigent une phase de cryptographie comme mécanisme fondamental afin d'assurer la confidentialité de l'information numérique.

Le cryptage, ou chiffrement, garantit l'inviolabilité, l'intégrité et l'authenticité des données pendant leur stockage et leur transmission. On distingue généralement deux types de chiffrement essentiel [18] :

- **Chiffrement symétrique**

  Un algorithme symétrique est un algorithme qui permet de transformer un texte en clair en texte chiffré en utilisant une clé et de retransformer le texte chiffré en texte en clair en utilisant la même clé. Le secret de la communication est uniquement assuré par la clé qui est utilisée lors de la phase de chiffrement et de déchiffrement. L'algorithme utilisé ne fait pas partie du secret.

- **Chiffrement asymétrique**

  Les algorithmes asymétriques ont été inventés pour pallier précisément le problème de transmission sécurisée de la clé. On parle d'algorithmes asymétriques car ce n'est pas la même clé qui sert au chiffrement et au déchiffrement. Dans le cas de ces algorithmes, on parlera alors de clé privée et de clé publique. Ces deux clés sont intimement liées par une fonction mathématique complexe.

c. Signature numérique

Le paradigme de signature numérique est un procédé permettant de garantir l'authenticité de l'expéditeur (fonction d'authentification) et de vérifier l'intégrité du message reçu. La signature numérique assure également une fonction de non répudiation. C'est-à-dire qu'elle permet d'assurer que l'expéditeur a bien envoyé le message [15].

Les concepts de signature numérique sont principalement basés sur la cryptographie asymétrique. Cette technique permet de chiffrer en utilisant la clé privée et déchiffrer en utilisant la clé publique [19].

d. Le hachage

Une fonction de hachage par fois appelée fonction de condensation est une fonction permettant d'obtenir un condensé d'un texte, c'est -à- dire une suite de caractères assez courte représentant le texte qu'il condense.

La fonction de hachage a des propriétés : doit être telle qu'elle associe un et un seul haché à un texte en clair (cela signifie qu'une moindre modification du document entraîne la modification de son haché). D'autre part, il doit s'agir d'une fonction à sens unique (one-way faction) afin qu'il soit impossible de retrouver le message original à partir du condensé. S'il existe un moyen de retrouver le message en clair à partir du haché, la fonction de hachage est dit « à brèche secrète » [15].

e. Firewall

Un pare-feu 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 échanges avec le réseau. Il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante.

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

Le système pare-feu 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 [15].

Il existe deux types de firewall [20] :

- **Le pare-feu personnels ou les Appliance de pare-feu personnel :** Le module ou Appliance de pare-feu personnel est conçu pour protéger de petits réseaux informatiques. Ils permettent, en outre, de sécuriser les postes de travail utilisés à distance via internet et un FAI (Fournisseur d'accès à Internet). Les pare-feu personnels, sauf cas particuliers, ne peuvent protéger qu'un seul système ou poste de travail, uniquement le machine sur lequel il est installé.
- **Le pare-feu intégré dans un serveur ou au système d'exploitation :** Des logiciels de pare-feu sont disponibles dans certains systèmes d'exploitation, comme linux. Ou comme éléments additionnels. Ils peuvent être utilisés pour sécuriser le serveur sur lequel il est implémenté. Les plates-formes de pare-feu doivent être mises en place sur des machines contenant un système d'exploitation prévu uniquement pour des applications de sécurité.

Un firewall offre les avantages suivants [21] :

- Identifier le type de trafic qui sera acheminé ou bloqué.
- Autoriser un administrateur à contrôler les zones aux quelles un client peut accéder sur un réseau.
- Contrôler le flux de trafic en rejetant les requêtes non autorisées.

f. Proxy

Un serveur proxy (serveur mandataire) est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local (utilisant parfois des protocoles autre que le protocole TCP /IP) et internet.

La plupart de temps, le serveur proxy est utilisé pour le web, il s'agit alors d'un proxy http. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP, etc.).

Le principe de fonctionnement d'un serveur proxy est assez simple : il s'agit d'un serveur « mandaté » par une application pour effectuer une requête sur internet à sa place. Ainsi, lorsqu'un utilisateur se connecte à l'aide d'une application cliente configurée pour utiliser un serveur proxy, celle-ci va connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur proxy va alors se connecter au serveur que l'application cliente cherche à joindre et lui transmettre la requête. Le serveur va ensuite donner sa réponse au proxy, qui va à son tour la transmettre à l'application cliente [15].

g. Zone démilitarisé

Dans le domaine des réseaux informatiques, une zone démilitarisée (DMZ, Demilitarized Zone) est un sous-réseau physique ou logique qui sépare un réseau local interne (LAN, Local Area Network) d'autres réseaux non sécurisés tels qu'Internet. Les serveurs, ressources et services extérieurs sont placés dans cette zone afin d'être accessibles depuis Internet, tandis que le reste du LAN interne n'est pas accessible. Cette configuration dote le LAN d'un niveau de sécurité supplémentaire, en empêchant les pirates d'accéder directement aux serveurs et aux données internes via Internet.

Tout service fourni aux utilisateurs sur Internet doit être placé dans la zone démilitarisée. Cela concerne notamment les services suivants : Web, messagerie, DNS, FTP et VoIP. Les systèmes sur lesquels sont exécutés ces services dans la zone démilitarisée sont accessibles par les pirates. Il est donc important de les rendre résistants à des attaques constantes [22].

h. Technologie AAA

Les différentes fonctions qui peuvent être réalisées par l'intermédiaire d'un serveur AAA sont : Authentication, Authorization et Accounting. Ceci par

l'intermédiaire de protocoles tels que RADIUS (Remote Authentication Dial In User Service) ou Diameter [23] :

- **Authentification(Authentication)**

  L'authentification a pour objectif de vérifier l'identité des processus communicants. Plusieurs solutions simples sont mises en œuvre pour cela, comme l'utilisation d'un identifiant (login) et d'un mot de passe (password). L'authentification peut s'effectuer par un numéro d'identification personnel, comme le numéro inscrit dans une carte à puce, ou code PIN (Personal Identification Number). L'authentification peut être simple ou mutuelle. Elle consiste essentiellement à comparer les données provenant de l'utilisateur qui se connecte à des informations stockées dans un site protégé. Des attaques sur les sites mémorisant les mots de passe forment une classe importante de piratage.

- **Autorisation (Authorization)**

  L'autorisation est la deuxième phase de la triade AAA. Elle agit une fois que l'utilisateur s'est authentifié. C'est dans cette phase qu'on donne ou non accès à la ressource demandée, en fonction de la politique de contrôle d'accès. Peu importe la politique utilisée, elle reste basée sur trois principes :

  - ✓ **Classification des informations :** Chaque information nécessite un certain niveau d'accès pour les consulter.
  - ✓ **Niveau d'accès des utilisateurs :** Détermine le niveau d'accès de chaque utilisateur.
  - ✓ **Permissions de l'utilisateur :** Détermine quels droits l'utilisateur aura sur les fichiers, lecture, écriture, lecture et écriture.

  Grâce à ses trois principes, une fois l'utilisateur authentifié il lui sera attribué certains droits sur certains fichiers. Bien sûr, cela peut aussi être des droits plus simples, mais pas moins importants, comme accéder au serveur mail [23].

- **Comptabilité (Accounting)**

  La dernière des trois phases de la triade AAA est désignée par le terme Accounting qui peut être traduit par traçabilité dans ce contexte. Les utilisateurs se sont authentifiés, puis ont obtenu une autorisation d'accès. Maintenant on garde une trace de toutes les actions effectuées par l'utilisateur. On dit que les actions de l'utilisateur sont archivées. Un administrateur réseaux

pourra ainsi, consulter les logs afin de vérifier les actions d'un utilisateur, ou bien retrouver l'auteur de telle ou telle action [23].

i. Système de détection d'intrusion

On appelle IDS (Intrusion Detection System) un mécanisme écoutant le trafic réseau de manière furtive afin de repérer des activités anomales ou suspectes et permettant ainsi d'avoir une action de prévention sur les risques d'intrusion.

Il existe deux grandes familles distinctes d'IDS :

- Les N-IDS (Network Based Intrusion Detection System), assurent la sécurité au niveau du réseau.
- Les H-IDS (Host Based Intrusion Detection System), ils assurent la sécurité au niveau des hôtes [15].

j. VLAN

La notion de VLAN est un concept qui permet de réaliser des réseaux de façon indépendante du système de câblage. Ces réseaux permettent de définir des domaines de diffusions restreints, cela signifie qu'un message émis par une station du VLAN ne pourra être reçu que par les stations de ce même VLAN. Un VLAN, est donc, un regroupement logique, et non physique, de plusieurs stations. Pour réaliser ce regroupement, on intervient directement, par voie logicielle, sur le ou les éléments actifs que sont les commutateurs VLAN [24].

k. VPN

Auparavant pour interconnecter deux LAN distants, il n'y avait que deux solutions, soit les deux sites distants étaient reliés par une ligne spécialisée permettant de réaliser un WAN entre les deux sites soient les deux réseaux communiquaient par le RTC.

Une des premières applications des VPN est de permettre à un hôte distant d'accéder à l'intranet de son entreprise ou à celui d'un client grâce à Internet tout en garantissant la sécurité des échanges. Il utilise la connexion avec son fournisseur d'accès pour se connecter à Internet et grâce aux VPN, il crée un réseau privé virtuel entre l'appelant et le serveur de VPN de l'entreprise [25].

7. Conclusion

Dans ce chapitre, nous avons présenté quelques principes de la sécurité informatiques, ses objectifs et attaques courantes, puis nous avons examiné les mécanismes fondamentaux de la sécurité mis en œuvre dans les réseaux, et plus particulièrement les VLAN et les VPN.

Dans le chapitre suivant, nous allons approfondir les réseaux locaux virtuels VLAN et les réseaux privés virtuels VPN.

Chapitre III : *Réseaux locaux virtuels et Réseaux privés virtuels*

1. Introduction

Les réseaux locaux virtuels (VLAN) sont apparus comme une nouvelle fonctionnalité dans l'administration réseau. Ils ont pour objectif de rassembler des machines dispersées géographiquement dans un réseau pour leur permettre de communiquer comme si elles étaient dans un même réseau local.

Les réseaux privés virtuels (VPN) est une technique permettant à un ou plusieurs postes distants de communiquer de manière sure, tout en empruntant les infrastructures publiques. Ce type de liaison est apparu suite à un besoin croissant des entreprises de relier les différents sites de façon sécurisée.

Dans ce chapitre, nous allons présenter les principales notions d'un réseau local virtuel, ces protocoles de transport (la norme 802.1Q, protocole ISL) et ces protocoles d'administration et de gestion des VLAN (VTP, DHCP et ACL). Par la suite, nous allons présenter quelques notions sur les réseaux privés virtuels.

2. Les réseaux locaux virtuels

2.1 Définition des VLAN

Les VLAN (Virtual Local Area Network) définis par les standards IEEE 802.1q (pour la notion de VLAN) et 802.1.p (pour la qualité de service QoS (Quality of Service)) permettent de regrouper des machines sans avoir à tenir compte de leur emplacement sur le réseau. Les messages émis par une station d'un VLAN ne sont reçus que par les autres stations de ce même VLAN. Les machines physiquement connectées au réseau mais qui n'appartiennent pas au VLAN, ne reçoivent pas les messages. La division du réseau local est alors une division logique et non physique et les stations d'un même domaine de diffusion ne sont pas obligées d'être sur le même segment LAN [26].

2.2 Les différents niveaux de VLAN

Les échanges à l'intérieur d'un domaine sont sécurisées et les communications inter-domaines sont autorisées et peuvent être contrôlées par les filtres configurés dans le routeur. L'appartenance à un VLAN étant définie logiquement et non géographiquement, les VLAN permettent d'assurer la mobilité (déplacement) des postes de travail. Selon le regroupement effectué, on distingue [27] :

2.2.1 VLAN par ports

Les VLAN de niveau 1 ou VLAN par port (Port-based VLAN) comme illustré dans la figure III.1, associent chaque port d'un commutateur à un VLAN. Une station raccordée à 1 port est automatiquement affectée au VLAN du port. Si le port est raccordé à un hub, toutes les stations de ce hub appartiennent au même VLAN (VLAN par segment). La configuration est statique (VLAN statique), le déplacement d'une station implique son changement de VLAN. C'est le mode le plus sécurisé.

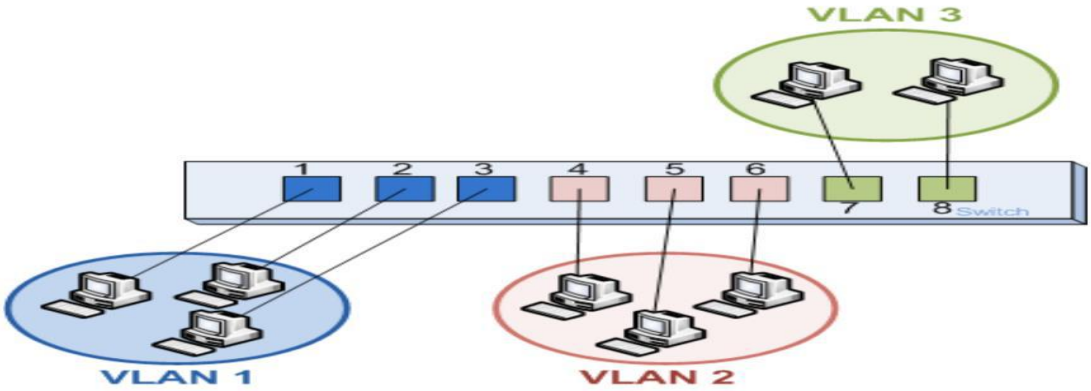

Figure III.1 : VLANs par port [28].

2.2.2 VLAN par adresses MAC

Les VLAN de niveau 2 ou VLAN MAC (MAC Address-based VLAN) : Les stations appartenant au VLAN sont associées par leur adresse MAC (voir figure III.2), selon des tables d'adresses introduites par l'administrateur. Les stations peuvent se trouver dans des lieux géographiquement différents. La ou les stations sur un même port peuvent donc être simultanément reliées à des VLAN différents. Ce type de VLAN évite d'avoir à configurer les commutateurs lorsqu'un utilisateur est déplacé. On comprend donc la nécessité d'échanger les tables d'adresses MAC entre commutateurs, ce qui malheureusement engendre un encombrement supplémentaire du réseau. Ces VLAN sont très utilisés pour les protocoles non routables.

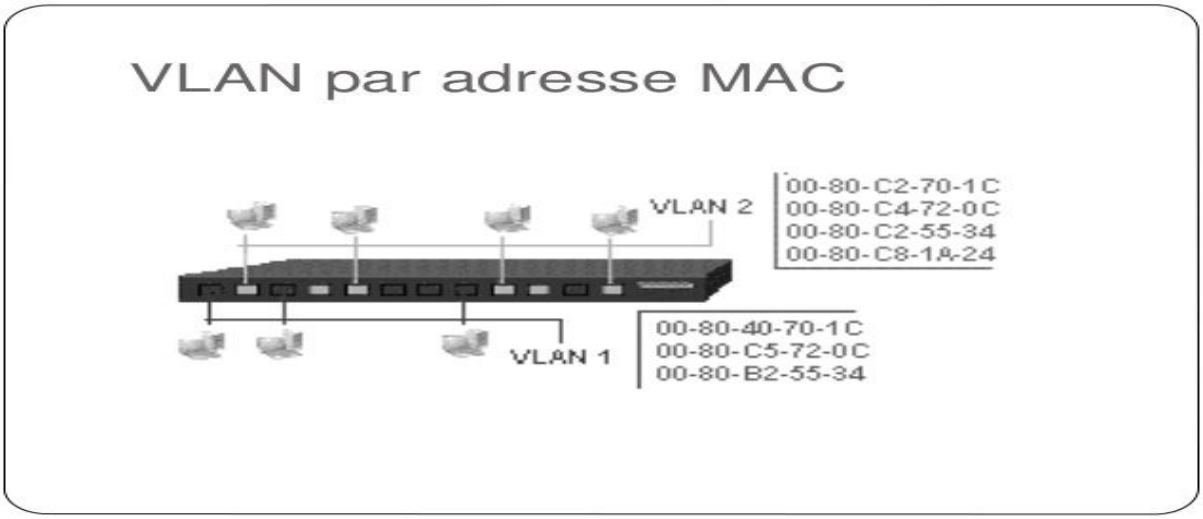

Figure III.2 : VLANs par adresse MAC [29].

2.2.3 VLAN d'adresses réseaux

Les VLAN de niveau 3 ou VLAN d'adresses réseaux (Network Address-based VLAN) comme illustré dans la figure III.3, sont constitués de stations définies par leur adresse réseau (plage d'adresses) ou par masque de sous-réseau (Subnet d'IP). Les utilisateurs d'un VLAN de niveau 3 sont affectés dynamiquement à un VLAN. Une station peut appartenir à plusieurs VLAN par affectation statique. Ce mode de fonctionnement est le moins performant, le commutateur devant accéder à l'adresse de niveau 3 pour définir le VLAN d'appartenance. L'adresse de niveau 3 est utilisée comme étiquette, il s'agit bien de commutation et non de routage. L'en-tête n'est pas modifié.

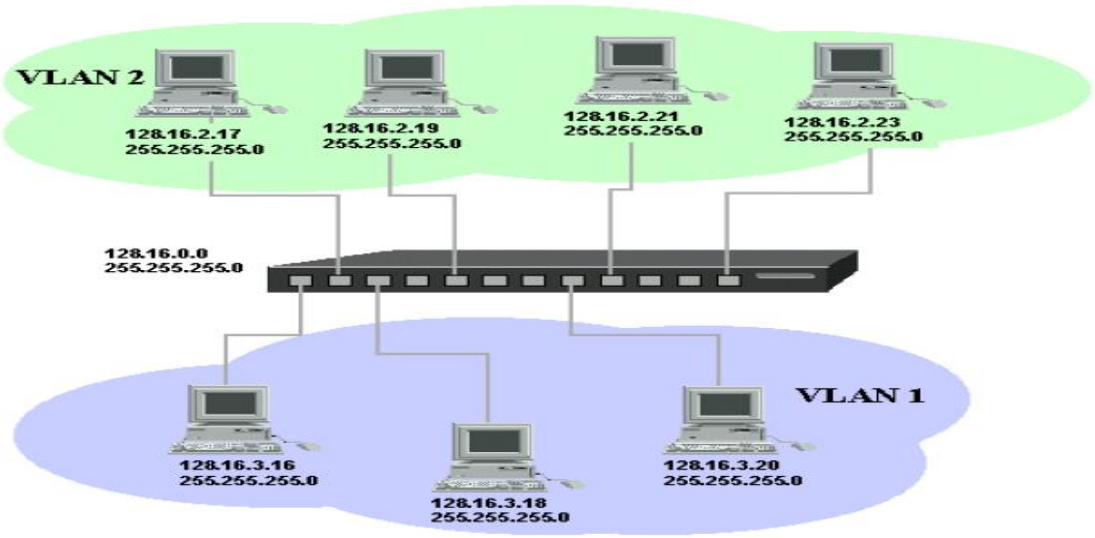

Figure III.3 : VLANs par adresses réseaux [30].

Il est aussi envisageable de réaliser des VLAN par :

- Protocole (IP, IPX...), la communication ne pouvant s'établir qu'entre stations utilisant le même protocole.
- Par application (N◦ de port TCP), la constitution des VLAN est alors dynamique, un utilisateur pouvant successivement appartenir à des VLAN différents selon l'application qu'il utilise.
- Par mot de passe (constitution dynamique des VLAN au login de l'utilisateur).

2.3 Avantages des VLAN

Parmi les avantages liés à la mise en œuvre d'un VLAN, on retiendra notamment [31] :

- **Flexibilité de segmentation du réseau :** Les utilisateurs et les ressources entre lesquels les communications sont fréquentes peuvent être regroupés sans devoir prendre en considération leur localisation physique. Il est aussi envisageable qu'une station appartienne à plusieurs VLAN en même temps.
- **Simplification de la gestion :** L'ajout de nouveaux éléments ou le déplacement d'éléments existants peut être réalisé rapidement et simplement.
- **Augmentation considérable des performances du réseau :** Comme le trafic réseau d'un groupe d'utilisateurs est confiné au sein du VLAN qui lui est associé, de la bande passante est libérée, ce qui augmente les performances du réseau.
- **Meilleure utilisation des serveurs réseaux :** Lorsqu'un serveur possède une interface réseau compatible avec le VLAN, l'administrateur a l'opportunité de faire appartenir ce serveur à plusieurs VLAN en même temps. Cette appartenance à de multiples VLAN permet de réduire le trafic qui doit être routé (traité au niveau du protocole de niveau supérieur, par exemple IP) "de" et "vers" ce serveur, et donc d'optimiser ce trafic. Le VLAN améliore considérablement l'utilisation du réseau.
- **Renforcement de la sécurité du réseau :** Les frontières virtuelles créées par les VLAN ne pouvant être franchies que par le biais de fonctionnalités de routage, la sécurité des communications est renforcée.

2.4 Trunk de VLAN

Un trunk est un lien entre deux équipements, configuré de telle sorte que l'on peut y faire circuler des trames comportant des informations relatives au VLAN sur lequel elles transitent. On peut placer un trunk entre deux commutateurs, entre un commutateur et un hôte

supportant le trunking et entre un commutateur et un routeur pour effectuer un routage inter-VLAN [32].

2.5 Protocoles de transport des VLANs

Dans ce qui suit, nous allons présenter deux protocoles de transports utilisés par des VLANs [33] :

2.5.1 La norme IEEE 802.1Q

La norme IEEE 802.1Q est utilisée pour étendre la portée des VLANs sur plusieurs switchs. 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 comme illustré dans la figure III.4, on parle alors de VLANs « 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 faut noter que seuls les switchs ajoutent et enlèvent les « tags » dans les trames. Les machines n'ont donc pas à gérer le marquage qui leur est inconnu.

- **Trois types de trames sont définis :**

  1. Les trames non étiquetées (untagged frame) ne contiennent aucune information sur leur appartenance à un VLAN.

  2. Les trames étiquetées (tagged frame) possèdent un marqueur qui précise à quel VLAN elles appartiennent.

  3. Les trames étiquetées avec priorité (priority-tagged frame) sont des trames qui possèdent en plus un niveau de priorité défini selon la norme IEEE 802.1P.

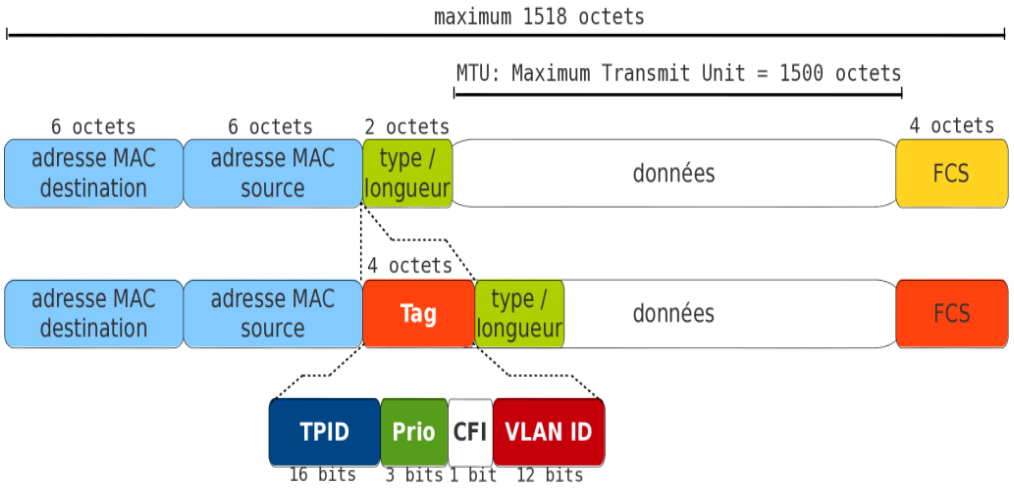

Figure III.4 : Format de la trame IEEE 802.1Q [33].

Le champ **TPID** (Tag Protocol Identifier**)** à une valeur fixe 0x8100 (en notation hexadécimale) qui identifie une trame de type 802.1Q.

Le champ **TCI** (Tag Control Information) est constitué de trois parties :

1. Le champ **Priority** indique le niveau de priorité de la trame et est utilisé lorsque que le champ VID est nul.
2. Le champ **CFI** (Canonical Format Identifier) indique que le format est standard (Ethernet) ou non.
3. Le champ **VID** (VLAN Identifier) contient l'identifiant du VLAN auquel appartient la trame.

Les VLANs peuvent être déclarés manuellement ou dynamiquement. Dans la déclaration dynamique, l'administrateur définit les VLANs sur un switch et un seul. Le protocole MVRP (Multiple VLAN Registration Protocol) permet la diffusion de ces informations aux autres switchs du réseau.

2.5.2 Le 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.

2.6 Quelques protocoles d'administration et de gestion des VLAN

2.6.1 Le protocole VTP (VLAN Trunking Protocol)

Le protocole VTP (VLAN Trunking Protocol) a été créé par CISCO pour résoudre des problèmes opérationnels dans des réseaux commutés contenant des VLAN. C'est un protocole propriétaire CISCO. 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 [34].

Un commutateur doit alors être déclarés en 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 crées sur le commutateur serveur.

Pour créer une interface VLAN, il faut entrer dans la base de données des VLANs avec la commande vlan data base :

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

Les dispositifs de VTP peuvent être configurés pour fonctionner suivant les trois modes suivants [34] :

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 modifiable.

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.

2.6.2 Protocole DHCP

DHCP signifie Dynamic Host Configuration Protocol. S'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau local d'obtenir dynamiquement (c'est-à-dire sans intervention particulière) sa configuration (principalement, sa configuration réseau).

Vous n'avez qu'à spécifier à l'ordinateur de se trouver une adresse IP tout seul par DHCP. Le but principal étant la simplification de l'administration d'un réseau.

Le protocole DHCP sert principalement à distribuer des adresses IP sur un réseau, 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 (BOOTP est utilisé en étroite collaboration avec un serveur TFTP sur lequel le client va trouver les fichiers à charger et à copier sur le disque dur). Un serveur DHCP peut renvoyer des paramètres BOOTP (Bootstrap Protocol) ou de configuration propres à un hôte donné [35].

2.6.3 Protocole Spanning-Tree

Le protocole Spanning-Tree (STP) est un protocole de couche 2 (liaison de données) conçu pour les switchs et les bridges. La spécification de STP est définie dans le document IEEE 802.1d. Sa principale fonction est de s'assurer qu'il n'y a pas de boucles dans un contexte de liaisons redondantes entre des matériels de couche 2. STP détecte et désactive des boucles de réseau et fournit un mécanisme de liens de backup. Il permet de faire en sorte que des matériels compatibles avec le standard ne fournissent qu'un seul chemin entre deux stations d'extrémité [36].

2.6.4 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 [37].

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.
- 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 que voici :

- **Listes de contrôle d'accès standard :** Les listes d'accès standard vérifient l'adresse d'origine des paquets IP qui sont routés. Selon le résultat de la comparaison, l'acheminement est autorisé ou refusé pour un ensemble de protocoles complet en fonction des adresses réseau, de sous-réseau et d'hôte.
- **Listes de contrôle d'accès étendues :** Les listes d'accès étendues sont utilisées plus souvent que les listes d'accès standard car elles fournissent une plus grande gamme de contrôle. Les listes d'accès étendues vérifient les adresses d'origine et de destination du paquet, mais peuvent aussi vérifier les protocoles et les numéros de port. Cela donne une plus grande souplesse pour décrire ce que vérifie la liste de contrôle d'accès. L'accès d'un paquet peut être autorisé ou refusé selon son emplacement d'origine et sa destination, mais aussi selon son type de protocole et les adresses de ses ports.
- **Listes de contrôle d'accès nommées :** Les listes de contrôle d'accès nommées IP ont été introduites dans la plate-forme logicielle CISCO IOS version 11.2, afin d'attribuer des noms aux listes d'accès standard et étendues à la place des numéros.

3. Réseau privé virtuel

3.1 Définition

Un réseau privé virtuel VPN est un réseau qui permet d'utiliser internet comme support pour étendre un réseau local. Les informations circulent d'un point à un autre du réseau par un tunnel VPN. Elles sont cryptées avec des protocoles sécurisés. Cette technologie dispense d'avoir recours à de coûteuses solutions de location de connexions privées et spécifiques [38].

Le but d'un réseau privé virtuel est de fournir aux utilisateurs et administrateurs du système d'information des conditions d'exploitation, d'utilisation et de sécurité à travers un réseau public identiques à celles disponibles sur un réseau privée. En d'autre termes, on veut regrouper des réseaux privés, séparés par un réseau public (internet) en donnant l'illusion pour l'utilisateur qu'ils ne sont pas séparés, et tout en gardant l'aspect sécurisé qui était assuré par la coupure logique au réseau internet [39].

3.2 Fonctionnement d'un VPN

Un réseau VPN repose sur un protocole appelé « protocole de tunneling ». Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à

l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu couteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée comme internet.

Les données à transmettre peuvent être prises en charge par un protocole différent d'IP. Dans ce cas, le protocole de tunneling encapsule les données en ajoutant un entête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation [40].

3.2.1 Contraintes d'un VPN

Le principe d'un VPN est d'être transparent pour les utilisateurs et pour les applications y ayant accès. Il doit être capable de mettre en œuvre les fonctionnalités suivantes :

- **Authentification d'utilisateur :** seuls les utilisateurs autorisés doivent avoir accès au canal VPN.
- **Cryptage des données :** lors de leur transport sur Internet, les données doivent être protégées par un cryptage efficace.
- **Gestion de clés :** les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées (pertes, vols, licenciement).
- **Prise en charge multi protocoles :** la solution VPN doit supporter les protocoles les plus utilisés sur Internet [41].

3.3 Types des VPN

Suivant les besoins, trois types de VPN sont distingués [41] :

3.3.1 Le VPN d'accès : Il est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau de leur entreprise. L'utilisateur se sert d'une connexion Internet afin d'établir une liaison sécurisée. La figure III.5 schématise un VPN d'accès.

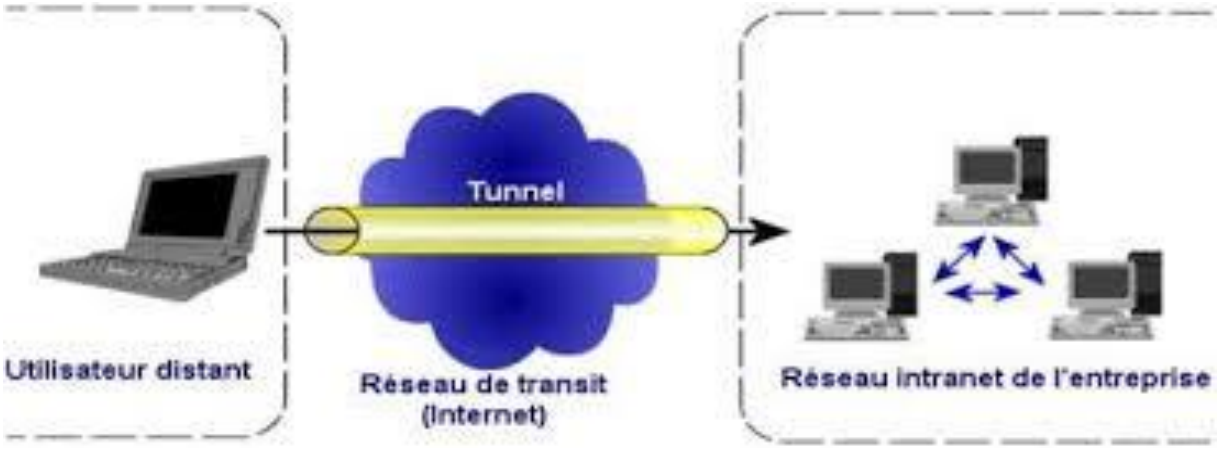

Figure III.5 : VPN d'accès [41].

3.3.2 L'intranet VPN : Il est utilisé pour relier deux ou plusieurs intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Ce type est également utilisé pour relier des réseaux d'entreprise, sans qu'il soit question d'intranet (partage de données, de ressources, exploitation de serveurs distants ...). La figure III.6 schématise l'intranet VPN. La figure III.6 schématise l'intranet VPN.

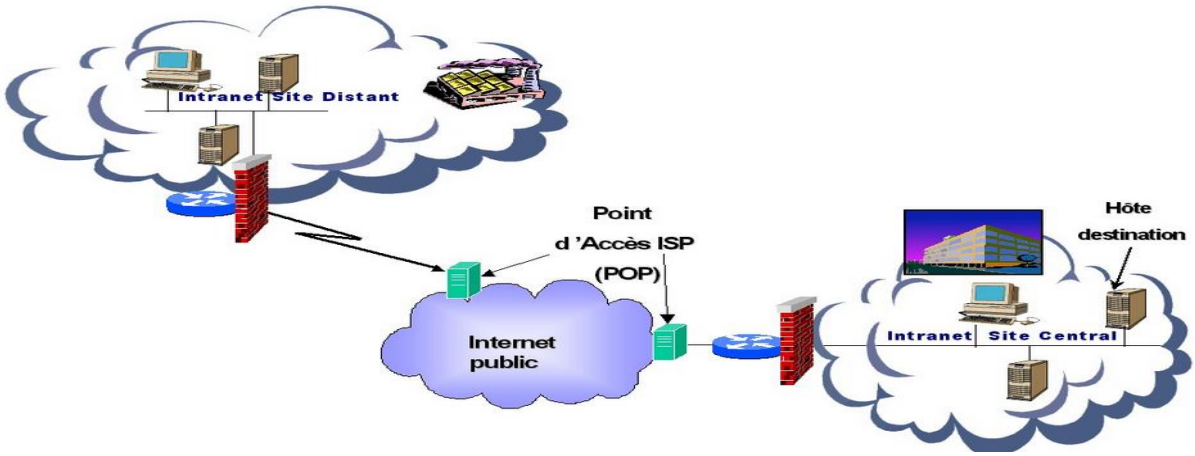

Figure III.6 : L'intranet VPN [42].

3.3.3 L'extranet VPN : Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers et il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès. Souvent, seule une partie des ressources est partagée, ce qui nécessite une gestion rigoureuse des espaces d'échange. La figure III.7 schématise l'extranet VPN.

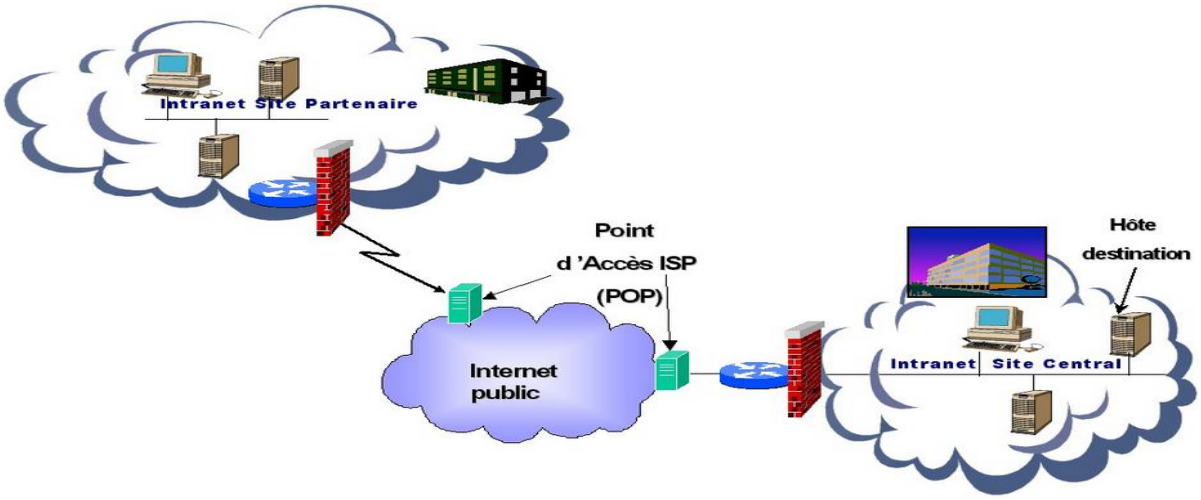

Figure III.7 : L'extranet VPN [42].

3.4 L'intérêt d'un VPN

La mise en place d'un VPN permet de connecter de façon sécurisée des ordinateurs distants au travers d'une liaison non fiable (Internet), comme s'ils étaient sur le même réseau local. Ce procédé est utilisé par de nombreuses entreprises afin de permettre à leurs utilisateurs de se connecter au réseau d'entreprise hors de leur lieu de travail. Les réseaux privés virtuels procurent les avantages ci-dessous [43] :

- Les connexions VPN offrent un accès au réseau local à distance et de façon sécurisée.
- Elles permettent d'administrer efficacement et de manière sécurisée un réseau local à partir d'une machine distante.
- Elles permettent aux utilisateurs qui travaillent à domicile ou depuis d'autres sites distants d'accéder à distance à un serveur d'entreprise par l'intermédiaire d'une infrastructure de réseau public, telle qu'Internet.
- Elles permettent également aux entreprises de disposer de connexions routées partagées avec d'autres entreprises sur un réseau public, tel qu'Internet, et de continuer à disposer de communications sécurisées, pour relier, par exemple des bureaux éloignés géographiquement.
- Elle est routée via Internet et fonctionne logiquement comme une liaison de réseau étendu (WAN) dédiée.
- Les connexions VPN permettent de partager des fichiers et programmes de manière sécurisée entre une machine locale et une machine distante.

3.5 Principaux protocoles utilisés dans les VPNs

Les principaux protocoles de tunneling de ce niveau sont les suivants :

3.5.1 PPP (Point to Point Protocol)

Est un protocole qui permet de transférer 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 des trames PPP, puis transmet ces paquets encapsulés au travers de la liaison point à point. PPP est employé généralement entre un client d'accès à distance et un serveur d'accès réseau. Le protocole PPP est défini dans la RFC 2153 [44].

PPP est le fondement des protocoles PPTP et L2TP utilisés dans les connexions VPN sécurisées.

PPP est la principale norme de la plupart des logiciels d'accès distant. La figure III.8 représente le format d'une trame PPP [45].

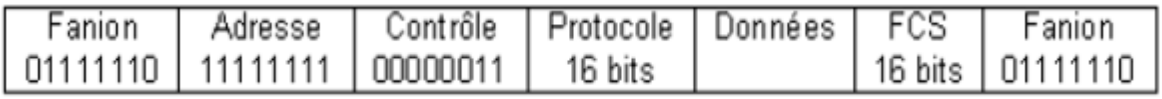

Figure III.8 : Format d'une trame PPP [45].

3.5.2 PPTP (Point to Point Tunneling Protocol)

Le principe du protocole PPTP est de créer des paquets et de les encapsuler dans des datagrammes IP [41].

Le tunnel PPTP se caractérise par :

- Une initialisation du client.
- Une connexion de contrôle entre le client et le serveur.
- La clôture du tunnel par le serveur.

Par la suite, une deuxième connexion est établie. Elle permet d'encapsuler les paquets PPP dans des datagrammes IP. C'est cette deuxième connexion qui forme le tunnel PPTP. La figure III.9 schématise les étapes de tunneling PPTP.

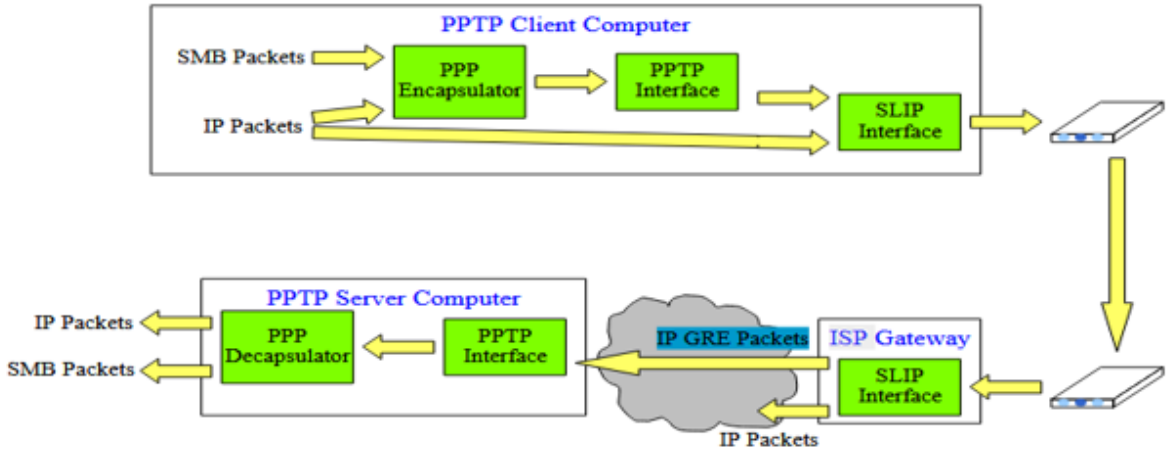

Figure III.9 : Exemple de tunneling PPTP [41].

3.5.3 L2F (Layer 2 Fprwarding)

Cisco a développé ce protocole autour des années 1996. L'IETF a en fait un standard en 1998 avec le RFC 2341 [46]. Son fonctionnement est assez voisin de PPTP [47].

3.5.4 L2TP (Layer Two Tunneling Protocol)

L2TP, défini par la RFC 2661 [48], est issu de la convergence des protocoles PPTP et L2F (Layer Two Forwarding).

Il est actuellement développé et évalué conjointement par Cisco, Microsoft, 3Com ainsi que d'autres acteurs du marché des réseaux.

L2TP encapsule une liaison de couche 2 (liaison de données) sur un lien réseau (couche 3), ce qui permet à un PC distant d'avoir accès au réseau de son entreprise comme s'il était connecté au réseau local, et ainsi d'avoir accès aux serveurs de fichiers, aux imprimantes, etc. Lorsqu'il est configuré pour transporter les données sur IP, L2TP peut être utilisé pour faire du tunneling sur Internet [49].

3.5.5 MPLS (MultiProtocole Label Switching)

Est souvent considéré comme situé dans un niveau intermédiaire entre le niveau 2 et le niveau 3. C'est pourquoi en lui affecter un niveau hybride 2.5 qui n'existe pas dans les couches OSI traditionnellement, Est un protocole qui permet d'établir un tunnel privé au sein d'un réseau public, il est surtout utilisé par les fournisseurs d'accès à l'Internet pour proposer à leurs clients un moyen de créer un réseau privé entre plusieurs sites d'une même entreprise [49].

3.5.6 IPSec

Ce protocole très populaire est un les plus robustes et des plus versatiles mais il est aussi un des plus complexes**.**

Désigne un ensemble de RFC destinées à incorporer les techniques de chiffrement (et d'autres, relatives aussi à la sécurité) au protocole IP lui-même, plutôt que d'avoir recours à des solutions externes. IPv6 a été conçu pour comporter d'emblée toutes les spécifications IPSec [49].

IPSec comporte essentiellement deux protocoles :

- Le protocole AH (Authentification Header) assure l'authenticité et l'intégrité des données acheminées, c'est un protocole réseau, de couche 3 donc, que l'on peut voir comme une option d'IP.
- Le protocole de transport ESP (couche 4) (Encapsulating Security Payload) assure la confidentialité et l'intégrité des données, leur authenticité étant assurée de façon optionnelle.

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.
- En mode transport un en-tête IPSec est intercalé entre l'en-tête IP d'origine et les données du paquet IP. La figure 6 illustre ces différentes possibilités.

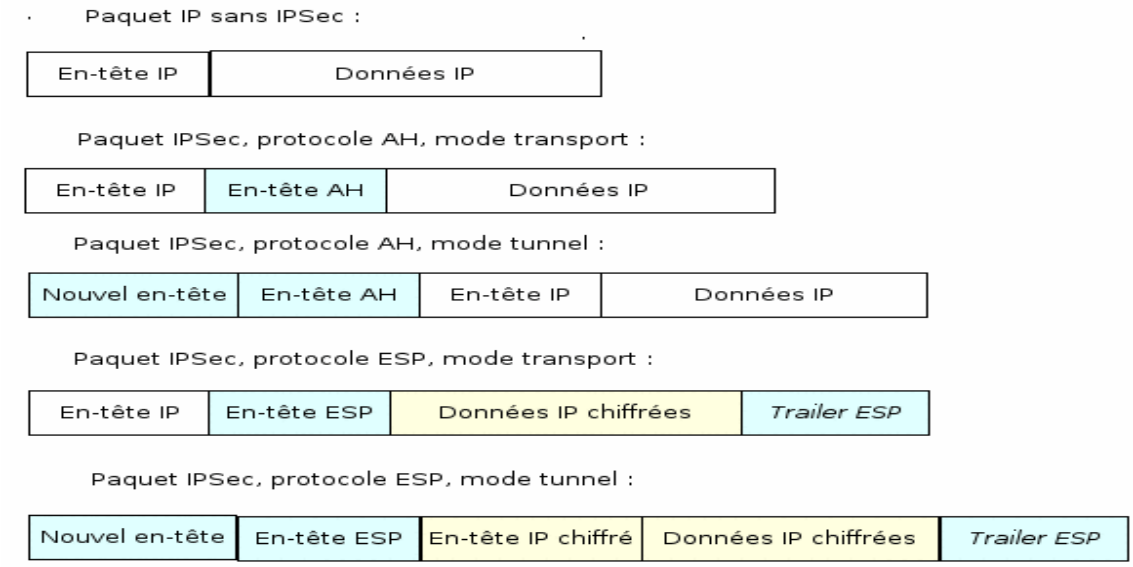

Figure III.10 : Protocoles et modes IP Sec [49].

IPSec n'est pas un remplaçant d'IP mais un complément. Ainsi, il intègre des notions essentielles de sécurité au datagramme IP qui en assureront l'authenticité l'authentification et le cryptage. Pour cela, il fait largement usage de clé de sessions.

Sa position dans les couches basse du modèle OSI lui permet donc de sécuriser tous type d'applications et protocoles réseaux basée sur IP sans distinction. IPSec est très largement utilisé pour le déploiement de réseau VPN à travers Internet à petite et grande échelle. La figure III.12 illustre le positionnement du protocole IPSec dans la pile IP.

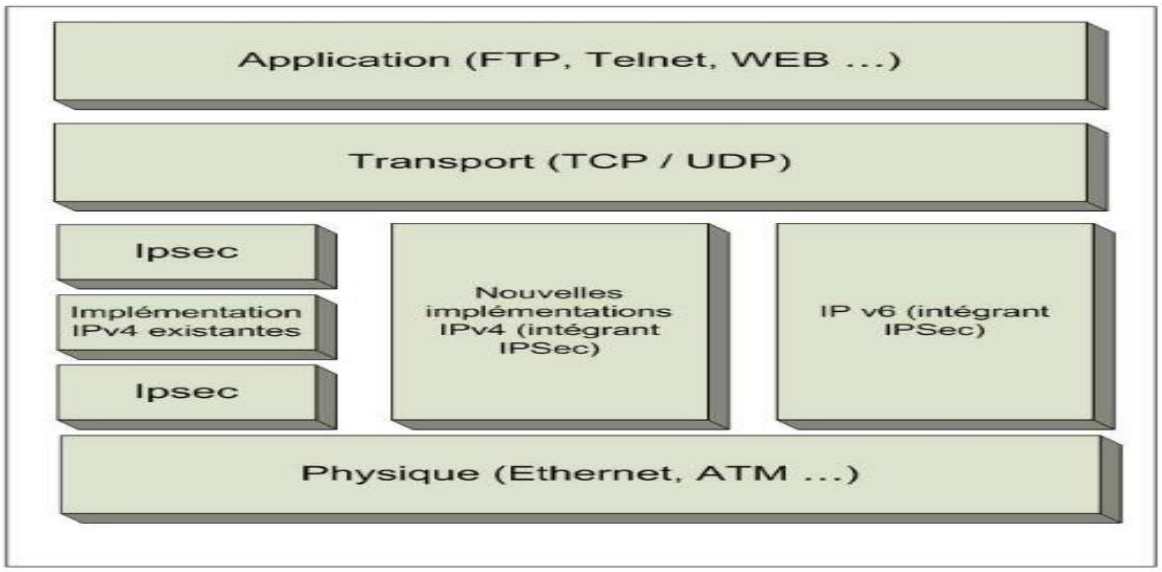

Figure III.11 : Positionnement du protocole IPSec dans la pile IP [49].

3.5.7 SSL/TLS (Secure Socket Layer) / (Transport Layer Security)

Ces protocoles sont en plein essor car très simple de mise en œuvre et utiliser un port banal (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 par exemple) [47].

3.5.8 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. Pour l'anecdote nous pouvons par exemple noter que les férus d'échanges illégaux de fichiers musicaux et vidéos en ont bien compris l'intérêt puisque certaines des techniques suggérées pour contourner les lois font appel à lui [47].

4. Conclusion

Au cours de ce chapitre, nous avons pu aborder en détail les solutions de la sécurité proposées à savoir les VLAN et VPN, ainsi que ses principaux concepts tels que la limitation des domaines de diffusions, la mobilité des utilisateurs et sans oublier le point important de notre objectif qu'est la sécurité.

Le prochain chapitre va être consacré au côté pratique de la réalisation de notre travail.

Chapitre IV *: Présentation de l'organisme d'accueil et la réalisation*

1. Introduction

Dans ce chapitre, nous avons deux parties essentielles. La première consiste à présenter l'organisme d'accueil (l'entreprise SCS (Soummam Computer System)) et la deuxième partie, sera consacré à la mise en œuvre de la solution proposée pour la réalisation, pour ce faire, nous commencerons par la présentation du simulateur utilisé, au départ nous allons décider de configurer le protocole VTP pour simplifier la mise en place des VLAN dans tous les commutateurs et prévoir une gestion plus rapide en cas d'évolution du nombre de ces VLAN.

Par la suite nous allons configurer le protocole DHCP qui permet l'attribution des adresses IP de manière automatique. Pour permettre la communication entre tous les services, il est essentiel de mettre en place le routage inter-VLAN, mais afin de réaliser le filtrage des accès, il sera nécessaire de configurer des listes de contrôle d'accès associée aux interfaces virtuelles du routeur de l'entreprise.

En deuxième étapes, nous avons besoin aussi de configurer toutes les liaisons entre les divers sites de l'entreprise, alors nous entamerons la configuration VPN avec des tests qui démontreront le bon fonctionnement de réseau.

2. Présentation de l'organisme d'accueil

2.1 Présentation générale

SOUMMAM COMPUTER SYSTEM (SCS) est l'une des premières entreprises spécialisées de la fourniture et la maintenance des équipements et réseaux informatiques afin de répondre à une démarche accrue du marché de l'informatique en Algérie. Depuis, la société s'est spécialisés dans l'importation, la distribution et la vente des produits informatiques, bureautiques et multimédias. Elle est aujourd'hui un acteur majeur de la commercialisation et de la distribution informatique en Algérie. Elle répond à l'ensemble des besoins des entreprises et des particuliers en matière d'importation, de distribution et de vente des produits informatiques, bureautiques et multimédias. Grace à son sérieux, son dynamisme, la qualité de ses prestations et de ses produits, elle est devenue aujourd'hui un acteur incontournable dans ce secteur.

2.2 Organigramme général de Soummam Computer System (SCS)

Voici le schéma général du groupe SCS dont chaque direction a pour but d'assurer le bon fonctionnement de chaque partie du groupe comme le montre la figure IV.1 :

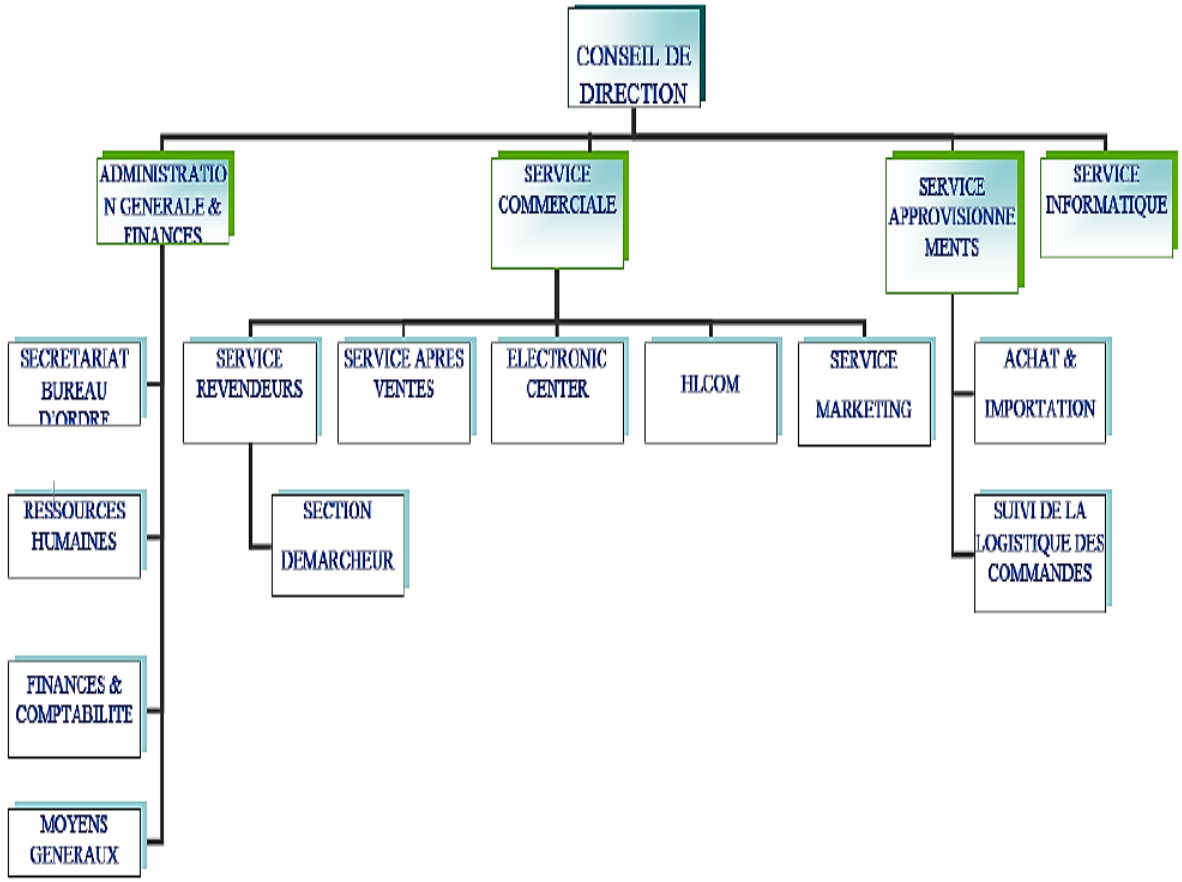

Figure IV.1 Organigramme de SCS.

2.3 Structure hiérarchique du groupe

Un label qui ne cesse d'accaparer des parts dans un marché caractérisé par une rude SCS dispose de ses propres moyens logistiques, de ses propres showrooms répartis sur tous les grands centres urbains et fait du rapprochement du service après-vente du client final une priorité.

2.4 Situation géographique

Soummam Computer System, dans le souci d'accomplir sa mission, dispose de plusieurs localités :

- Un centre de distribution en gros dans la zone industrielle de quatre chemins, le personnel technique est chargé des différentes opérations de maintenance en informatique, électronique et bureautique.
- L'électronique centre, centre commercial sur trois niveaux à Sidi Ahmed.
- Service après-vente situé à Ihaddaden.
- SCS Mobiliers Shows room et vente de divers mobiliers situé à proximité du siège social à Sidi Ahmed, le showroom permet à la clientèle une approche de diverses gammes de produits de mobiliers domestique et équipement de bureau.
- Centre Maxi Power Showroom à Quartier Sghir.

  Hormis la wilaya de Bejaia, SCS s'est répartis sur plusieurs endroits sur le territoire Algérien tels que : Alger et Oran.
- Atelier de maintenance qui assure à leur clientèle un service après-vente de qualité, situé à rue Saint Charles KOUBA, Alger.

2.5 L'informatique dans SCS

Le service informatique est subdivisé en deux sous service dont le service réseau et le service marketing.

Le service réseau est composé de quatre administrateurs réseau parmi lesquels on dispose d'un chef de service, ils sont chargés de :

- Installer et maintenir les équipements réseaux.
- Administrer les différents serveurs (domaine, base de données, partage, proxy).

2.6 Organigramme de la direction système d'informatique

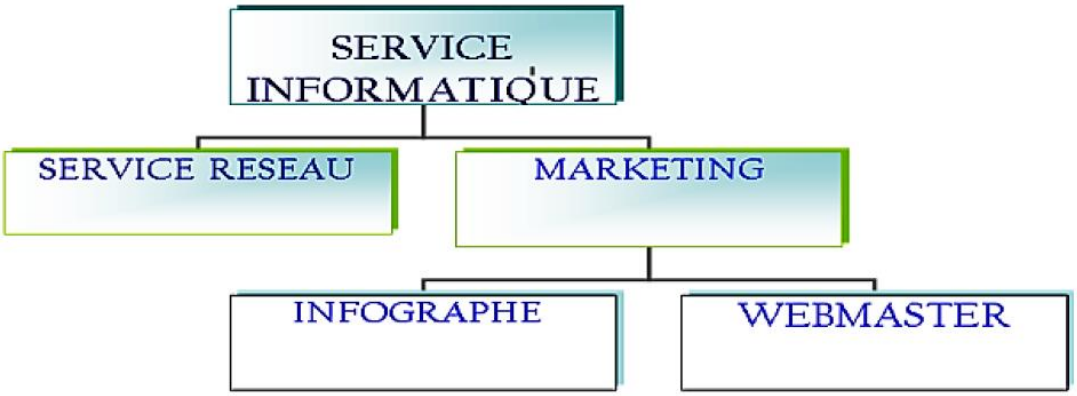

Figure IV.2 Organigramme du service d'accueil.

Le service informatique est subdivisé en deux sous service dont le service réseau et le service marketing.

Le service réseau est composé de quatre administrateurs réseau parmi lesquels on dispose d'un chef de service, ils sont chargés de :

- Installer et maintenir les équipements réseaux.
- Administrer les différents serveurs (domaine, base de données, partage, proxy).

Quant au service marketing, il est constitué d'un infographe qui est en étroite collaboration avec le service commerciale afin de réaliser les publicités sur les produits, et d'un webmaster qui s'occupe de la conception et de la mise à jour des pages web de l'entreprise. Tous deux sont sous la directive d'un chef de service.

3. Architecture de réseau SCS

La figure IV.3 illustre l'architecture générale du réseau actuelle de l'entreprise SCS

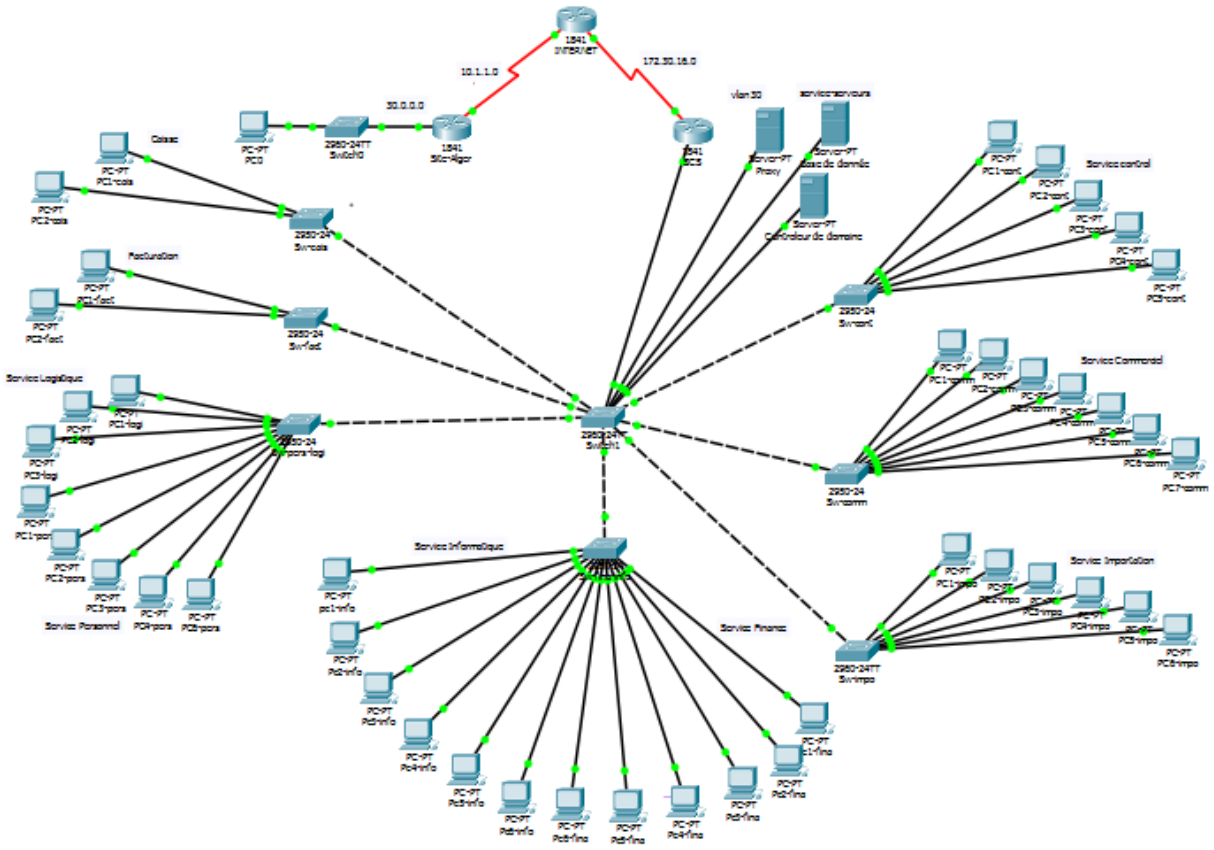

Figure IV.3 : Architecture de réseau actuelle « SCS ».

4. Problématique

L'Enterprise comme elle a été décrite par l'architecture générale de réseau de SCS, dispose de quatre sites distants, l'un se situe à Béjaïa, les deux autres à Alger et le quatrième à Oran. Ce qui est demandé est de pouvoir connecter tous les sites avec des liaisons virtuelles sécurisées.

Sur le site de Béjaïa (le cas de notre étude), où la présence de plusieurs services dans l'entreprise impose le besoin d'implémenter un moyen de segmentation du réseau afin de résoudre tous les problèmes rencontrés à savoir :

- L'absence d'un système de gestion centralisée des utilisateurs.
- L'absence d'une segmentation du réseau en vlan ou en sous-réseau.
- L'adressage se fait manuellement.
- La surcharge de la bande passante.
- La difficulté de sécuriser les communications entre les différents services.
- La difficulté de sécuriser les lignes de communication entre les différents sites distants.

5. Solutions proposées

Dans le milieu professionnel, il est toujours important de définir des techniques de sécurité sur le réseau et au regard de tous ces problèmes, nous avons suggéré des concepts et des solutions durant notre stage qui pouvant renforcer la sécurité du leur système. C'est ainsi qu'il nous a été empêché à réfléchir sur la solution des VLANs et VPNs.

La solution VLAN est la première étape du processus d'amélioration des performances du réseau contre les surcharges rencontrées, et en deuxième étape nous avons proposé la solution VPN pour la sécurité des échanges entre les divers sites de l'entreprise.

6. Objectifs attendus

Les fonctions à satisfaire sont les suivants:

- Mise en place de Vlan et d'un Switch fédérateur avec fonction DHCP.
- Améliorer le trafic sur le réseau.

7. Présentation de simulateur Cisco Packet Tracer

Packet Tracer comme illustré dans la figure IV.4 est un logiciel de CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux

sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs.

Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc

Cisco Packet Tracer est un moyen d'apprentissage et de la réalisation de divers réseaux et découvrir le fonctionnement des différents éléments constituant un réseau informatique.

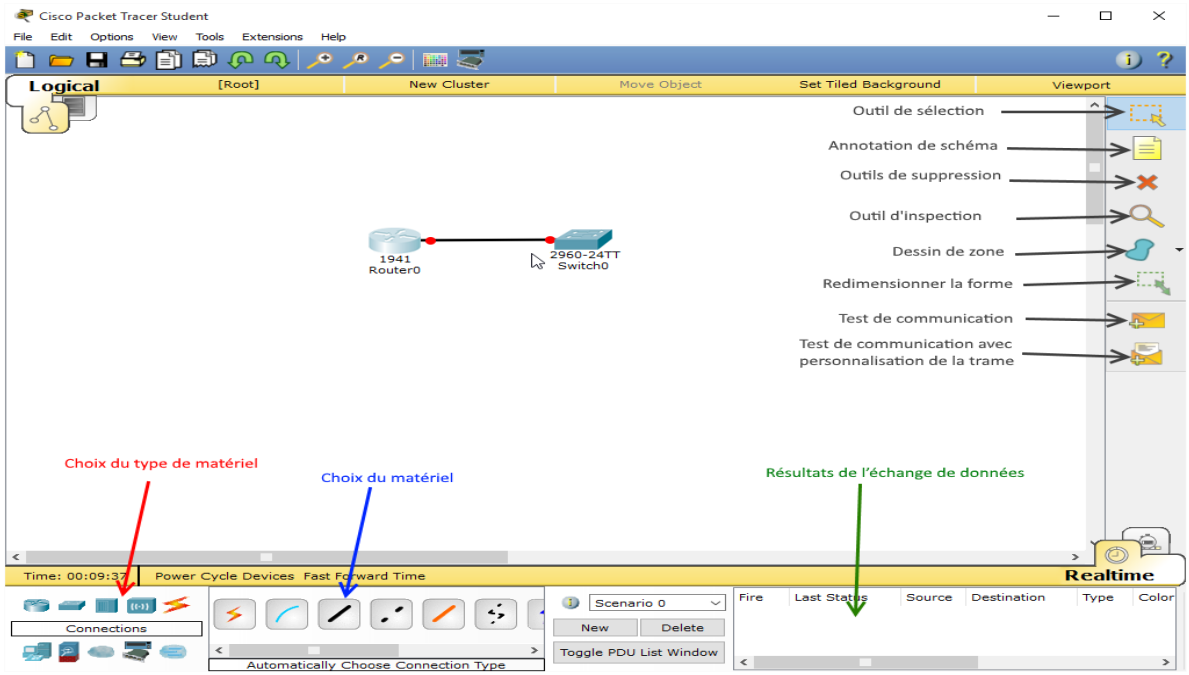

Figure IV.4: Interface Cisco Packet Tracer.

8. Outils de configuration des équipements

Interface de ligne de commande CLI (Command Line Interface) illustrée dans la figure IV.5 est l'interface utilisateur principale utilisée pour la configuration, la surveillance et la maintenance des périphériques Cisco. Cette interface utilisateur nous permet directement et simplement d'exécuter des commandes de Cisco IOS.

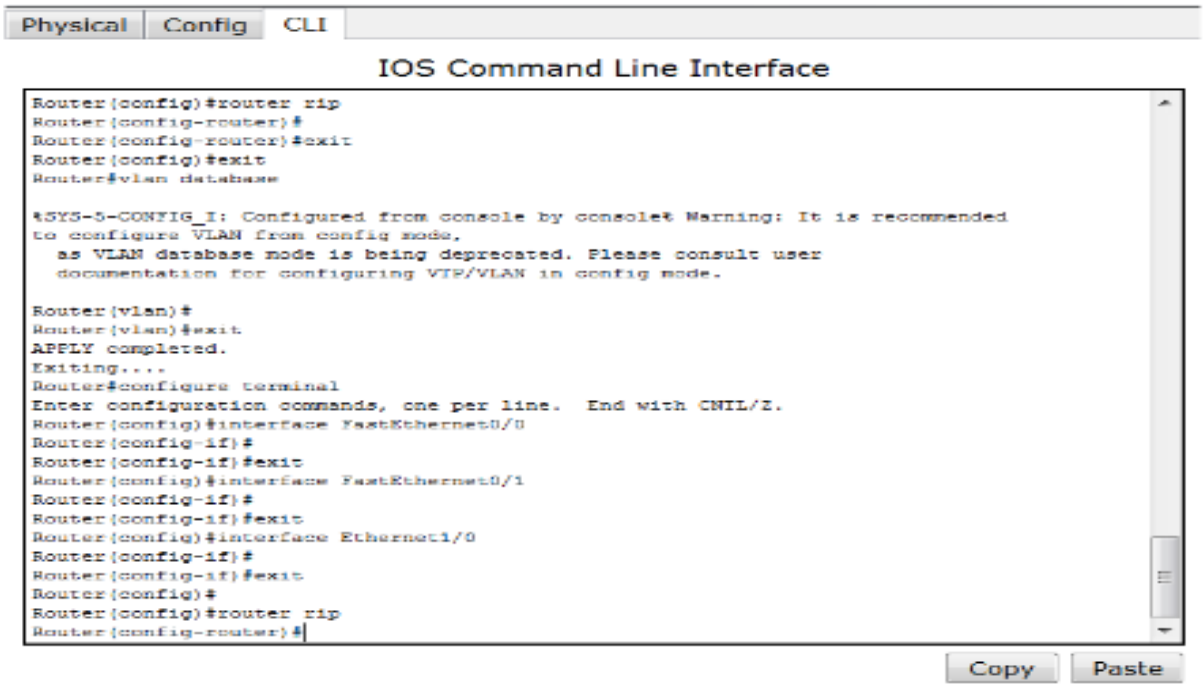

Figure IV.5 : Interface CLI.

9. Présentation des équipements utilisés

Pour installer le réseau sous Packet Tracer, nous avons besoin du matériel suivant :

- 3 routeurs 1841.
- Un switch fédérateur ou Multilayer 3560.
- 7 commutateurs Cisco 2960.
- 3 serveurs Generic.
- 42 PC.
- Des câbles droits et croisés pour connecter entre les différents équipements.

10. Architecture proposée de SCS

La figure IV.6 présente l'architecteur proposée de l'entreprise SCS sous packet tracer :

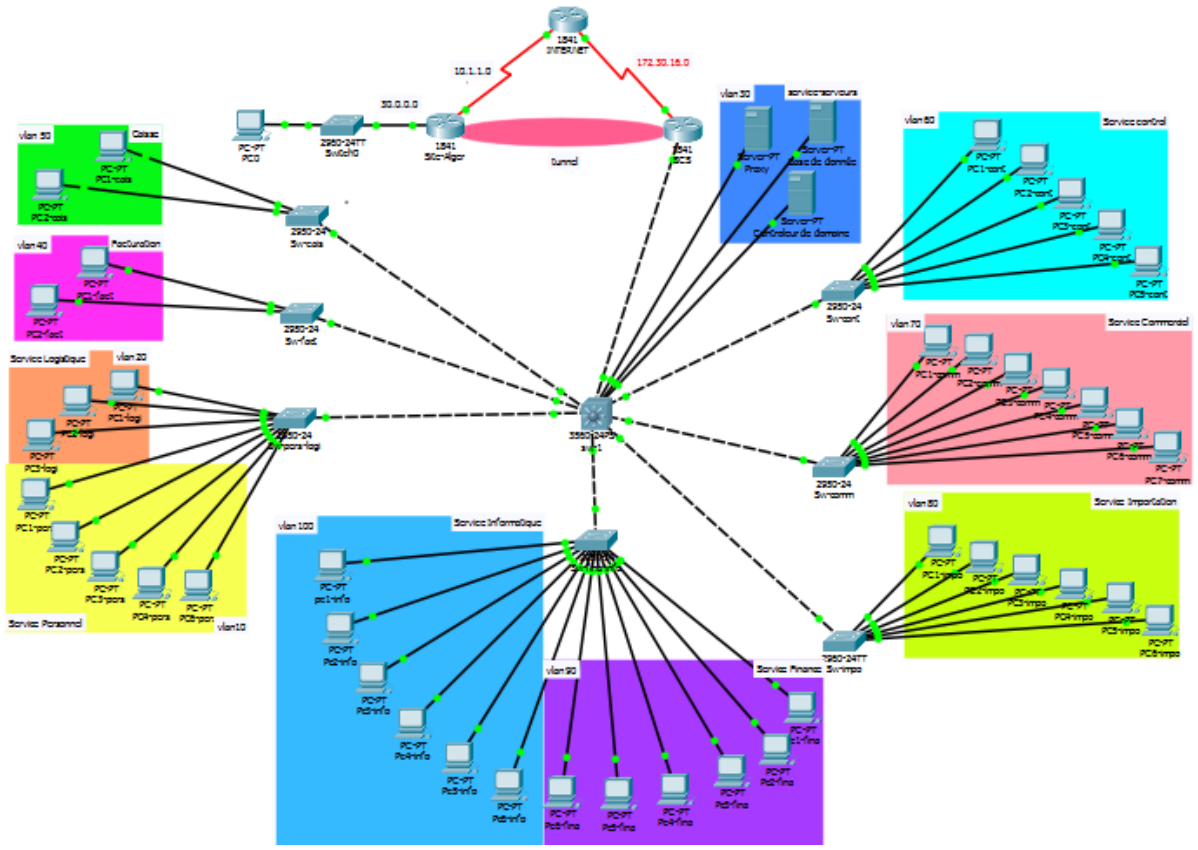

Figure IV.6 : L'architecture proposée de SCS sous Packet Tracer.

11. Segmentation VLAN

L'organisation réseau se fera en le segmentant à l'aide des VLAN, telle que les différents VLAN existant dépendent des différents services du réseau, par conséquent il y'aura naissance de 10 VLAN à savoir :

- Personnel.
- Logistique.
- Serveurs.
- Facturation.
- Caisse.
- Control.
- Commercial.
- Importation.
- Finance.
- Informatique.

Les Vlans seront nommées et identifiées dans la configuration comme suit :

Nom du VLAN	ID-VLAN	Description
Personnel	10	VLAN pour service Personnel
Logistique	20	VLAN pour service Logistique
Serveurs	30	VLAN pour serveurs
Facturation	40	VLAN pour service Facturation
Caisse	50	VLAN pour service Caisse
Control	60	VLAN pour service Control
Commercial	70	VLAN pour service Commercial
Importation	80	VLAN pour service Importation
Finance	90	VLAN pour service Finance
Informatique	100	VLAN pour service Informatique

Tableau IV.1 : Liste des noms et les identifiants des VLAN.

12. Plan d'adressage

L'entreprise SCS dispose d'un réseau informatique équipé de 42 ordinateurs. L'administrateur réseau de l'entreprise a choisie l'adresse réseau 192.168.1.0/24, de la classe C et de masque 255.255.255.0.

Dans un réseau comportant différents services comme celui de SCS, il devient nécessaire de subdiviser l´ensemble pour optimiser les échanges entre les machines. Pour ce faire, nous allons choisir de découper le réseau en plusieurs sous réseaux logique, donc nous allons attribuer quatre bits de la partie hôte d'origine de l'adresse et nous allons les utiliser pour créer des sous-réseaux. Avec ces quatre bits, il est possible de créer seize sous-réseaux. Avec les quatre bits de la partie ID hôte restants, chaque sous-réseau peut avoir jusqu'à seize adresses d'hôte, ce qui fait le nouveau masque de sous réseaux sera 255.255.255.240.

Le tableau IV.2 montre le plan d'adressage des VLANs :

ID	Adresse sous-réseaux	Masque sous-réseaux	Adresse de la 1ère machine	Adresse de la dernière machine	Passerelle
10	192.168.1.16	255.255.255.240	192.168.1.17	192.168.1.30	192.168.1.30
20	192.168.1.32	255.255.255.240	192.168.1.33	192.168.1.46	192.168.1.46
30	192.168.1.48	255.255.255.240	192.168.1.49	192.168.1.62	192.168.1.62

40	192.168.1.64	255.255.255.240	192.168.1.65	192.168.1.78	192.168.1.78
50	192.168.1.80	255.255.255.240	192.168.1.81	192.168.1.94	192.168.1.94
60	192.168.1.96	255.255.255.240	192.168.1.67	192.168.1.110	192.168.1.110
70	192.168.1.112	255.255.255.240	192.168.1.113	192.168.1.126	192.168.1.126
80	192.168.1.128	255.255.255.240	192.168.1.129	192.168.1.142	192.168.1.142
90	192.168.1.144	255.255.255.240	192.168.1.145	192.168.1.158	192.168.1.158
100	192.168.1.160	255.255.255.240	192.168.1.161	192.168.1.174	192.168.1.174

Tableau IV.2 : Plan d'adressage des VLAN.

13. Etapes de simulation

Pour la réalisation de cette architecture nous allons lancer une série de configuration des équipements en montrant un exemple de chaque configuration.

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

13.1 Configuration des commutateurs

a. Configuration de base

Au début d'une configuration de base du commutateur, on commence par :

- L'attribution d'un nom significatif au switch, Par exemple, la nomination du switch: Sw-pers-logi.
- Sécuriser l'accès au mode privilégié : nous avons choisi le mot de passe « cisco ».
- Sécuriser l'accès à la ligne de console et au terminal virtuel (vty) : nous avons choisi « cisco » comme mot de passe d'accès à la console, cet exemple montre les commandes de mise en place du mot de passe sur le switch Sw-pers-logi, la même chose sera faite pour les autres commutateurs (voir figure IV.7).

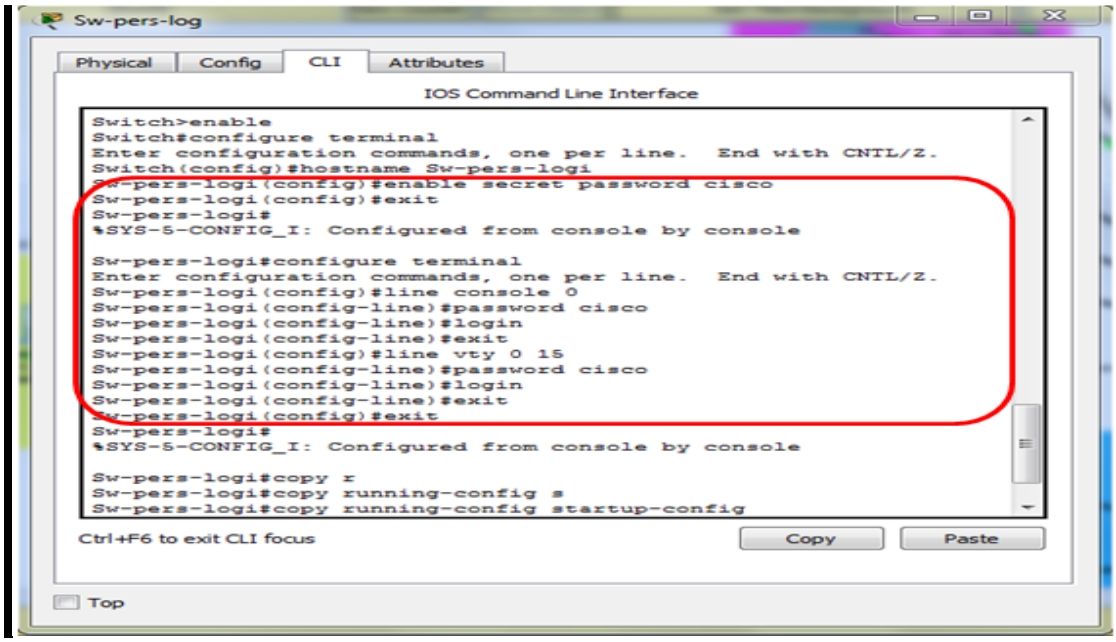

Figure IV.7 : Configuration des mots de passe au switch Sw-pers-logi.

b. Configuration de protocole VTP sur les commutateurs

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

- **Mode serveur**

La configuration du VTP serveur est faite au niveau de switch fédérateur, comme le montre la figure IV. 8 ci-dessous :

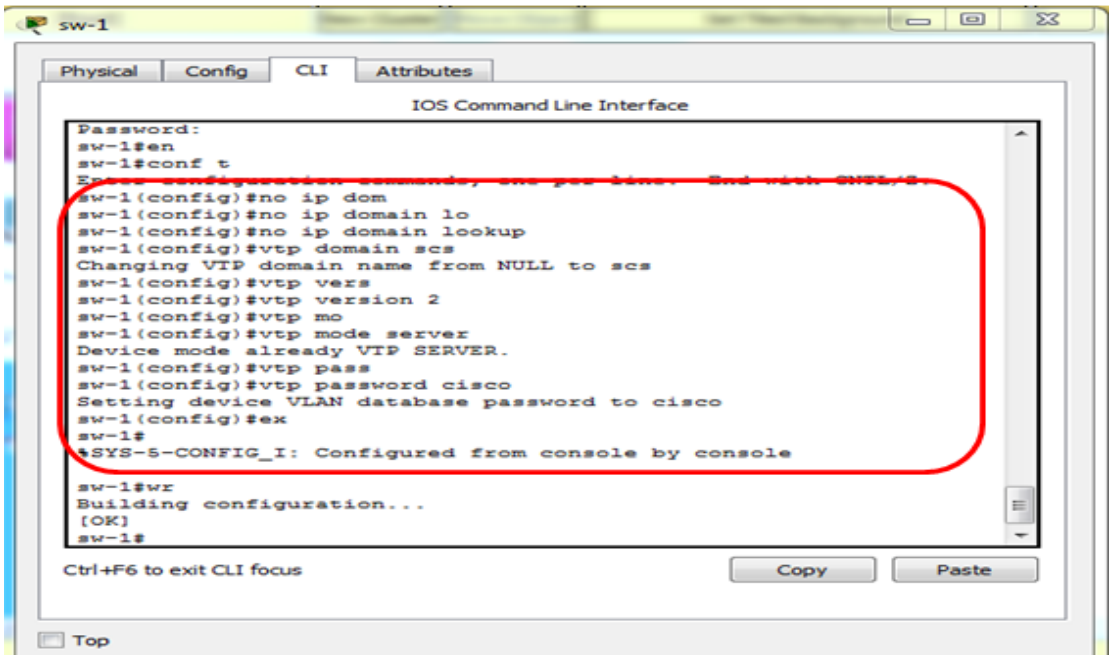

Figure IV.8 : Configuration du VTP serveur sur le switch fédérateur.

✓ **Vérification de la création de VTP server**

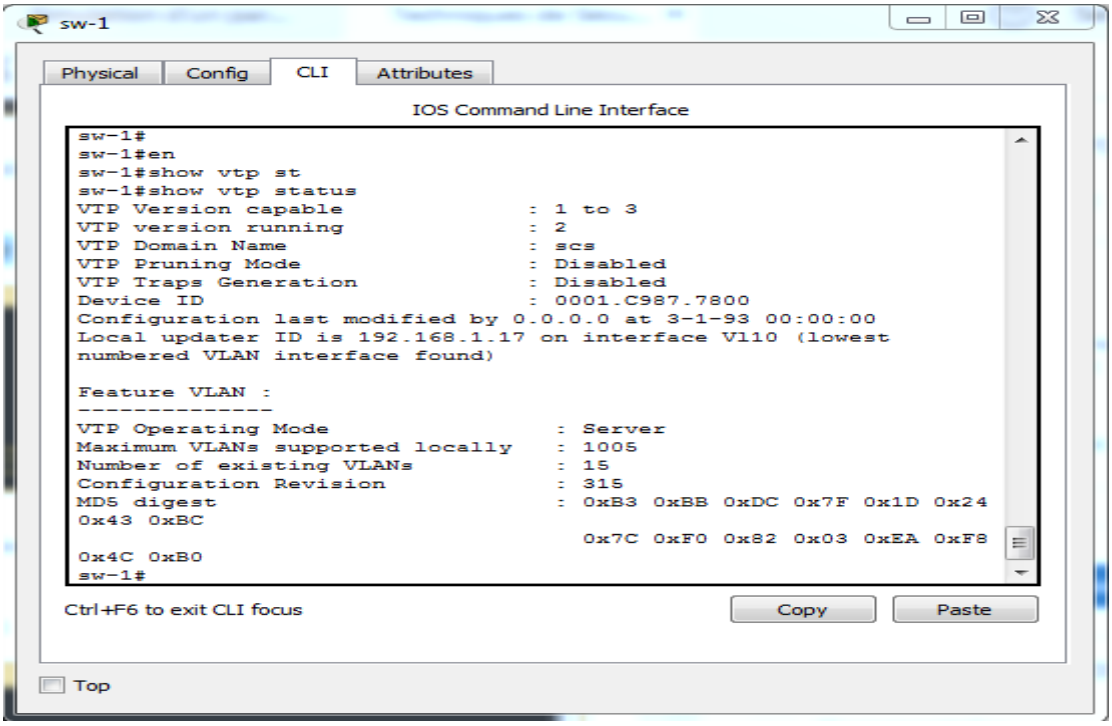

Figure IV.9 Vérification de la création de VTP server.

- **Mode client**

La configuration du VTP client sera au niveau de tous les commutateurs accès (voir figure IV.10).

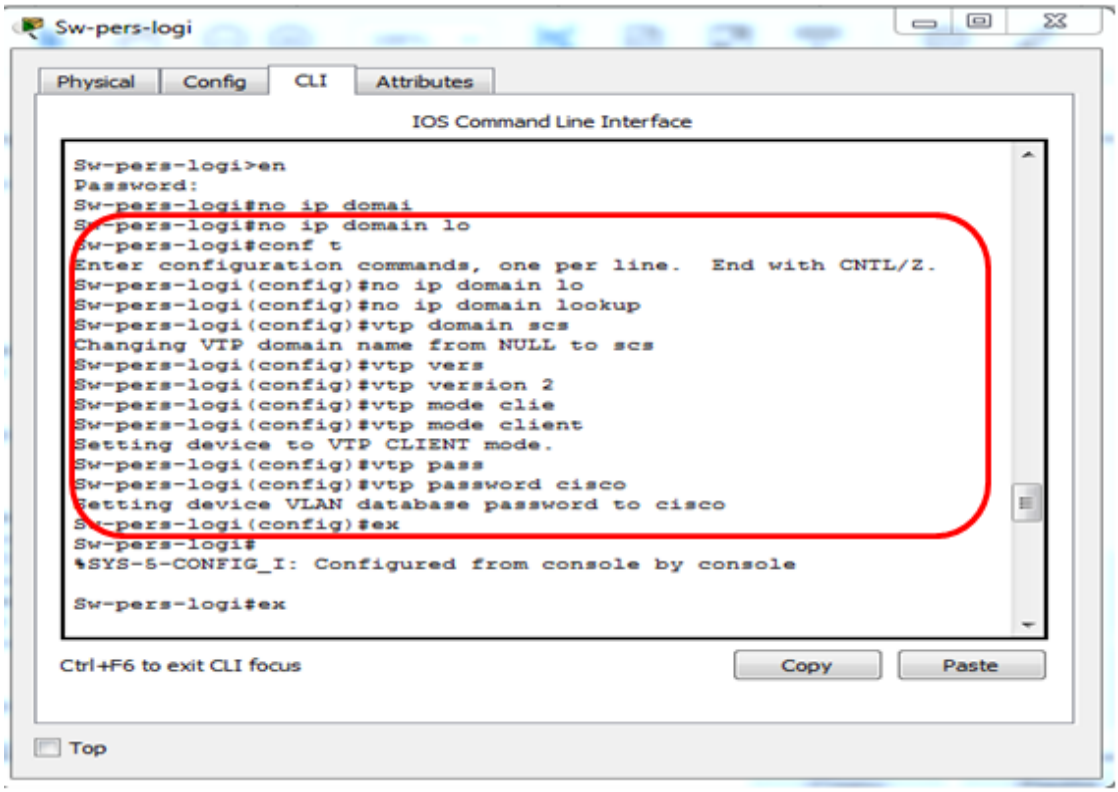

Figure IV.10 : Configuration du VTP client sur le switch.

c. Création des VLANs

La création des VLANs est faite au niveau de switch fédérateur sera répartie aux autres commutateurs du réseau (clients), En effet, l'ensemble des VLANs vont être créés automatiquement (voire figure IV.11).

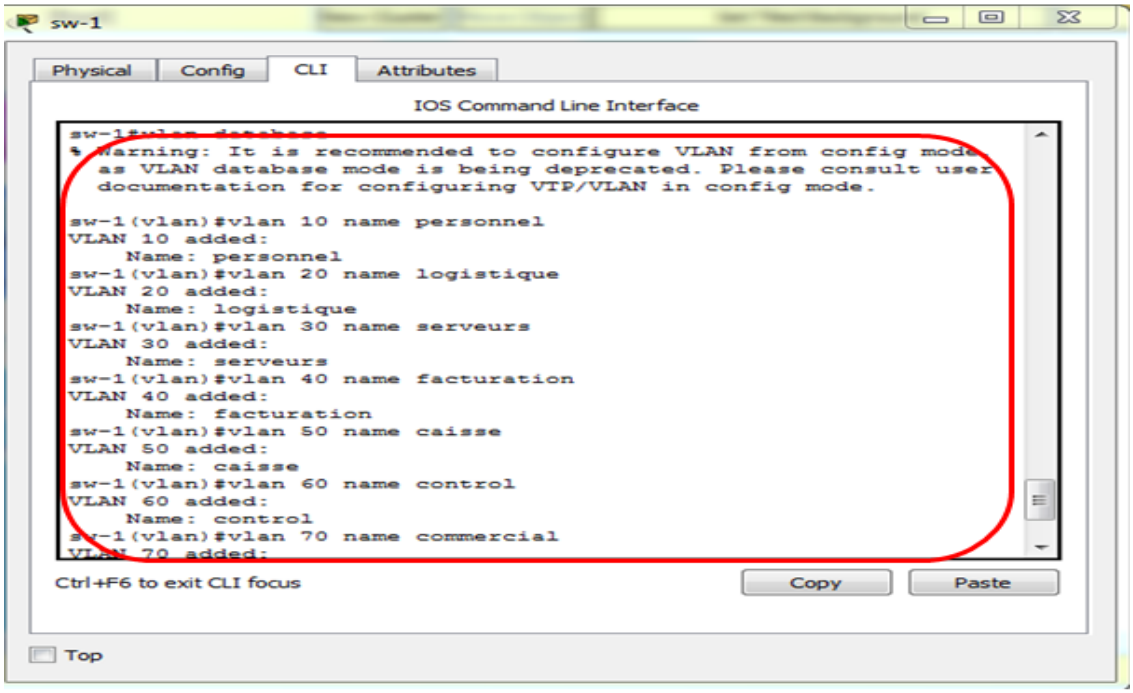

Figure IV.11 : Création des VLANs.

✓ **Vérification de la création des VLANs**

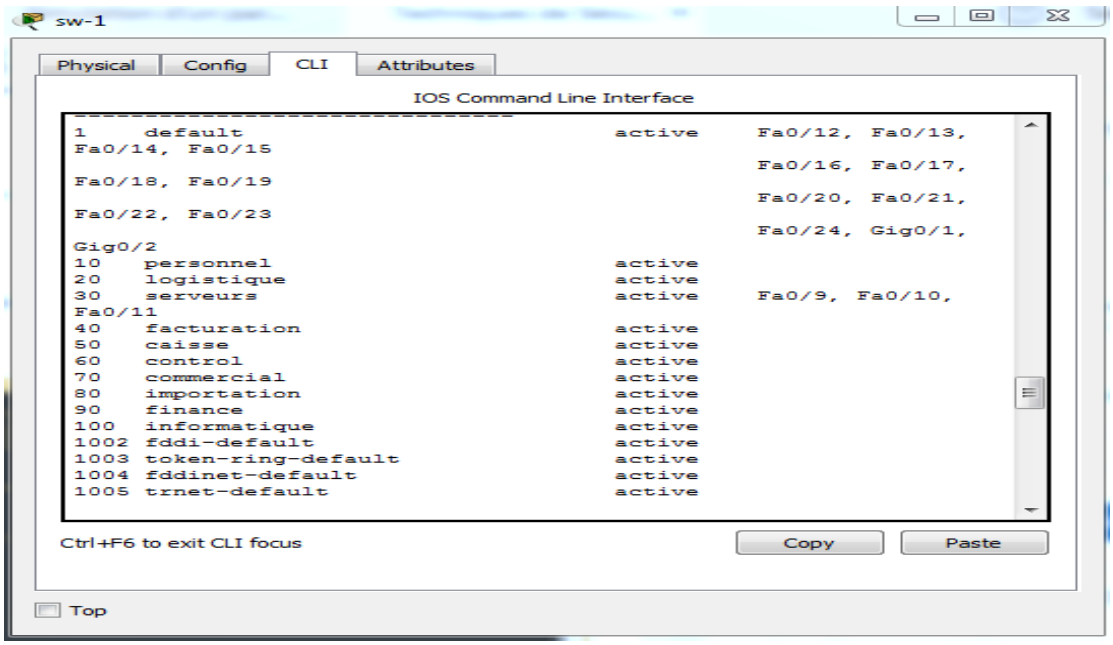

Figure IV.12 : Vérification de la création des VLANs.

d. Configuration des VLANs

Dans cette partie de configuration, nous allons attribuer les adresses IP pour chaque VLAN au niveau du Switch fédérateur, comme illustré dans la figure IV.13 :

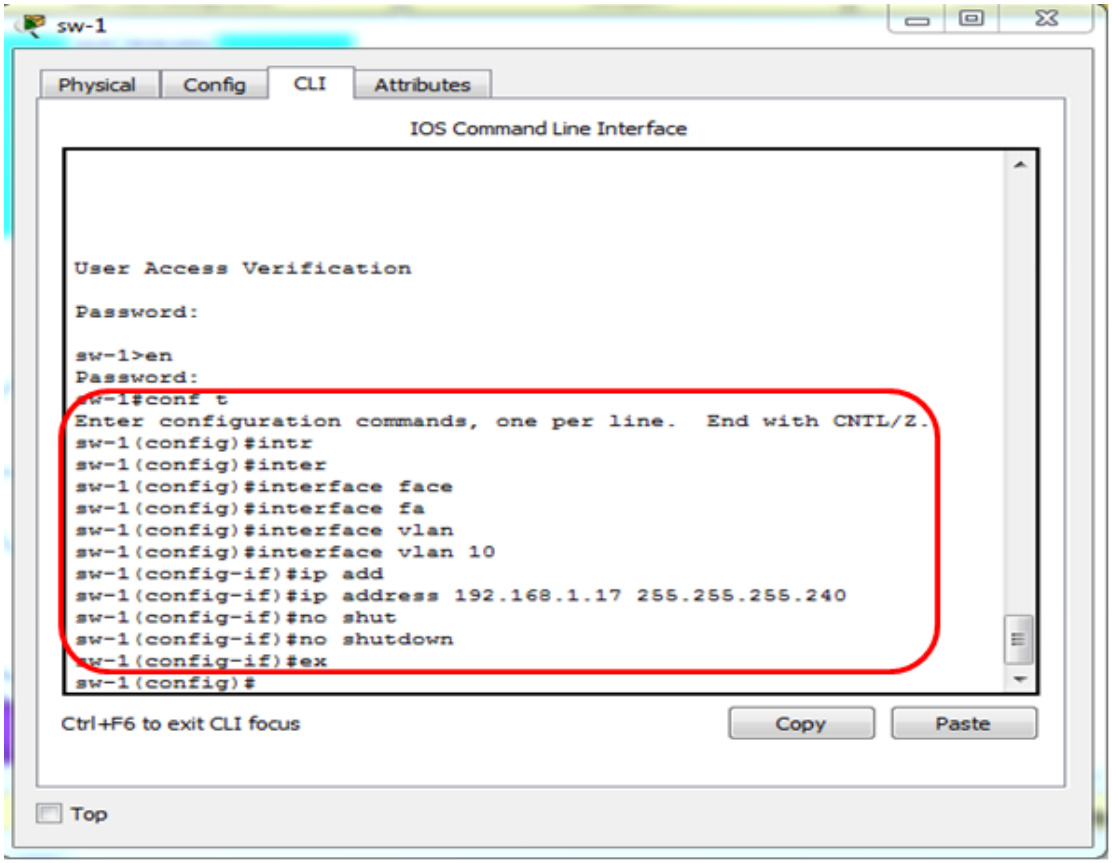

Figure IV.13 : Attribution des adresses IP pour chaque VLAN au niveau du Switch fédérateur.

- **Configuration des ports**

Les interfaces entre tous les switchs d'accès, cœur, périphérique et distants sont configures en mode trunk pour qu'elles puissent transporter les informations des différentes Vlans. Les interfaces qui seront connectés à des postes de travail seront configurées en mode accès.

✓ **Configuration des agrégations (Trunk)**

Le lien trunk est nécessaire entre le switch serveur et les switch clients, les commandes suivantes nous permettent d'associer un port à un VLAN en mode trunk en ajoutant la commande « range » qui pourra réunir toutes les interfaces en une seule fois comme la montre la figure IV.14 :

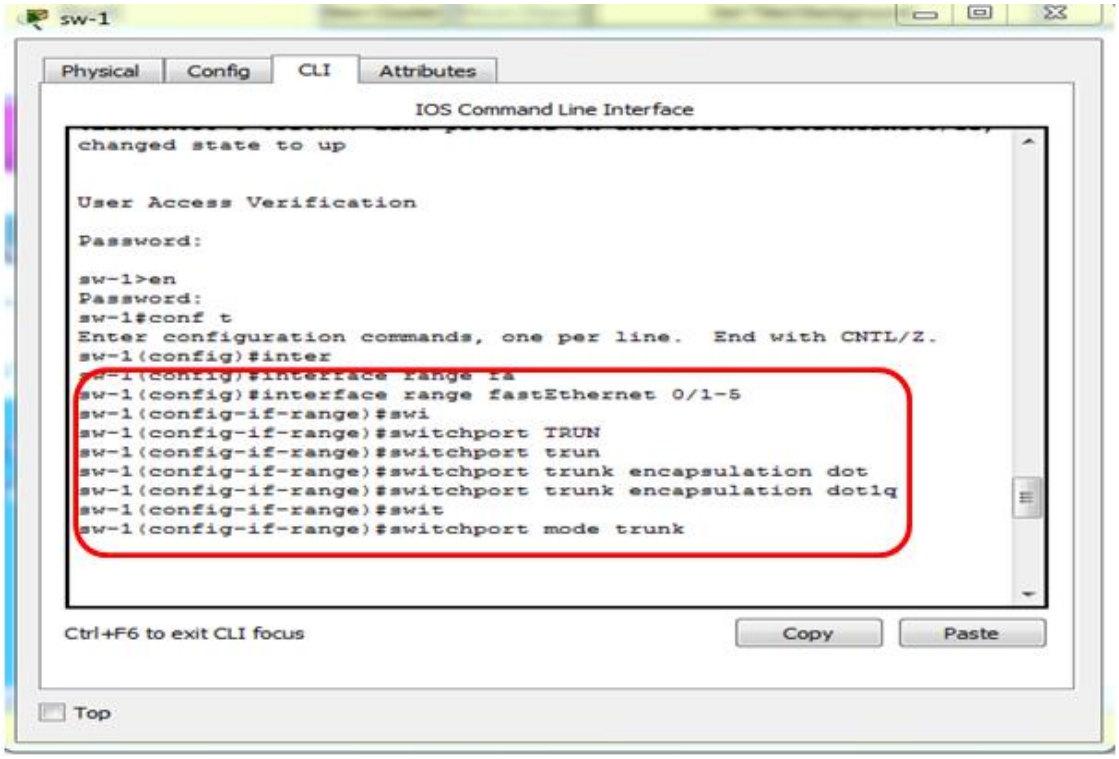

Figure IV.14 : La configuration en mode trunk.

- **Configuration des agrégations (Access)**

Les ports vont être assignés aux différents VLANs existants au niveau de chaque commutateur Accès, les commandes suivantes nous permettent d'associer un port à un VLAN en mode Accès (voir figure IV.15) :

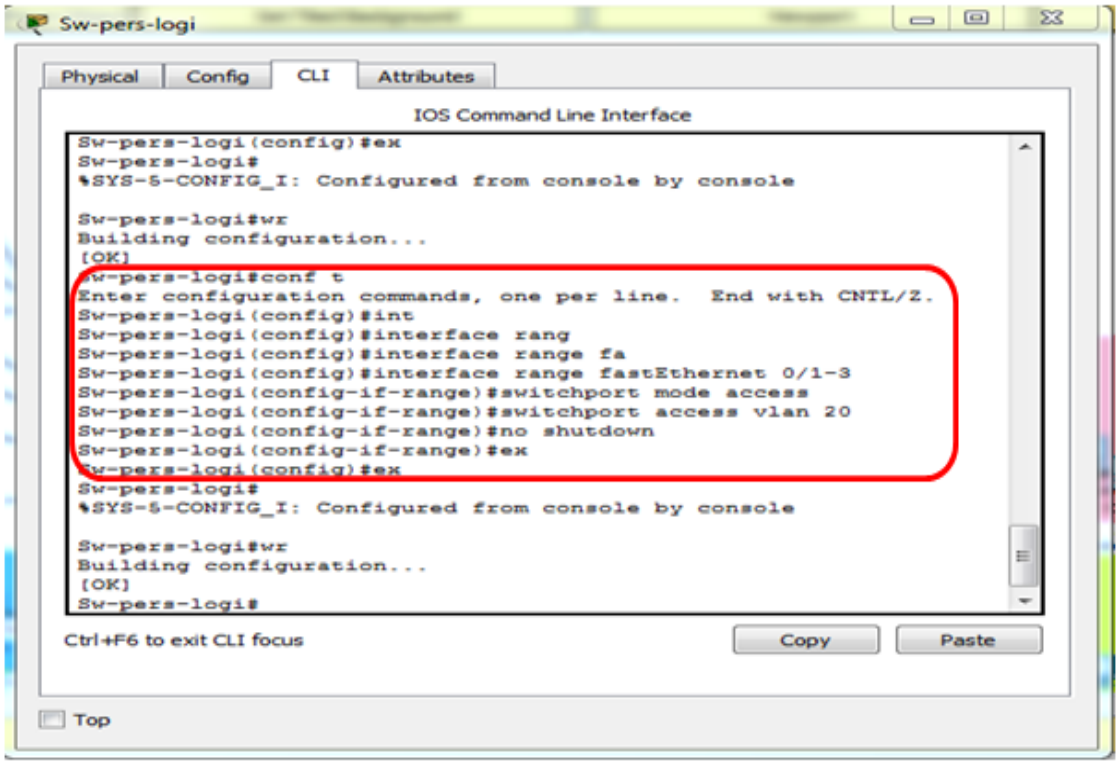

Figure IV.15 : La configuration en mode accès.

e. Configuration de DHCP

Afin de simplifier à l'administrateur la gestion et l'attribution des adresses IP, on utilise un serveur DHCP qui permet de configurer les paramètres réseaux client, au lieu de les configurer manuellement.

On va créer les pools DHCP pour chaque VLANs, et pour cela on a qu'à suivre les commandes comme illustré dans la figure IV.16 :

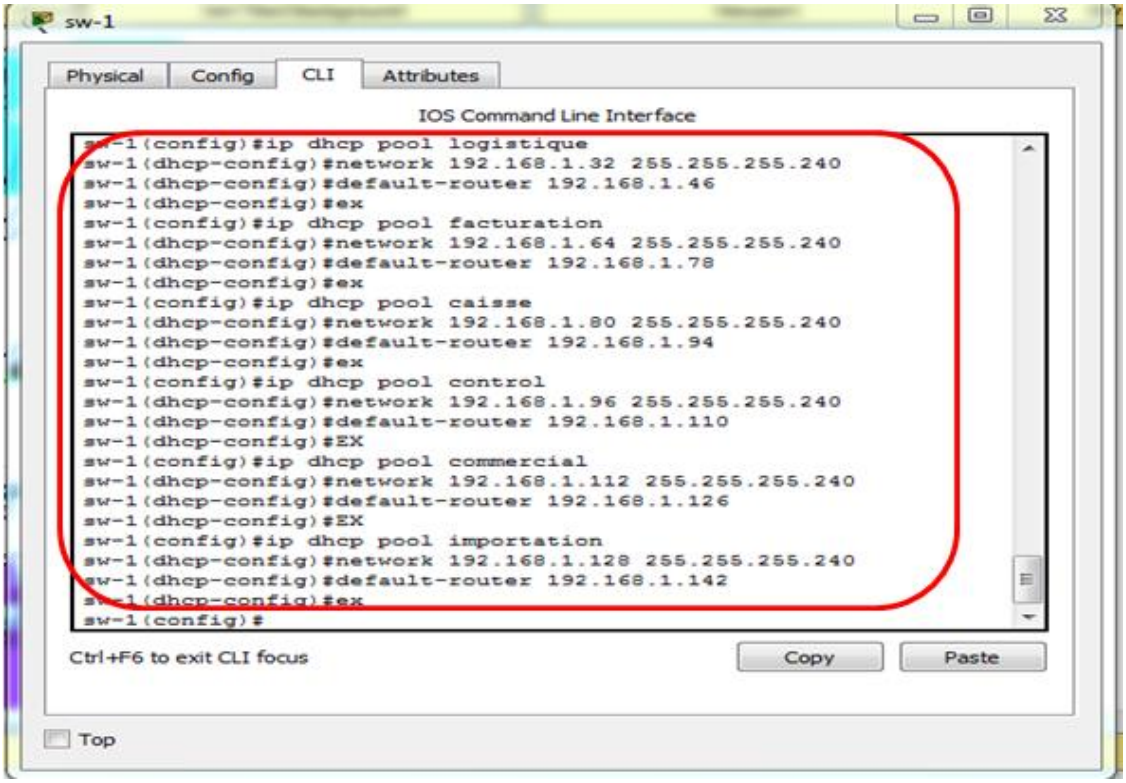

Figure IV.16 : Configuration de DHCP.

13.2 Configuration de routeur

Nous avons trois étapes pour configurer le routeur, la première pour la configuration de base, la deuxième pour routage inter-VLANs et la dernière pour configurer les listes de contrôle ACL.

a. Configuration de base

Pour configurer le routeur on commence par :

- L'attribution d'un nom significatif au routeur.
- Sécuriser l'accès au mode privilégié : nous avons choisi le mot de passe « cisco » pour sécuriser l'accès au mode privilégié.
- Sécuriser l'accès à la ligne de console et au terminal virtuel (vty) : nous avons choisi « cisco » comme mot de passe d'accès à la console, cet exemple montre les commandes de mise en place du mot de passe sur le routeur (voir figure IV.17) :

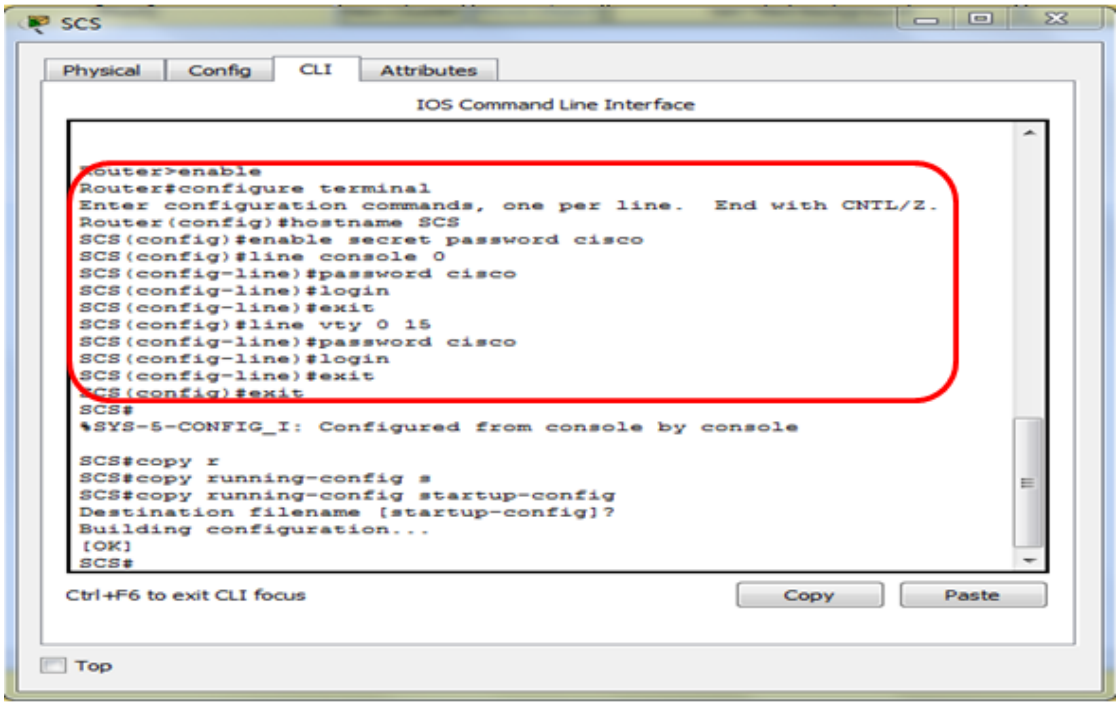

Figure IV.17 : Configuration des mots de passe au routeur SCS.

b. Routage inter-VLANs

Le routage intre-VLANs permet aux plusieurs VLANs différents de communiquer entre eux, voici quelques commandes à suivre pour configurer le routage inter-VLANs (voir figure IV.18) :

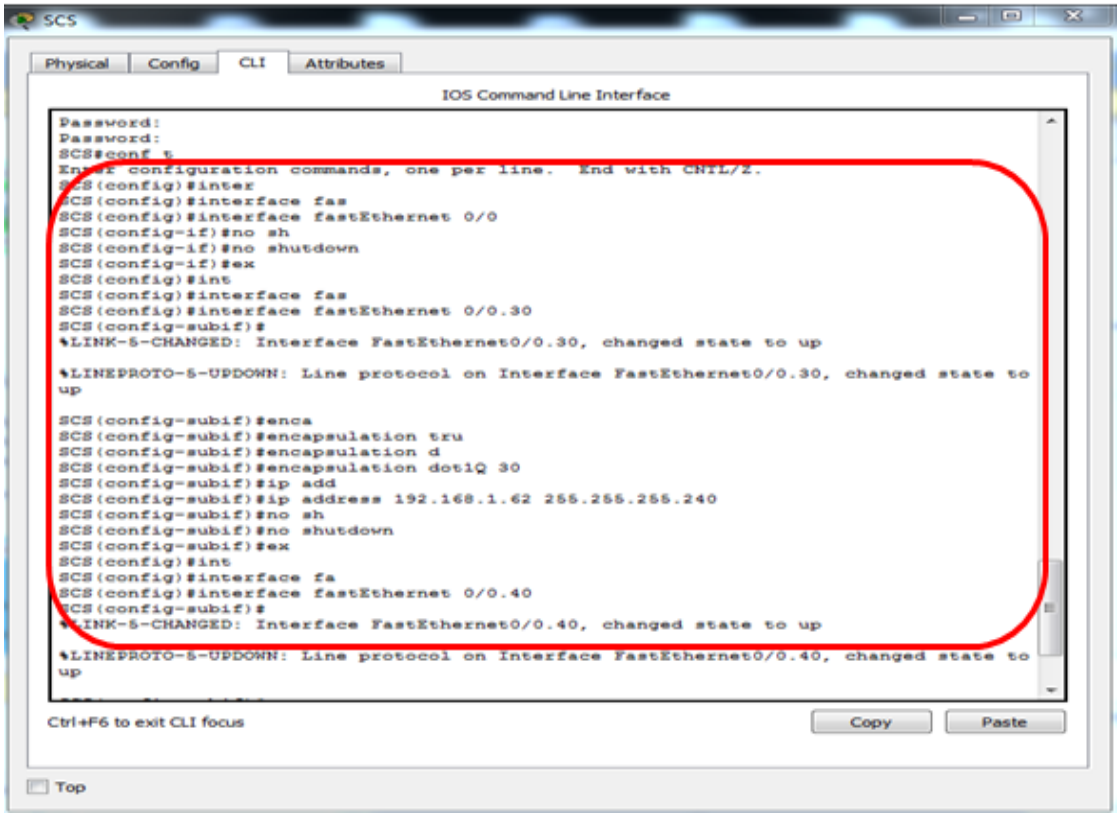

Figure IV.18 : Routage inter-VLAN.

c. Access Control Liste (ACL)

On a utilisé les listes des contrôles d'accès afin de limiter la communication entre certains VLANs, nous avons pris comme exemple le VLAN 60 qui est le VLAN Control auquel nous avons autorisé la communication qu'avec le VLAN serveurs, et bloqué la communication avec les autres VLANs comme le démontre la figure IV.19 :

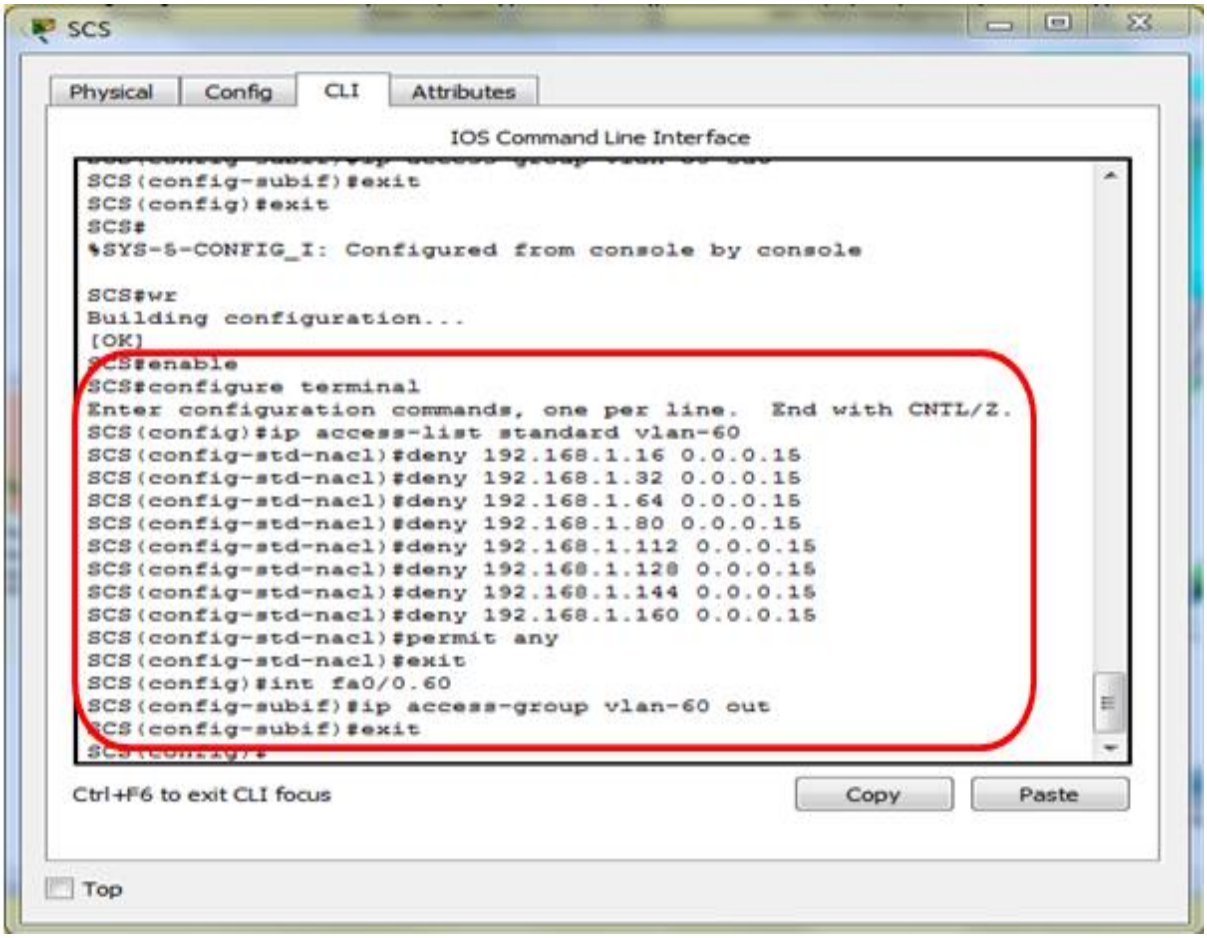

Figure IV.19 : Configuration des ACLs au niveau du routeur.

- **Tests et validation de la configuration des vlans**

  Dans cette partie nous allons vérifier la communication entre tous les ordinateurs et les serveurs en utilisant la commande Ping (voir figure IV.20).

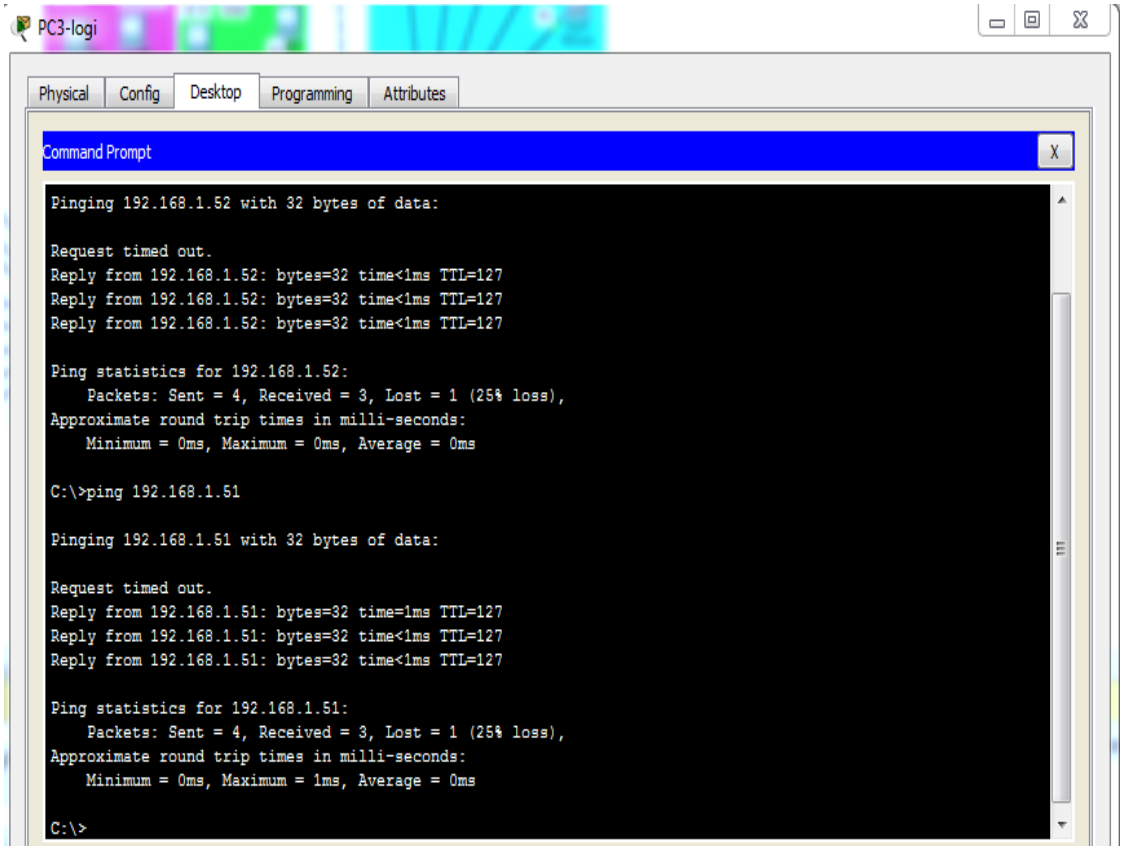

Figure IV.20 : Tests et validation de la configuration de VLAN.

13.3 Configuration des VPN

Dans notre projet, on a met en place des tunnels VPNs afin de sécuriser les données transmis entre tous les sites distants de SCS, nous avons créé deux tunnels VPN qui relie le réseau d'entreprise SCS et le site d'Alger.

a. Mise en place de la fonction NAT sur le router de Béjaia et Alger

Nous volons que le trafic dirigé vers de véritables destinations internet soit converti par la NAT, et que celui destiné à un tunnel IPSec soit traité par le protocole IPSec (et pas par la conversion NAT), pour cela, l'Access List sera préparée pour la création du VPN, c'est-à-dire qu'on exclut les communications entre les deux LANs de la règle NAT. Voir la figure IV.21 :

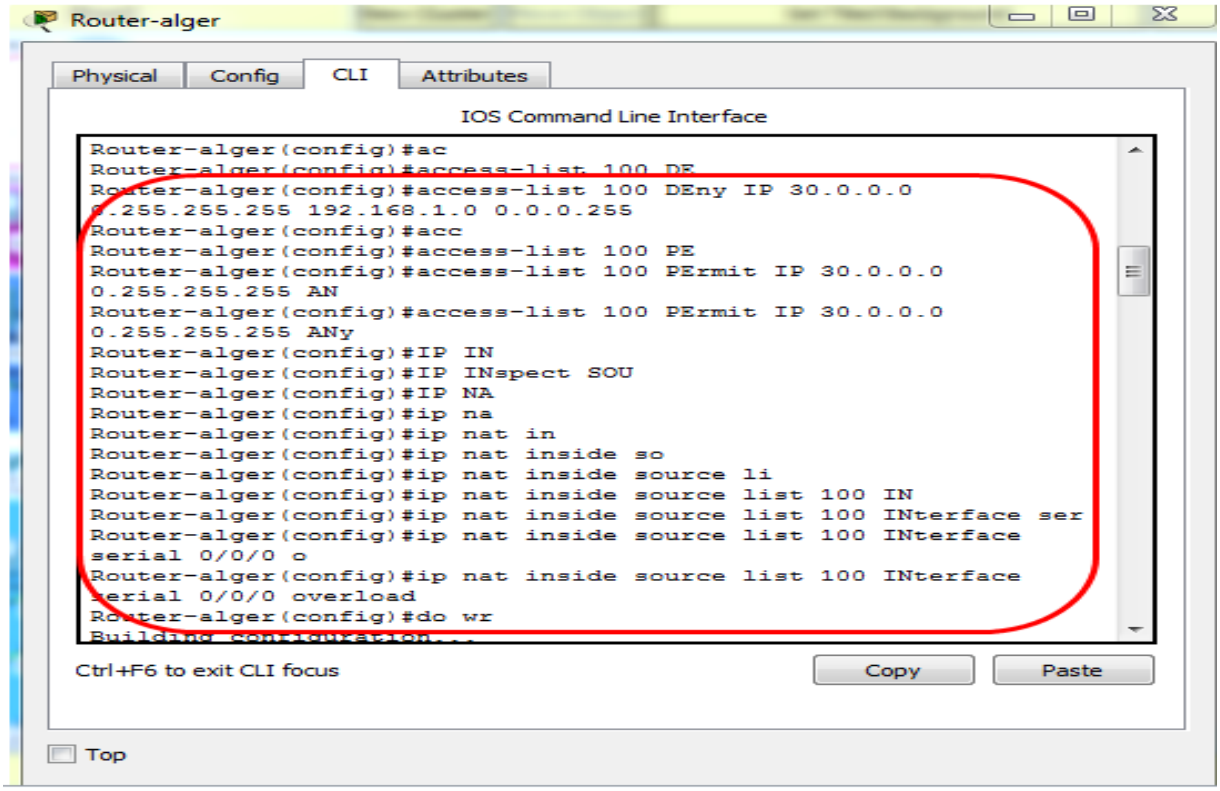

Figure IV.21 : Configuration de la fonction NAT.

b. Configuration d'un tunnel VPN IPSec

ISAKMP et IPsec sont la base de la construction et le chiffrement des tunnels VPN, pour obtenir le tunnel VPN IPSec on doit diviser le travail en deux étapes qui sont les suivantes :

- **Configuration d'ISAKMP**

  Nous allons configurer l'ISAKMP qui détermine quelle encryptions on utilise, quelle type d'authentification, etc. Nous avons utilisé les paramètres suivants :

  - Encryptage AES.
  - Mode de secret partagé PSK.
  - Authentification par clé pré-partagées.
  - Algorithme de hachage SHA (valeur par défaut).
  - Méthode de distribution des clés partagées DH-2 (clés Diffie-Hellman groupe 2 - 1024bits).
  - Durée de vie 86400 secondes (valeur par défaut).

Et nous avons spécifié le protocole de hash utilisé, le type et la durée de validité des clés de sessions. Par la suite nous avons indiqué si le routeur 'peer' (celui situé au bout du tunnel) est identifié par un nom ou son adresse. Voir la figure IV.22 :

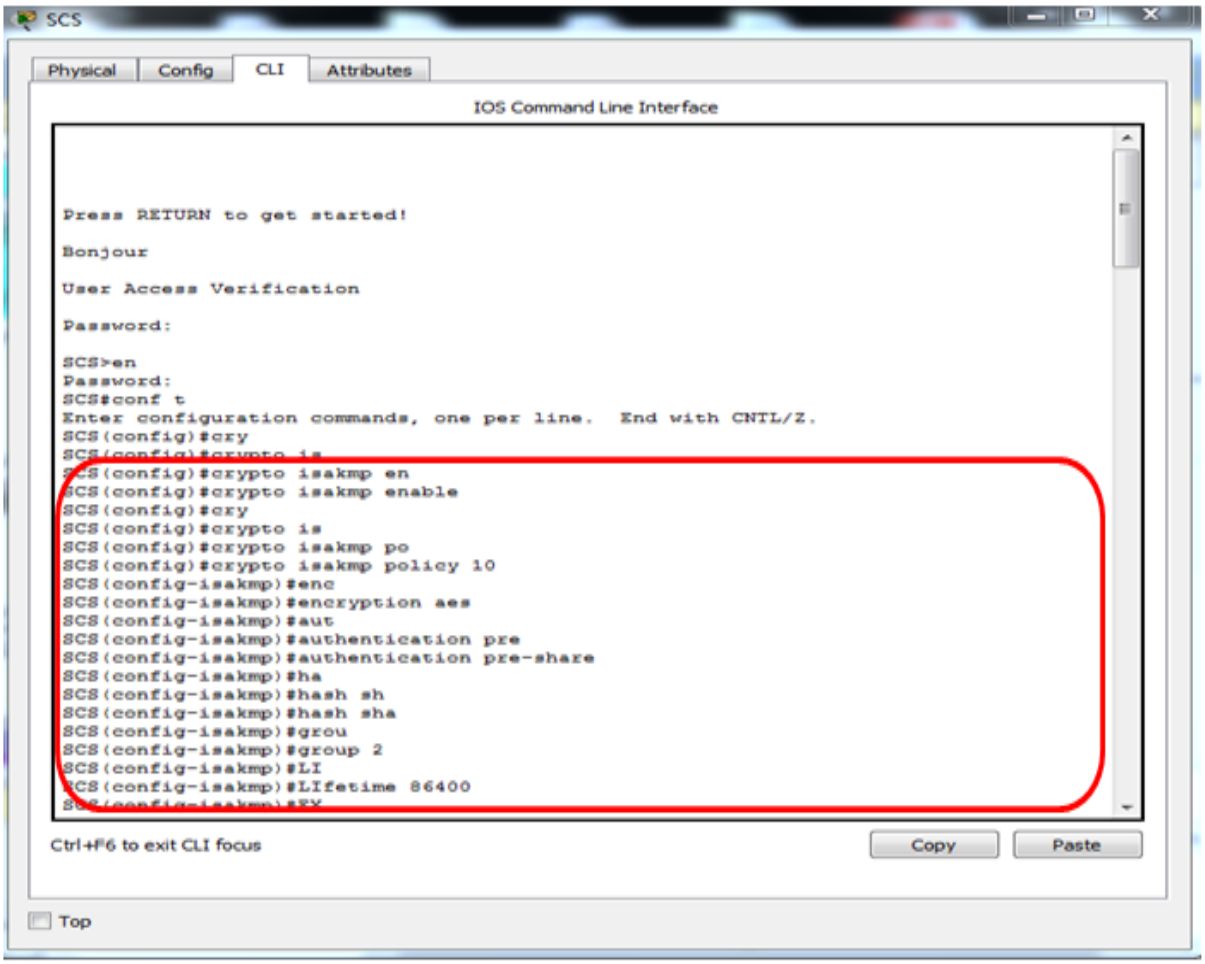

Figure IV.22 : Configuration d'ISAKMP.

- **Configuration d'une clé**

  La figure IV.24 illustre les différentes étapes de la configuration d'une clé 'ISAKMP'.

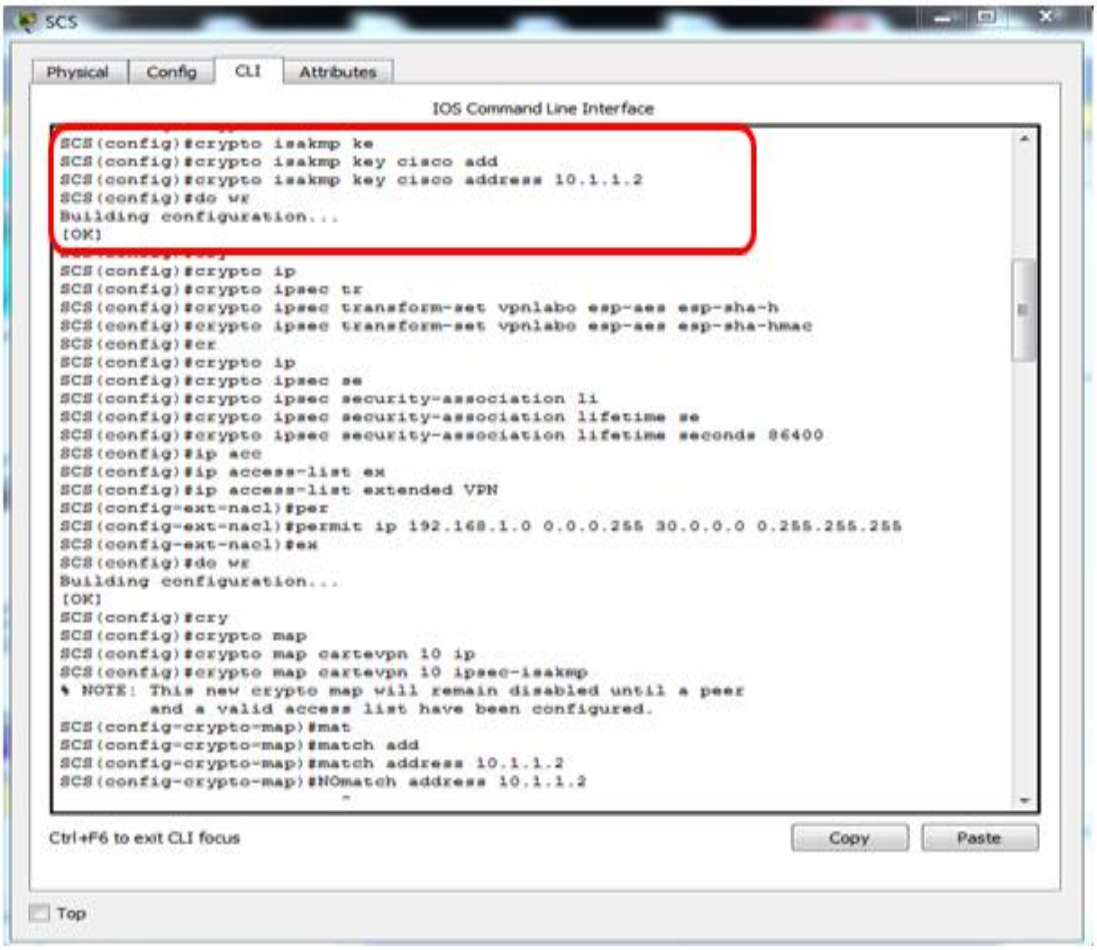

Figure IV.23 : Configuration d'une clé ISAKMP.

- **Configuration d'IPSec (ACL, crypto MAP)**

Pour configurer le protocole IPSec on a besoin de configurer les éléments suivants :

- **Création d'ACL étendu**

L'ACL étendu que l'on crée permettra de définir le trafic qui passera à travers le tunnel VPN. Dans notre projet, le trafic s'achemine du réseau 192.168.1.0/24 à 30.0.0.0/8 (voir la figure IV.25)

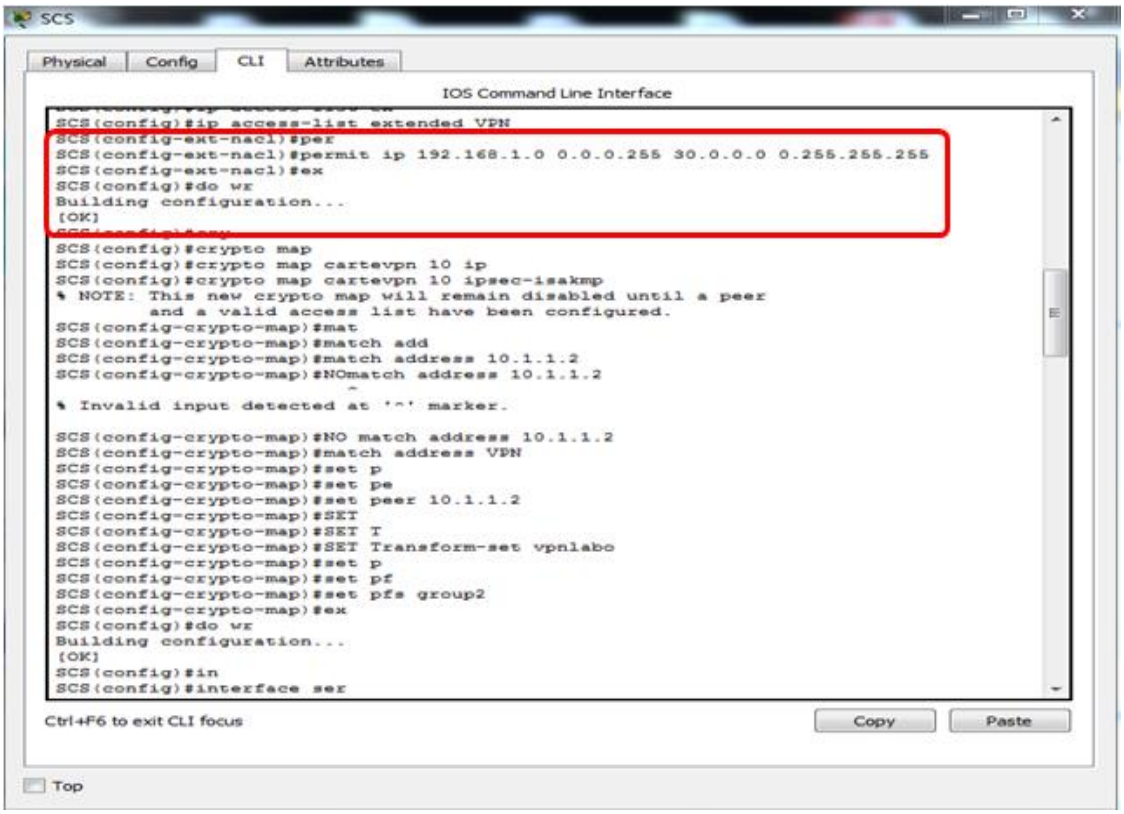

Figure IV.24 : Configuration d'ACL.

- **Créer l'IPSecTransform**

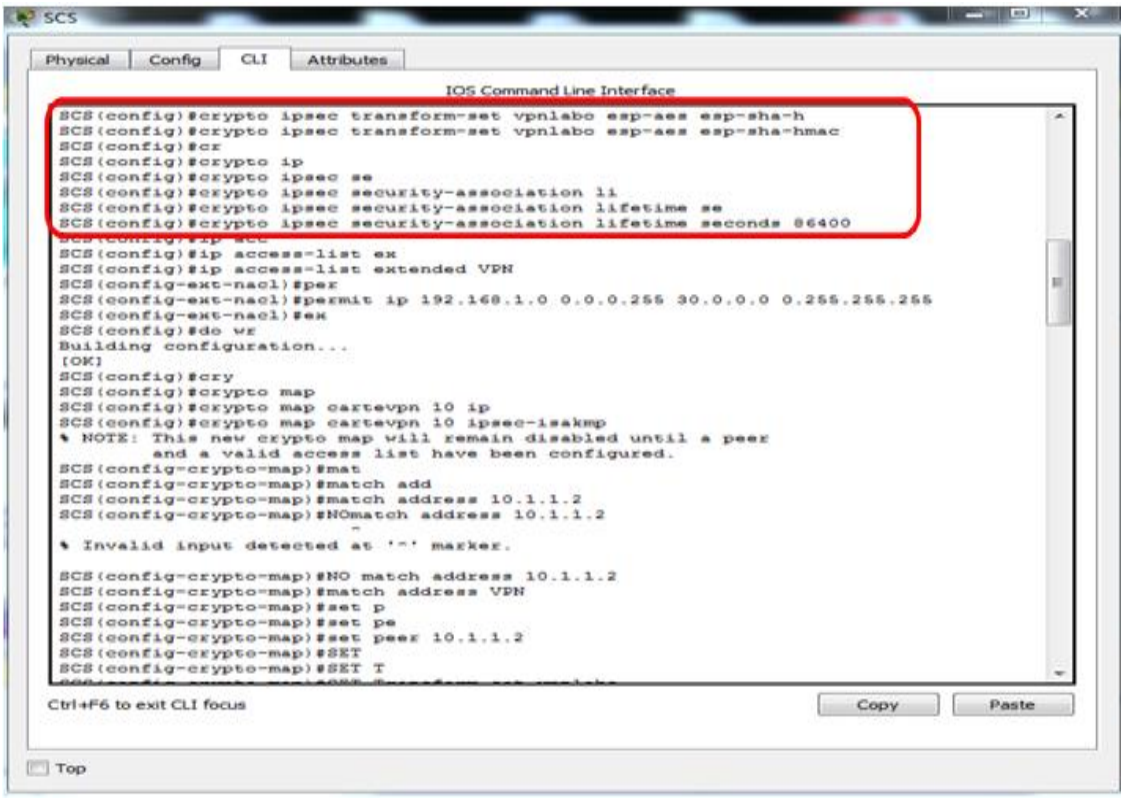

Figure IV.25 : Configuration d'IPSec.

- **Créer crypto carte et l'application de la crypto map sur l'interface serial**

Crypto carte permit d'etablir le lien entre ISAKMP définie précédemment et la configuration IPSec et Il faut aussi appliquer la crypto-map à l'interface WAN de Routeur, voir la figure IV.27 :

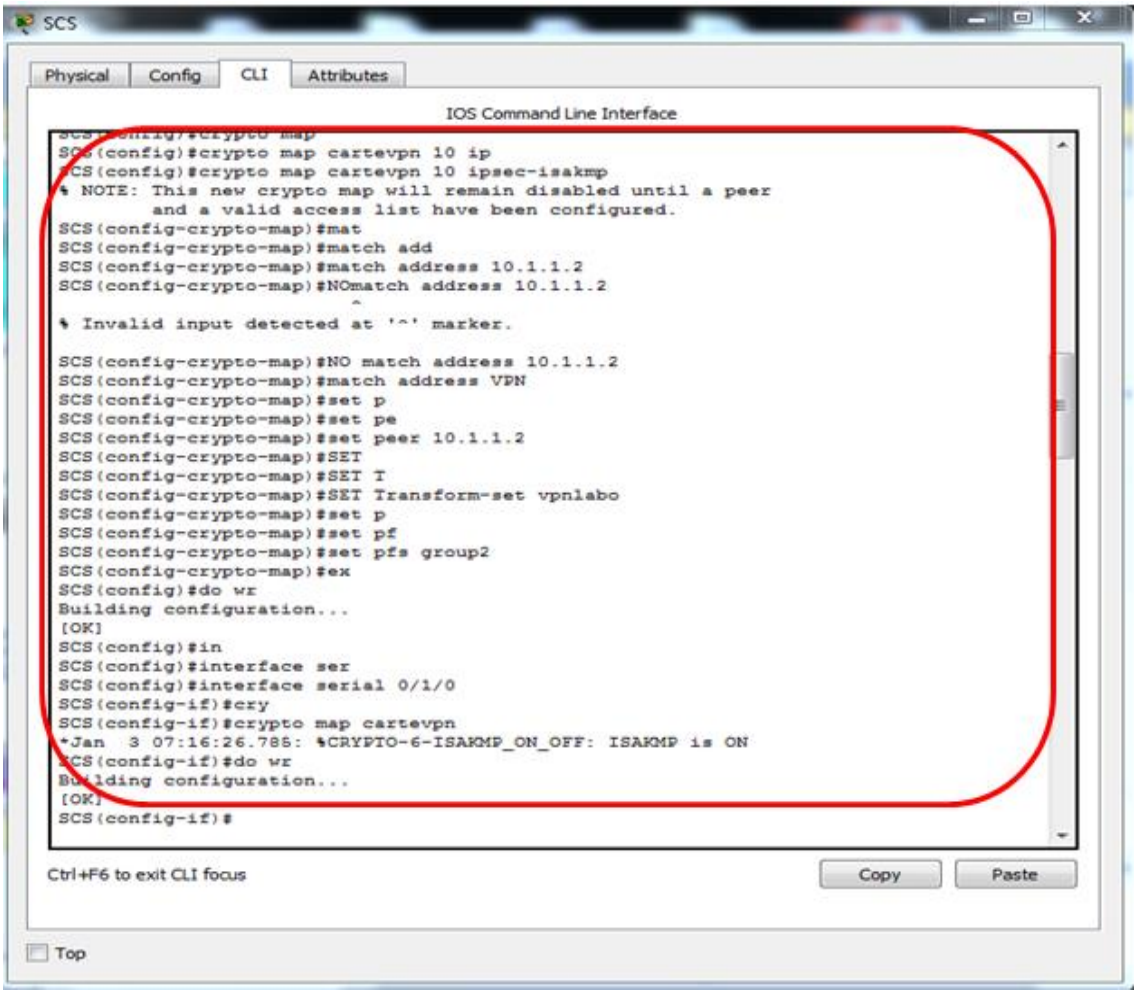

Figure IV.26 : Création de crypto map.

- **Vérification du fonctionnement tunnel VPN**

Pour établir la liaison VPN et vérifier le fonctionnement, il faut envoyer du trafic au travers du tunnel, on faisant un ping entre les stations.

Une fois le tunnel configuré, plusieurs commandes permettent de vérifier si le tunnel fonctionne. Telle que, show crypto isakmp policy, show crypto isakmp sa, show crypto ipsec sa, comme illustré dans la figure suivante :

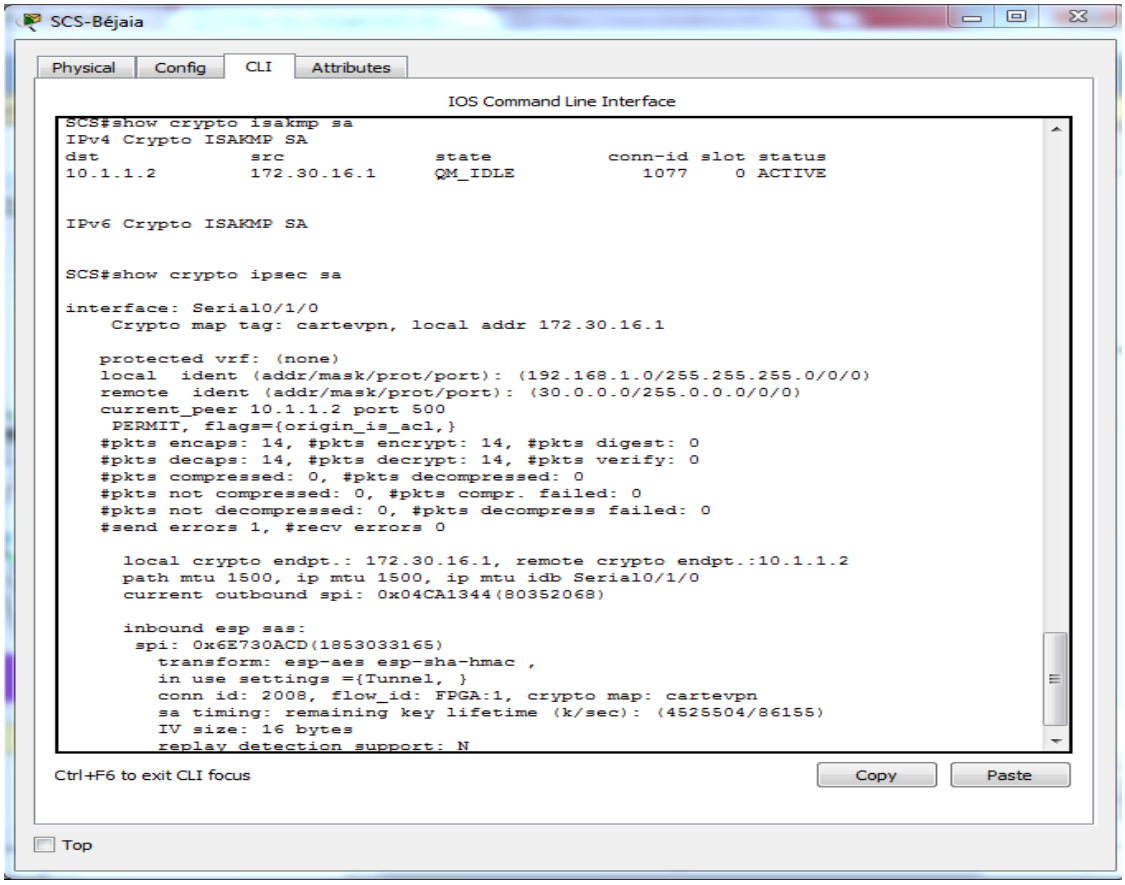

Figure IV.27 : Vérification du fonctionnement tunnel VPN.

14. Conclusion

La connaissance préalable d'une infrastructure réseaux est nécessaire pour acquérir la maitrise globale d'un environnement réseaux. Ce chapitre vient de présenter l'organisme d'accueil «SCS» et sa structure ainsi que le service informatique de l'entreprise dans lequel nous avons effectué notre stage, puis nous avons étudié les équipements utilisés dans les parties réseau et sécurité.

Par la suite nous avons vu les différentes étapes à suivre pour la mise en place des réseaux VLANs et VPNs, en effet ces deux derniers permettent d'implémenter la sécurité, cela nous a conduit à mettre en avant une problématique bien précise, une étude descriptible et la mise en œuvre des solutions proposées qui permettront de mieux organiser les réseaux.

Pour valider nos solutions, nous avons effectué un ensemble de tests afin de prouver l'efficacité de réseau.

Conclusion générale et perspectives

Conclusion générale et perspectives

Notre travail est divisé en deux parties, à savoir l'approche théorique qui était subdivisé en trois chapitres dont le premier a porté sur les généralités des réseaux informatiques, le second sur la sécurité et le troisième sur les réseaux VLANs et VPNs. La deuxième partie offre une présentation de l'organisme d'accueil et traite l'approche pratique qui est la réalisation en utilisant le simulateur Packet Tracer plus précisément la segmentation des réseaux VLANs (définir les protocoles d'administration et de gestion comme VTP, ACL et DHCP que nous avons implémenté sur notre architecteur) et la configuration des liaisons virtuelles VPNs.

Nous avons étudié d'abord l'architecture existante du réseau de l'entreprise SCS (Sommam Computer System), dans laquelle nous avons effectué notre stage, ce qui nous a permis de proposer une nouvelle architecture avec une meilleure fluidité et sécurité du réseau. Dans cette nouvelle architecture, nous avons proposé deux améliorations en utilisant le simulateur Packet Tracer :

La segmentation en VLAN, où nous avons segmenté le réseau d'une manière à avoir une bande passante optimisée et une organisation souple et sécurisée. Puis, nous avons mis en place des lignes virtuelles VPN qui permettant d'interconnecter des entités distantes (SCS et Alger) en toute sécurité. Il en ressort que la technologie VPN basée sur le protocole IPSec est l'un des facteurs clés de succès, qui évolue et ne doit pas aller en marge des infrastructures réseaux sécurisés.

Les résultats obtenus lors des simulations effectués sur packet Tracer ont montré le bon fonctionnement du VLAN et VPN au sein de l'entreprise.

En guise de perspectives, nous envisageons de :

La mise en place des mécanismes pour la supervision des équipements de réseau afin de détecté leurs pannes ou leurs disfonctionnement, Implémentation et configuration des systèmes de détection d'intrusions. Ainsi que, la configuration d'une zone démilitarisée (DMZ) est très importante.

Liste bibliographique

Liste bibliographique

[1] : Atelin Philippe, Réseaux informatiques Notions fondamentales, Editions ENI, France, Janvier 2009.

[2] : https://www.supinfo.com/articles/single/5709-classification-reseaux-informatiques, consulté le 23 mars 2018.

[3] : Dordoigne José, Réseaux informatiques Notions fondamentales, édition ENI, France, Mars 2015.

[4] : Bertrand Petit, Architecture des réseaux, 3ème édition, Janvier 2010.

[5] : https://fr.scribd.com/document/260293619/chap2reseau, consulté le 9 avril 2018.

[6]:https://benhur.teluq.uquebec.ca/SPIP/inf1160/IMG/pdf/inf1160-notionsfondamentales, consulté le 20 Mars 2018.

[7] :https://fr.wikibooks.org/wiki/Les_r%C3%A9seaux_informatiques/Les_mod%C3%A8les_OSI_et_TCP, consulté 09 Avril 2018.

[8] : Guy Pujolle, Les réseaux, édition EYROLLES, France, 2008.

[9] : Clément Michael, Le protocole TCP/IP, 1er édition, Paris, Octobre 2006.

[10] : Jacques Philipp, l'Architecture des Réseaux TCP/IP, 1er édition, France, 2006.

[11] : Pierre Volle, E-commerce De la stratégie à la mise en œuvre opérationnelle, PEARSON 3ème édition, France, 2014.

[12] : https://www.inetdoc.net/articles/adressage.ipv4/adressage.ipv4.class.html, consulté 09 Avril 2018.

[13] : Sylvain Caicoya, Le guide complet TCP/IP, 2ème édition, 2013.

[14] : Aman Vladimir, Concevoir la sécurité informatique en entreprise, 2014.

[15] : Solange Ghernaouti-Hélie, Sécurité informatique et réseaux, 2ème édition, 2008.

[16] : Jean-François Pillou et Jean-Philippe Bay, Tout sur la Sécurité informatique, DUNOD 3ème édition, France, Août 2013.

[17] : Laurent Bloch et Christophe Wolfhugel, Sécurité informatique principes et méthodes, EYROLLES 2ème édition, France, 2012.

[18] : Jean-François, La sécurité informatique dans la petite entreprise, France, Décembre 2012.

[19] : http://dspace.univ-tlemcen.dz/bitstream/112/1046/8/chapitre2, consulté le 09 Avril 2018.

[20] : http://www-igm.univ-mlv.fr/~dr/XPOSE2006/depail/fonctionnement.html, consulté le 09 Avril 2018.

[21] : Jean-François Carpentier, la sécurité informatique dans la petite entreprise, Edition ENI, France, décembre 2012.

[22] : https://medimagh.wordpress.com/quelle-est-la-difference-entre-un-proxy-et-un-firewall/, consulté le 06 Mai 2018.

[23] : http://alois.aubel.online.fr/form/admin/firewall/firewall3.html, consulté le 15 Mai 2018.

[24] : https://blog.devensys.com/aaa-authentication-authorization-accounting/, consulté le 06 Mai 2018.

[25] : F.MOUFFOK, les réseaux virtuels-VLAN.

[26] : http://www.guill.net/, consulté le 10 Mai 2018.

[27] : Pierre-Alain Goupille, Technologie des Ordinateurs et des réseaux, DUNOD 8ème édition, France, 2014.

[28] : https://www.memoireonline.com/04/10/3431/m_Etude-et-optimisation-du-reseau-local-de-inova-si6.html, consulté 11 Mai 2018.

[29] : https://fr.slideshare.net/SirineIbrahim/vlanspanning-tree, consulté 11Mai 2018.

[30] : http://mariepascal.delamare.free.fr/IMG/pdf/VLAN_CM.pdf, consulté 12 Mai 2018.

[31] : Jean-Pierre Arnaud, Réseaux et Télécoms, DUNOD 2ème édition, France, 2006.

[32] : http://docplayer.fr/1818454-Vlan-virtual-lan-introduction-ii-le-vlan-2-1-les-vlan-de-niveau-1-port-based-vlan.html, consulté le 15 Mai 2018.

[33] : Cours CISCO CCNA2, chapitre 3 VLAN, netacad, 2017.

[34] : http://docplayer.fr/30423599-Les-vlan-informatique-et-science-du-numerique.html, consulté le 15 Mai 2018.

[35] : Roger Sanchez, Les réseaux locaux virtuels, CERTA, janvier 2006.

[36] : Collectif, Dictionnaire Hachette encyclopédie illustré, Paris, Ed. Hachette livre, 1998.

[37] : Mise en place des réseaux LAN interconnectés en redondance par 2 réseaux WAN, Rapport de stage de perfectionnement 2011, université virtuelle de Tunis.

[38] : Laurent Schalkwijk et André Vaucamps, CISCO Routage et Commutation, édition ENI, France, Octobre 2015.

[39] : http://ekladata.com/YOxfOm0tNMwdX6BRIcH3tjdQluw/CONFIGURER-UN-SERVEUR-VPN-SOUS-WINDOWS-SEVEN, consulté le 20 Mai 2018.

[40] : http://igm.univ-mlv.fr/~duris/NTREZO/20032004/DeReynal-DeRorthais-Tan-VPN, consulté le 20 Mai 2018.

[41] : http://perso.modulonet.fr/placurie/Ressources/BTS2-AMSI/Chap-8Les%20VPN, consulté le 20 Mai 2018.

[42] :https://wapiti.telecomlille.fr/commun/ens/peda/options/st/rio/pub/exposes/exposesrio2001ttv02/Roudel_Maroc/index.htm

[43] : https://www.tala-informatique.fr/wiki/images/f/fb/Les_VPN, consulté le 25 Mai 2018.

[44] : W. Simpson, PPP Vendor Extensions, May 1997.

[45] : Ahmed ROUANE, Sécurité de réseau, Janvier 2010.

[46] : A. Valencia, M. Littlewood et T. Kolar, Cisco Layer Two Forwarding (Protocol) "L2F", May 1998.

[47] : Jean-Paul Archier, Les VPN Fonctionnement mise en œuvre et maintenance des réseaux privés virtuels, Editions ENI, France, Juin 2010.

[48] : W. Townsley et A. Valencia, Layer Two Tunneling Protocol "L2TP", Aout 1999.

[49] : Laurent Blochet et Christophe Wolfhugel, Sécurité informatique principes et méthode, Groupe EYROLLES, France, 2007.

Résumé

L’objectif de notre travail consiste à sécuriser le réseau de l’entreprise SCS en lui proposant des nouveaux mécanismes de sécurité. Durant la période de notre stage a la SCS, nous avons fait une étude approfondie sur la sécurité du réseau de l’entreprise, afin de relever les différentes insuffisances présentées, ainsi que, les failles de sécurité. Ensuite, nous avons proposé des solutions de sécurité basées sur les VLANs et les VPNs. Pour cela, nous commencerons d'abord par la segmentation de réseau local, à travers les VLANs dans lequel nous avons configuré les protocoles VTP, DHCP et les ACLs. A ce stade, nous avons pu sécuriser tous le réseau, mais notre but ne se limite pas au niveau local, ce qui fait la sécurité des trafics entrants et sortant aussi est très importante. Pour cela, nous avons opté pour la technologie VPNs, où nous avons configuré le protocole IPSec afin de sécuriser les tunnels de transmissions. Vers la fin et pour simuler notre travail, nous avons eu recours aux simulateurs de matériels réseaux CISCO Packet Tracer.

Mots clés : Sécurité, VLANs, VPNs, IPSec, SCS.

Abstract

The goal of our work is to secure the SCS network by providing new security mechanisms. During the period of our internship at SCS, we did a thorough study on the security of the network of the company, in order to identify the various deficiencies presented, as well as, the security flaws. Then we proposed security solutions based on VLANs and VPNs. For that, we will start first with LAN segmentation, through VLANs in which we have configured VTP, DHCP and ACLs. At this point, we have been able to secure all the network, but our goal is not limited to the local level, which makes the security of incoming and outgoing traffic is also very important. For this, we opted for VPNs technology, where we configured the IPSec protocol to secure transmission tunnels. Towards the end and to simulate our work, we used the CISCO Packet Tracer network hardware simulators.

Keywords : Security, VLANs, VPNs, IPSec, SCS.