République Algérienne Démocratique et Populaire Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de Fin de Cycle

En Vue de L'obtention du Diplôme Master Professionnelle
En Informatique

Option
Administration et Sécurité des Réseaux

Théme

Etude et configuration de liaisons virtuelles (VLAN et VPN) au sein de l'Entreprise Portuaire de Bejaia "EPB".

Présenté par : **Mlle NEDJADI Yamina**
Mlle TIMERIDJINE Nadjette

Devant le jury composé de :

Président	**Mr BOUKERRAM Abdellah**	**Professeur**	**U. Béjaia.**
Rapporteur	**Mme AIT KACI AZZOU Samira**	**MAA**	**U. Béjaia.**
Examinatrice	**Mme KOUICEM Amel**	**MAA**	**U. Bejaia.**

Promotion 2015/2016 .

Remerciements

En préambule à ce mémoire nous souhaitons adresser nos remerciements les plus sincères aux personnes qui nous ont apportées leur aide et qui ont contribuées à l'élaboration de ce mémoire ainsi qu'à la réussite de cette année universitaire.

Nous tenons à remercier sincèrement Madame AIT KACI AZZOU Samira, qui s'est toujours montrés à l'écoute, sans oublier les membres de la commission du jury qui évaluerons notre travail.

Nos remerciements s'adressent particulièrement à Monsieur BETTACHE Idir pour son encouragement et précieux conseils.

Nous tenons à remercier également Monsieur MOHAMMEDI Mohamed et Monsieur MEKHOUKHE Fares pour leurs aides.

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

Dédicace

Je dédie ce modeste travail :
À ceux qui ont donné un sens à mon existence , en m'offrant une éducation digne de confiance ; à vos mes très chers parents
À mes frères et soeurs : pour tous leurs encouragements
À ma binôme ***Yamina*** avec qui j'ai partagé de belles années d'études.
À ma très chère amie **Nassima**.
À mon chèr ami **Adel**
À mes amies
Et toute personne que je connais et qui me sont chers et tous ceux qui m'aiment. . .

Nadjette

Je dédie ce modeste travail :
À mes chers parents
À mon mari **Bachir** et mon cher fils **Amine Billal**
À ma sœur **Ryane** et mes frères
Sans oublier particulièrement ma binôme ***Nadjette***
votre affection et votre soutien m'ont été d'un grand secours tout au long de mon parcours.
Je vous remercie du fond du coeur d'être toujours à mes cotés et de me donner cette force pour continuer. Je vous dédie ce travail en signe de reconnaissance.

Yamina

Table des matières

Table des figures

Liste des abréviations

ACL	**A**ccess **C**ontrol **L**ist
AH	**A**uthentication **H**eader
CIDR	**C**lassless **I**nter **D**omain **R**outing
DHCP	**D**ynamic **H**ost **C**onfiguration **P**rotocol
EPB	**E**ntreprise **p**ortuaire de **B**ejaia
ESP	**E**ncapsulating **S**ecurity **p**ayload
HTTP	**H**yper **T**ext **T**ransfer **P**rotocol
HDLC	**H**igh **D**ata **L**evel **C**ontrol
IKE	**I**nternet **K**ey **E**xchange
IP	**I**nternet **P**rotocol
IPSec	**I**nternet **P**rotocol **S**ecurity
IPX	**I**nter-network **P**rotocol e**X**change
ISO	**I**nternational **S**tandards **O**rganization
LAN	**L**ocal **A**rea **N**etwork
L2F	**L**ayer **T**wo **F**orwarding
L2TP	**L**ayer **T**wo **T**unneling **P**rotocol
MAC	**M**edia **A**ccess **C**ontrol
MAN	**M**etropolitan **A**rea **N**etwork
MYSQL	**M**y **S**tructured **Q**uery **L**anguage
NAT	**N**etwork **A**ddress **T**ranslation
OSI	**O**pen **S**ystems **I**nterconnection
PING	**P**acket **I**nternet **G**roper
PHP	**H**ypertext **P**reprocessor
PPP	**P**oint to **P**oint **P**rotocol
PPTP	**P**oint to **P**oint **T**unneling **P**rotocol
QoS	**Q**uality **o**f **S**ervice
RFC	**R**equest **F**or **C**omments
RIP	**R**outing **I**nformation **P**rotocol
RN	**R**évision **N**umber
SMTP	**S**imple **M**ail **T**ransfer **P**rotocol
TCP	**T**ransport **L**ayer **P**rotocol

TCP/IP	**T**ransmission **C**ontrol **P**rotocol/ **I**nternet **P**rotocol
VLAN	**V**irtual **L**ocal **A**rea **N**etwork
VTP	**V**irtual **T**runking **P**rotocol
VPN	**V**irtual **P**rivate **N**etwork
WAN	**W**ide **A**rea **N**etwork
WiMAX	**W**orldwide **I**nteroperability for **M**icrowave **A**ccess

Liste des tableaux

Introduction générale

Les réseaux Informatiques sont devenus essentiels à la bonne marche des entreprises. La croissance accélérée de ces réseaux qui sont de plus en plus ouverts sur Internet, est à priori bénéfique, mais pose néanmoins un problème important de sécurité. En effet, il en résulte un nombre croissant d'attaques qui peuvent aboutir à de graves conséquences professionnelles et financières en menaçant l'intégrité, la confidentialité et la disponibilité de l'information. De nombreuses entreprises ont déjà compris l'importance de ces enjeux, ce qui les a poussées à émerger dans le domaine de la sécurité Informatique.

La sécurité se place actuellement au premier plan de la mise en œuvre et de l'administration des réseaux Informatique. La difficulté que représente la sécurité dans son ensemble, est de pouvoir trouver un compromis entre deux besoins essentiels : le besoin d'ouverture des réseaux afin de profiter des différentes fonctionnalités offertes et le besoin de protection des informations. L'application d'une stratégie de sécurité efficace est l'étape la plus importante qu'une entreprise doit franchir pour protéger son réseau. Les outils classiques offrants des solutions de sécurité minimum (authentification par login et mot de passe, installation d'un anti-virus, etc.) se révèlent utiles mais dans la plupart des cas, insuffisantes. Aucune personne n'ignore l'importance de l'information dans une institution qui nécessite l'organisation, la fiabilité et le bon fonctionnement du système d'information.

Les nouvelles technologies de l'information et de la communication, nous introduisent dans un siècle de vitesse tout en offrant de nouvelles perspectives en ce qui concerne la communication de l'information au sein de nos organisations. Même si la sécurité Informatique ne se limite pas à celle du réseau, il est indéniable que la plupart des incidents de sécurité surviennent par les réseaux, et vise ces derniers.

L'objectif de notre projet consiste donc à implémenter des mécanismes et des solutions sûres en utilisant les liaisons virtuelles(VLAN et VPN), permet-

tant de garantir une meilleure exploitation et attribution du réseau. Ainsi, assurer une communication sûre et confidentielle entre les utilisateurs au sein de l'entreprise.

Ce mémoire est subdivisé en quatre chapitres, comme suit :

Le premier chapitre sera consacré à la présentation des généralités sur les réseaux Informatiques, en décrivant les types de réseau ainsi que ses modèles et l'adressage IP.

Le deuxième chapitre sera une synthèse de l'état de l'art sur la sécurité des réseaux informatiques et les différents outils et techniques de sécurisation.

Le troisième chapitre est dédié à la présentation de l'organisme d'accueil EPB (Entreprise portuaire de Bejaia) et l'étude effectuée durant notre stage au sein de ce dernier.

Le quatrième chapitre décrit la partie pratique de notre stage, dans lequel nous allons présenter l'environnement de travail ainsi que la mise en œuvre des VLANs (Virtual LANs) et des VPNs (Virtual Private Networks).

Enfin, notre mémoire s'achève par une conclusion générale résumant les connaissances acquises durant la réalisation du projet ainsi que quelques perspectives.

Chapitre 1

Etat de l'art sur les réseaux informatiques

1.1 Introduction

Ce chapitre a pour objectif de comprendre les notions de bases sur les réseaux informatiques, afin de bien maitriser notre sujet.

Un réseau informatique *(network)* est un regroupement d'ordinateurs et d'équipements interconnectés entre eux, permettant la communication et le partage de différents éléments *(des fichiers, des imprimantes...)* entre différents stations relies, comme il permet aussi l'accès à distance aux bases de données.

1.2 Types de réseaux

1.2.1 Réseaux locaux *(LANs)*

Un réseau local *(Local Area Network)* est une infrastructure de communication, reliant des équipements informatiques et permettant de partager des ressources communes dans une aire géographique limitée à quelques centaines de mètres à l'aide d'un support de transmission.

L'objectif d'un réseau local dans une entreprise est de répondre à certain nombre de questions spécifiques aux équipements à interconnecter et aux applications à supporter**[19]**.

1.2.2 Réseaux étendus *(WAN)*

Les réseaux étendus *(Wide Area Network)* interconnectent des réseaux locaux, qui à leur tour, donnent accès aux ordinateurs ou aux serveurs de fichiers situés en d'autres lieux. Comme les réseaux étendus relient des réseaux utilisateurs géographiquement dispersés, ils permettent aux entreprises de communiquer entre elles sur de grandes distances. Les réseaux étendus permettent le partage d'ordinateurs, imprimantes et autres équipements raccordés à un LAN situé sur un lieu distant. Les réseaux étendus fournissent des communications instantanées à l'intérieur de grandes zones géographiques**[19]**.

1.2.3 Réseaux métropolitains *(MAN)*

Un réseau MAN *(Métropolitain Area Network)* est un réseau qui s'étend à une zone métropolitaine telle qu'une ville. Un réseau MAN comprend habituellement au moins deux réseaux LAN situés dans une zone géographique commune. Par exemple, une banque possédant plusieurs agences peut utiliser ce type de réseau**[19]**.

1.3 Modèles de réseaux

Il existe deux types de modèle de réseau de base : le modèle de référence et le modèle d'applications**[4]**.

1.3.1 Modèle OSI *(Open System Interconnection)*

Le modèle OSI est un modèle conceptuel. Il a pour but d'analyser la communication en découpant les différentes étapes en 7 couches, chacune de ces couches remplissant une tâche bien spécifique. Afin de connaitre les services de chaque couches on va les présenter ci-dessous l'une après l'autre :

1. **Couche Physique**

   Fournit les moyens mécaniques, optiques, électroniques, fonctionnels et procéduraux nécessaires à l'activation, au maintien et à la désactivation des connexions physiques nécessaires à la transmission des bits. Les systèmes sont interconnectés réellement au moyen de supports physiques de communication. Ces derniers ne font pas partie de la couche Physique.

2. **Couche Liaison de données**

   Assure la transmission d'informations entre deux ou plusieurs systèmes immédiatement adjacents. Détecte et corrige, dans la mesure du possible, les erreurs issues de la couche inférieure. Les objets échangés sont souvent appelés trames.

3. **Couche Réseau**

   Achemine les informations à travers un réseau pouvant être constitué de systèmes intermédiaires *(routeurs)*. Les objets échangés sont souvent appelés paquets.

4. **Couche Transport**

   Assure une transmission de bout en bout des données. Maintient une certaine qualité de la transmission, notamment vis-à-vis de la fiabilité et de l'optimisation de l'utilisation des ressources. Les objets échangés sont souvent appelés messages.

5. **Couche Session**

   Fournit aux entités coopérantes les moyens nécessaires pour synchroniser leurs dialogues, les interrompre ou les reprendre tout en assurant la cohérence des données échangées.

6. **Couche Présentation**

   Spécifie les formats des données des applications(compression, encryptions,etc).

7. **Couche Application**

   Donne aux processus d'application les moyens d'accéder à l'environnement de communication de l'OSI. Comporte de nombreux protocoles adaptés aux différentes classes d'application.

1.3.2 Le modèle TCP/IP

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

1. **Couche application**

   Le modèle TCP/IP regroupe en une seule couche tous les aspects liés aux applications et suppose que les données sont préparées de manière adéquate pour la couche suivante.

2. **Couche transport**

   La couche transport est chargée des questions de qualité de service touchant la fiabilité, le contrôle de flux et la correction des erreurs. L'un de ses protocoles TCP, fournit d'excellents moyens de créer avec souplesse, des communications réseau fiables.

3. **Couche Internet**

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

4. **Accès Réseau**

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

La figure suivante montre la correspondance entre le modèle OSI et TCP/IP

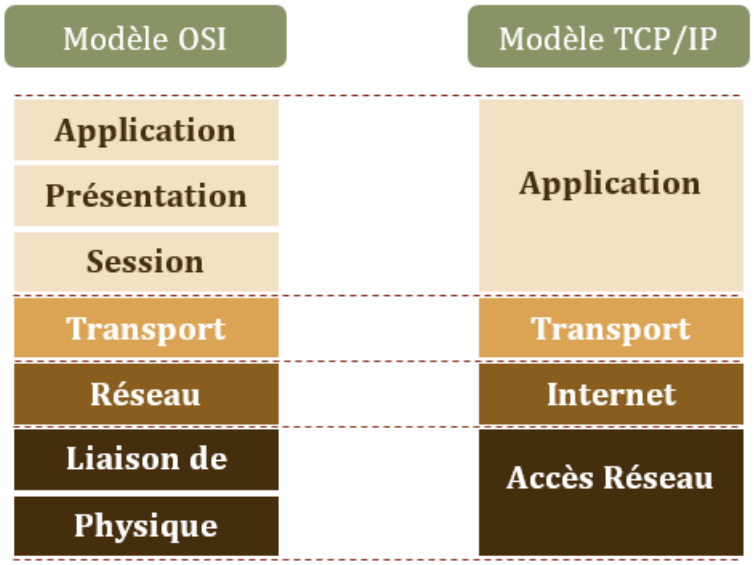


FIGURE 1.1 – *Comparaison entre les couches du modèle OSI et TCP/IP .*

1.3.3 Equipements de base d'un réseau informatique

• **Répéteur :** dispositif permettant d'étendre la distance de câblage d'un réseau local. Il amplifie et répète les signaux qui lui parviennent

• **Routeur :** Un routeur *(router)* est un dispositif permettant de relier des réseaux locaux de telle façon à permettre la circulation de données d'un réseau à un autre de façon optimale.

• **Passerelle :** Une passerelle *(Gateway)* est un dispositif permettant d'interconnecter des architectures de réseaux différentes. Elle assure la traduction d'un protocole d'un haut niveau vers un autre.

• **Concentrateur :** Un concentrateur *(hub)* est un dispositif permettant de connecter divers éléments de réseau.

• **Commutateur :** Un commutateur *(Switch)* est un dispositif permettant de relier divers éléments tout en segmentant le réseau.

• **Adaptateur :** Un adaptateur *(adapter)* est destiné à être insérés dans un poste de travail ou un serveur afin de les connecter à un système de câblage[14].

1.4 L'adressage IP

1.4.1 Le protocole IP

Le protocole IP *(Internet Protocol)* s'agit d'un protocole réseau de niveau trois, ce protocole permet d'émettre des paquets d'informations à travers le réseau, il est utilisé pour dialoguer les machines entre elles. Ainsi, il offre un service d'adressage unique pour l'ensemble des machines. Il n'est pas orienté connexion, c'est à dire qu'il n'est pas fiable Cela ne signifie pas qu'ils n'envoient pas correctement les données sur le réseau, mais qu'ils n'offrent aucune garantie pour les paquets envoyés sur l'ordre d'arrivée et la perte ou la destruction des paquets, cette fiabilité dépend de la couche de transport**[5]**.

1.4.2 Le format des adresses IP

Il existe deux formats d'adresse IP : Le format IPV4 et le format IPV6

1. **Le format IPV4 :** C'est une adresse de 32 bits, répartie en 4 fois 8 bits *(octet)*. Cette adresse est un identifiant réseau qu'on peut diviser en 2 portions : la portion du réseau et la portion hôte. La première identifie le réseau sur lequel est la machine et la deuxième identifie les machines en elles-mêmes. Pour identifier ces deux parties chaque adresse est liée à un masque de sous-réseau ce qui permet de définir sur quel réseau elle se trouve.
   Le format binaire d'une adresse IP est comme suit :
   xxxxxxxx . xxxxxxxx .xxxxxxxx. xxxxxxxx *(tel que x=0 ou x=1).*

   • **Le masque réseau** Le masque de réseau sert à séparer les parties réseau et hôtes d'une adresse. On retrouve l'adresse du réseau on effectuant un ET logique bit à bit entre une adresse complète et le masque du réseau.

   • **Les classes des adresses IP** Le but de la division des adresses IP en classes, est de facilité 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.

En effet, il existe 5 classes des adresses IP, à savoir : classe A, classe B, classe C, classe D et classe E, telle que, chaque classe a un format spécial de son adresse IP. « Adresse réseau et Adresse machine».

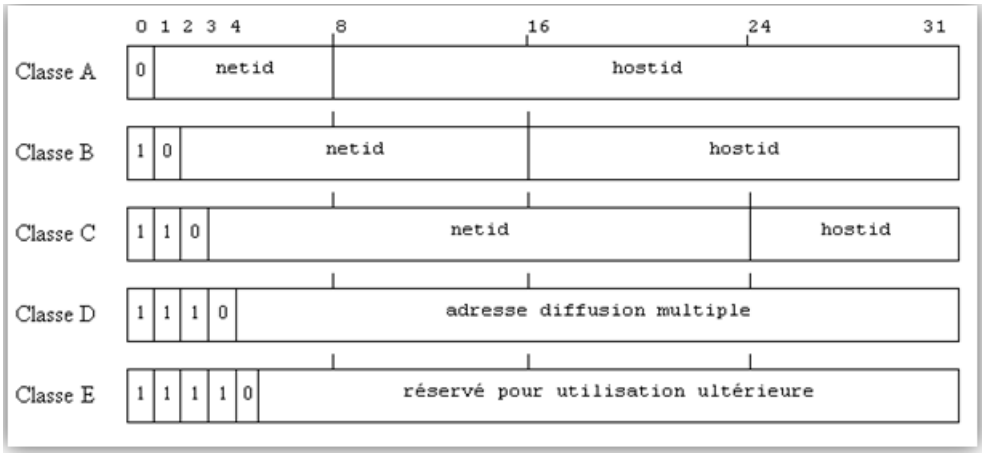


FIGURE 1.2 – *Caractéristiques des classes des adresses IP.*

- **Adresses Spécifiques**

Dans l'ensemble des adresses IP, il existe certaines adresses qui sont spécifiques, c'est- à-dire, qu'elles ont un usage particulier. Parmi ces adresses, citant : Les adresses privées et les adresses de diffusion.

- **Adresse privée**

Il existe des adresses privées, dans chaque classe :
— A –> 10.0.0.0 à 10.255.255.255
— B –> 172.16.0.0 à 172.31.255.255
— C –> 192.168.0.0 à 192.168.255.255

Une adresse IP privée n'est pas visible sur internet, au contraire d'une IP publique. On emploie les adresses privées à l'intérieur du réseau et les adresses publiques sont des adresses internet.

- **Adresse de diffusion**

L'adresse de diffusion est utilisée pour envoyer un message à toutes les machines d'un réseau. Elle est obtenue en mettant tous les bits de l'host-id à 1. Il existe aussi l'adresse de Broadcast " générale ", cette adresse permet l'envoi d'un message vers toutes les machines de tous les réseaux connectés. Le routeur quand il reçoit une adresse de Broadcast, va envoyer le message dans tous les périphériques du réseau concerné**[5]**.

2. **Format IPV6 :** Une adresse IPv6 est longue de 128 bits, soit 16 octets, c'est une notation hexadécimale, où les 8 groupes de 2 octets *(16 bits par groupe)* sont séparés par un signe deux-points « : » **[5]**. Exemple : 2001 : 0db8 : 0000 : 85a3 : 0000 : 0000 : ac1f : 8001

Dans une adresse IPv6, une unique suite de un ou plusieurs groupes consécutifs de 16 bits tous nuls peut être omise, en conservant toutefois les signes deux-points de chaque côté de la suite de chiffres omise, c'est-à-dire une paire de deux points « : : ».

Les réseaux sont notés en utilisant la notation CIDR *(Classless Inter-Domain Routing)* : la première adresse du réseau est suivie par une barre oblique et un nombre qui indique la taille en bits du réseau. La partie commune des adresses est appelée préfixe. Par exemple :

- Le préfixe 2001 : db8 : 1f89 : : /48 représente l'ensemble des adresses qui commence à 2001 : db8 : 1f89 : 0 : 0 : 0 : 0 : 0 et finit à 2001 : db8 : 1f89 : ffff : ffff : ffff : ffff : ffff.

- **Type d'adresses IPv6**

Certains préfixes d'adresses IPv6 jouent des rôles particuliers :

Préfixe	**Description**
: :/8	Adresses réservées
2000 : : /3	Adresses unicast routables sur Internet
fc00 : : /7	Adresses locales uniques
fe80 : : /10	Adresses locales lien
ff00 : : /8	Adresses multicast

TABLE 1.1 – Type d'adresses IPv6.

1.5 conclusion

Au cours de ce chapitre, nous avons parcouru des généralités sur les réseaux informatiques en soulignant leur importance, 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 Protocoles, les services offerts par ces derniers ainsi que l'adressage et ses classes.

Chapitre 2

Sécurité des réseaux informatiques

2.1 Introduction

La sécurité des réseaux informatiques, est devenue un enjeu majeur du fait de la rapidité des évolutions technologiques et de l'augmentation des risques qui en résulte.

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système, contre les menaces accidentelles ou intentionnelles. D'une manière générale, elle consiste à assurer que les ressources matérielles ou logicielles d'une organisation soient uniquement utilisées dans le cadre prévu.

2.2 Enjeux de la sécurité des réseaux informatiques

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

- **confidentialité :** La protection de données émises sur le réseau, de façon à ce qu'elles ne soient compréhensibles que par des entités autorisées.
- **authentification :** garantir que les données reçues proviennent bien de l'entité émettrice.
- **intégrité :** s'assurer que les données reçues n'ont subi aucune modification lors du transport dans le réseau.

• **non-répudiation :** Constitue un moyen efficace pour identifier l'auteur d'une transaction et d'assurer la preuve de l'authenticité de cette dernière[2].

2.3 Menaces sur les systèmes informatiques

Dans un système informatique, les menaces peuvent toucher les composantes matérielles, logicielles ou informationnelles. Il existe principalement deux types de menaces **[18]** :

• Les menaces accidentelles *(non-intentionnelles).*

•Les menaces intentionnelles *(Passive - Active).*

2.3.1 Menaces accidentelles *(non- intentionnelles)*

Les menaces accidentelles ne supportent aucune préméditation. Dans cette catégorie sont repris les bugs logiciels et les pannes matérielles et autres défaillances incontrôlables.

2.3.2 Menaces intentionnelles

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 les menaces passives et les menaces actives.

1. **attaque passive**
   C'est une méthode qui se base sur l'écoute du réseau à l'aide de sniffeurs : *(analyseurs du trafic réseau)*, elle consiste au détournement des données et des logiciels sans modifier le fonctionnement du réseau. Exemple : Espionnage industriel et commercial, copies illicites de logiciels.
2. **attaque active**
   Cette attaque consiste à modifier des données, à se glisser dans des équipements réseaux ou à perturber le bon fonctionnement de ce réseau. Exemple : virus, ver).

2.4 Quelques solutions de sécurité

2.4.1 Solutions de sécurité primaire

C'est l'ensemble des mesures offrant le minimum en matière de sécurité**[9]**

• Authentification des utilisateurs par login et mot de passe.

• Suppression des informations confidentielles des machines reliées au réseau si elles n'ont pas besoin d'y être.

• Protection physique des machines contenant des informations sensibles.

• Installation d'un logiciel anti-virus mit à jour.

2.4.2 Firewall et Proxy

Le firewall et le serveur proxy sont deux méthodes conçues afin d'éviter les attaques provenant d'internet par le routeur. Elles opèrent en effectuant une isolation du réseau interne d'une organisation.

1. **firewall *(pare-feu)* :** Un système permettant de protéger un ordinateur ou un réseau d'ordinateurs, des intrusions provenant d'un réseau tiers *(notamment Internet)*. Il s'agit d'une passerelle qui opère en filtrant les paquets de données échangés avec le réseau.
2. **serveur Proxy *(serveur mandataire)* :** Un intermédiaire entre les ordinateurs d'un réseau local et Internet. Utilisé la plus part du temps par le web, il s'agit alors d'un proxy HTTP qui permet :

    • D'accélérer la navigation : mémoire cache, compression de données, filtrage des publicités ou des contenus lourds.

    • La journalisation des requêtes *(logging)*.

    • La sécurité du réseau local.

    • Le filtrage et l'anonymat **[3]**.

2.4.3 Cryptographie

La cryptographie est l'étude de méthodes de chiffrement et de déchiffrement. Elle permet d'assurer l'authenticité, l'intégrité et la confidentialité des données.

1. **Cryptographie symétrique :** Elle est basée sur une clé unique partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypter les messages.
2. **Cryptographie asymétrique *(à clé publique)* :** Contrairement à la cryptographie symétrique, la cryptographie asymétrique utilise deux clés : une est privée et n'est connue que par l'utilisateur, l'autre est publique et donc accessible par tout le monde. **[10]**.

2.4.4 VLAN *(Virtual Local Area Network)*

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

En effet, dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels, il est possible de s'affranchir des limitations de l'architecture physique *(contraintes géographiques, contraintes d'adressage, etc.)* en définissant une segmentation logique *(logicielle)* basée sur un regroupement de machines grâce à des critères *(adresses MAC, numéros de port, protocole, etc.)*, Ces derniers permettent d'identifier les différents types de VLAN **[23]**.

1. **Types de VLAN**

Nous pouvons distinguer trois types de VLANs **[15]** :

- **VLAN de niveau 1*(par port)* :** Le réseau local virtuel est défini en fonction des ports du commutateur *(voir Figure 2.1)*. Un inconvénient majeur est que si une station se déplaçe cela implique une modification de la configuration du port auquel elle était associée et du port auquel elle s'associe.

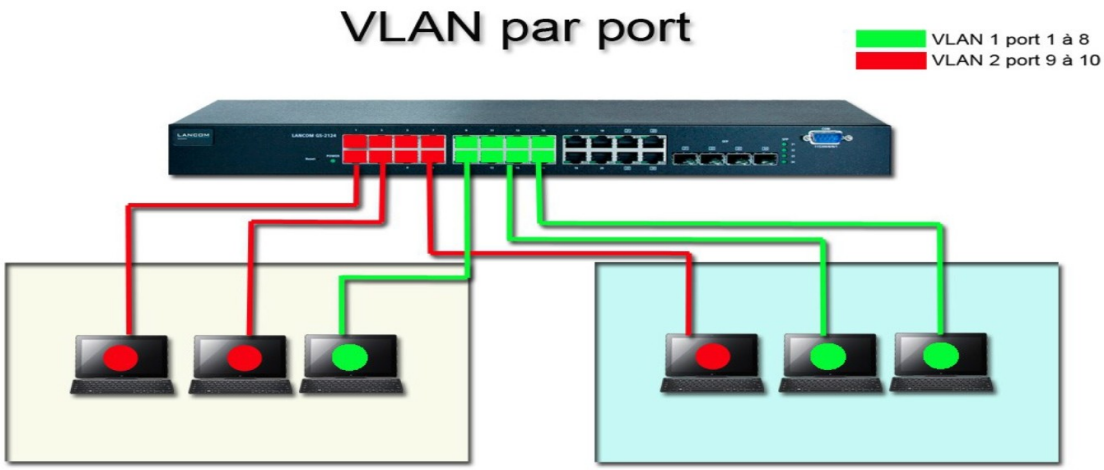


FIGURE 2.1 – *VLAN par port.*

• **VLAN de niveau 2** ***(par adresse MAC)*** **:** Dans ce cas, ce sont les adresses MAC des machines qui permettent de déterminer leur appartenance au VLAN. L'identification des machines par leurs adresses MAC uniques, permet de rendre leur appartenance au VLAN indépendante de leur emplacement.

Host MAC Adddres	**VLAN**
00 00 80 45 FE 21	VLAN2
00 00 80 45 DA 45	VLAN2
00 40 00 80 FE	VLAN3
00 40 10 AA 21	VLAN3
00 80 00 FF AB	VLAN24

TABLE 2.1 – Table de correspondance adresse MAC/VLAN d'un Switch.

• **VLAN de niveau 3 :** Nous en distinguons :

— Par sous-réseau : Le VLAN par sous-réseau permet de regrouper plusieurs machines suivant le sous-réseau au quel elles appartiennent. Pour créer un tel VLAN, il faut associer une adresse de sous-réseau à un VLAN *(voir Figure 2.2).*

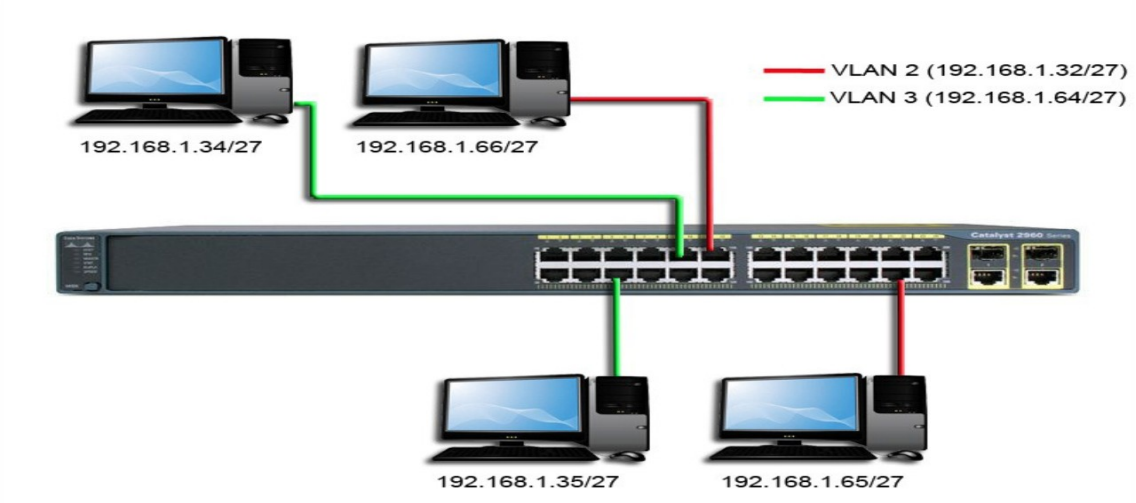


FIGURE 2.2 – *VLAN par sous-réseau (adresse IP).*

— Par protocole : Permet de créer un réseau virtuel par type de protocole, regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau. Example : HTTP → VLAN 2, SMTP → VLAN 3...

2. **Avantages du VLAN**

Parmi les avantages liés à la mise en œuvre d'un VLAN, on retiendra notamment**[6]** :

— La flexibilité de segmentation du réseau.
— La simplification de la gestion.
— L'augmentation considérable des performances du réseau.
— Le renforcement de la sécurité.
— La technologie évolutive et à faible coût.
— La régulation de la bande passante.

3. **Protocoles de transport des VLANs**

•**VTP *(Virtual Trunking Protocol)***

C'est un protocole de niveau 2, utilisé pour configurer et administrer les VLANs sur les périphériques CISCO. VTP permet d'ajouter, renommer ou supprimer, un ou plusieurs réseaux locaux virtuels sur un seul commutateur qui propagera cette

nouvelle configuration à l'ensemble des autres commutateurs du réseau. VTP permet ainsi d'éviter toute incohérence de configuration de VLANs sur l'ensemble d'un réseau local**[7]**.

— **Fonctionnement[22]**

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

- **VTP Server :** le switch en mode Server *(mode par défaut)*, permet à l'administrateur de faire des modifications sur les VLANs et de les propager automatiquement vers tous les switchs du réseau.

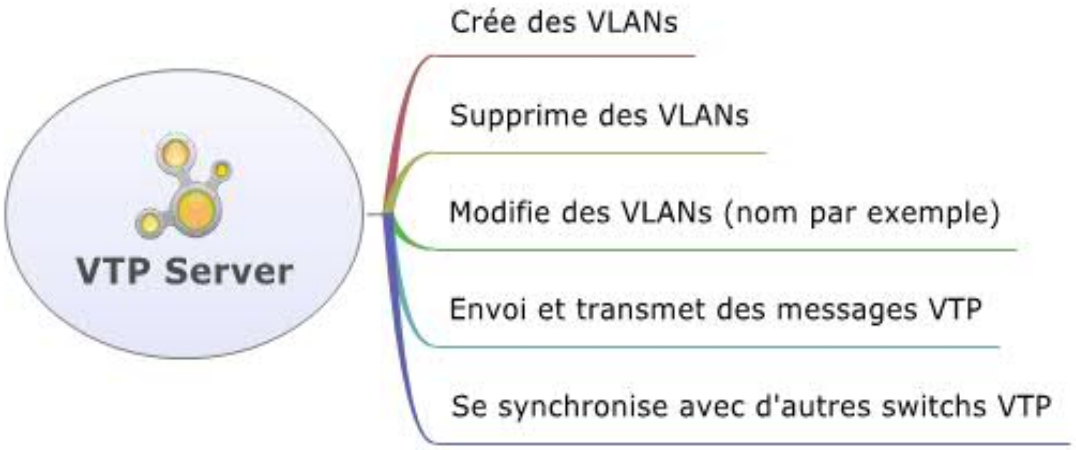


FIGURE 2.3 – *VTP Server.*

- **VTP Client :** Le switch en mode Client reçoit les mises à jour, les prend en charge, les transmet, mais ne permet pas à l'administrateur de faire des modifications sur les VLANs.

FIGURE 2.4 – *VTP Client..*

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

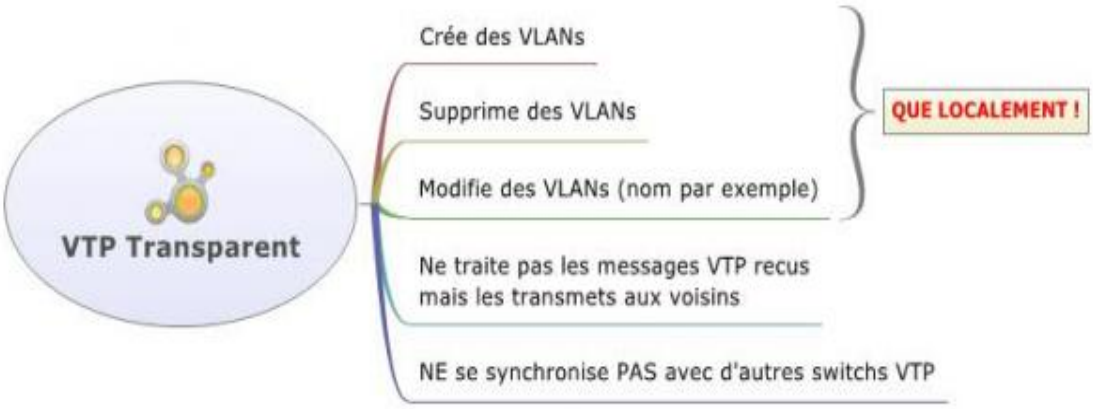


FIGURE 2.5 – *VTP Transparent..*

•Trunk

Le trunk est le mécanisme qui permet d'insérer l'identifiant du VLAN sur une trame utilisateur. Toute trame se propageant sur plusieurs switchs conservera toujours l'information de son appartenance à son VLAN. Et le switch de destination saura avec quels ports la trame peut être commutée *(ports appartenant au même VLAN)* **[12]**.

Le trunk peut être utilisés :

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

2.4.5 VPN *(Virtual Private Network)*

1. **Définition**

Un VPN repose sur un 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 **[26]**.

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 et 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.

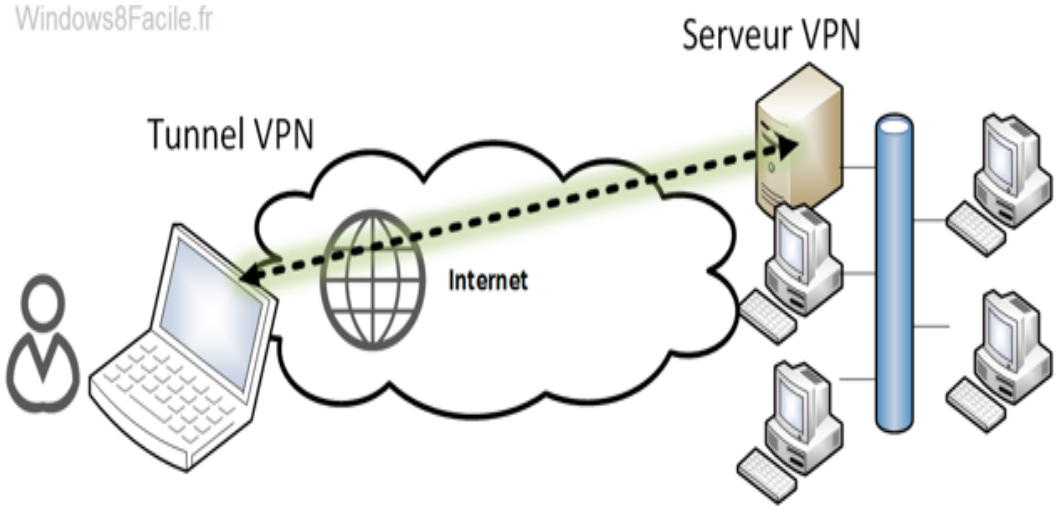


FIGURE 2.6 – *Schéma d'un réseau VPN.*

2. **Différents types de réseau VPN**

•**Site à site *(LAN to LAN)* :** Le site à site permet de relier deux réseaux de façon transparente. Généralement les deux sites ont des tranches IP différentes ce qui oblige les postes clients à passer par le routeur. Celui-ci est directement relié à l'équipement responsable du VPN ou implante directement les protocoles choisit pour la mise en place du VPN**[20]**.

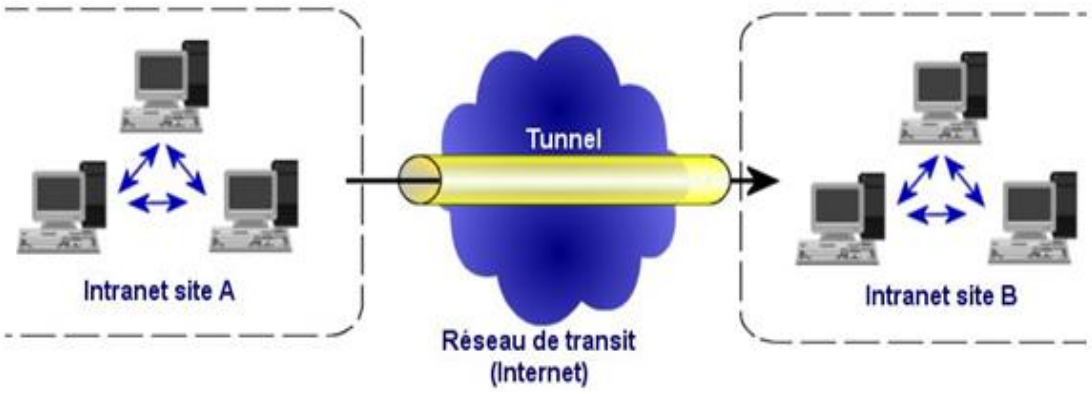


FIGURE 2.7 – *Architecture d'un VPN Site à Site.*

•**Poste à Site *(Host to LAN)* :** Il existe le type nomade, également appelé "Road Warrior *(chemin de guerrier)*" qui permet à un utilisateur distant de son entreprise de se connecter à celle-ci pour pouvoir profiter de ses services. Ainsi, il pourra lire ses mails, récupérer des fichiers présents sur le réseau de son entreprise**[20]**.

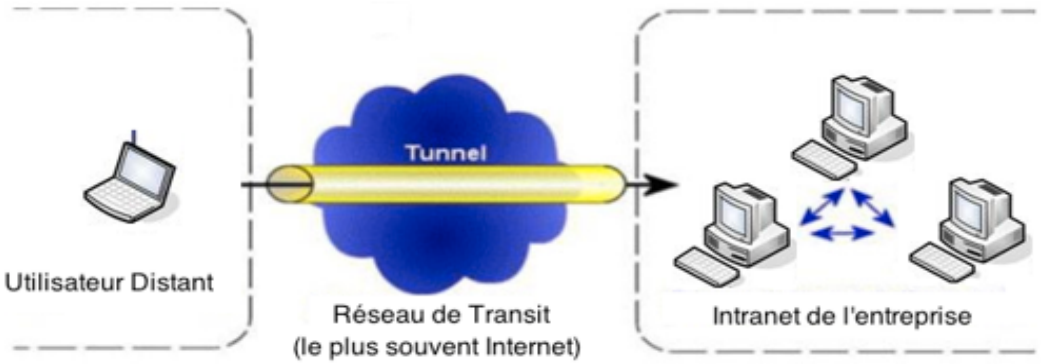


FIGURE 2.8 – *Architecture d'un VPN poste à site.*

•**Poste à poste *(Host to Host)* :** Dans ce cas de figure, on veut connecter deux ordinateurs distants entre eux pour des raisons de confidentialité. On crée donc un VPN entre eux, et toutes les données y transmises sont encryptées et compréhensibles que par les deux paires correspondantes**[20]**.

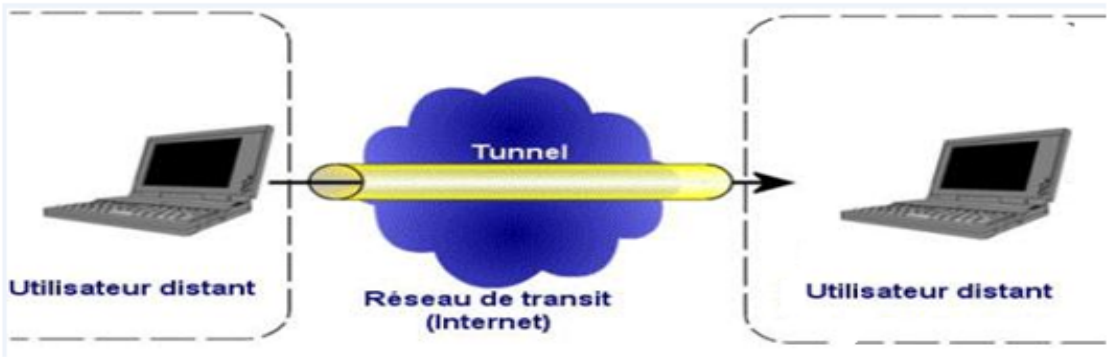


FIGURE 2.9 – *Architecture d'un VPN entre deux hôtes.*

3. **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 :

— Les connexions VPN offrent un accès au réseau local à distance et de façon sécurisée.
— Elles permettent d'administrer efficacement et de manière sécurisé 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 sécurisés entre une machine locale et une machine distante**[21]**.

4. **Principaux protocoles de VPN**

Il existe plusieurs protocoles dits de « tunnelisation » qui permettent la création des réseaux VPN, notamment :

•**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 cers 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.

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**[17]**.

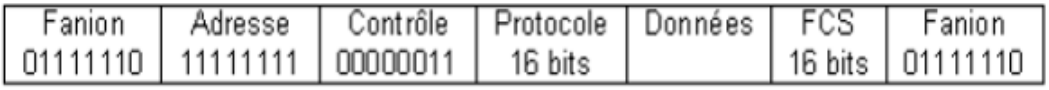


FIGURE 2.10 – *Format d'une trame PPP.*

Une connexion PPP est composée principalement de 3 parties :

— Une méthode d'encapsulation des datagrammes sur la liaison série .PPP utilise le format de trame HDLC *(high data level control)* de l'ISO.
— Un protocole de contrôle de liaison *(LCP-link control Protocol)* pour établir, configurer et tester la connexion de liaisons de données.
— Plusieurs protocoles de contrôle de réseaux *(NCP-network control protocol)* pour établir et configurer les différents protocoles de couche réseau.

•**PPTP *(Point To Point Tunneling Protocol)* :** Est un protocole réseau *(de niveau 2)* permettant un transfert sécurisé entre un client distant et un serveur privé. Il permet la création de VPN sur demande à travers des réseaux basés sur TCP/IP. Il peut de même être utilisé pour créer VPN entre deux ordinateurs dans le même réseau local.

PPTP est un protocole qui encapsule les paquets PPP dans des datagrammes IP pour la transmission sur internet ou un autre réseau public basé sur IP. Il peut même être utilisé pour des liaisons Site à Site. Une trame PPP *(un datagramme IP ou IPX ou Appletalk)* est encapsulée dans un en-tête GRE *(Generic Routing Encapsulation)* et un en-tête IP. L'en-tête IP contient les adresses IP sources et de destination qui correspondent respectivement au client et au serveur VPN**[16]**.

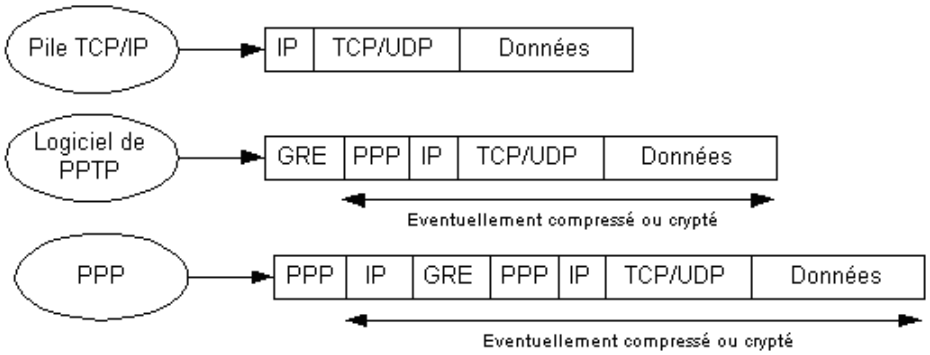


FIGURE 2.11 – *Format d'une trame PPTP.*

•**L2F** ***(Layer Two Forwarding)*** **:** Est un protocole de niveau 2, qui permet à un serveur d'accès distant de véhiculer le trafic sur PPP et transférer ces données jusqu'à un serveur L2F. Ce serveur dés-encapsule les paquets et les envoie sur le réseau,L2F est progressivement remplacé par L2TP qui est plus souple **[25]**.

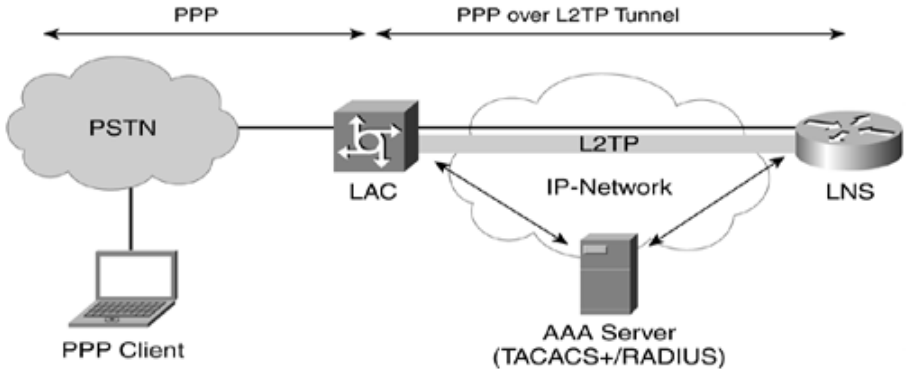


FIGURE 2.12 – *Tunnel L2F*

•**L2TP** ***(Layer Two Tunneling Protocol)*** **:** C'est un protocole de niveau 2, on peut accéder à un réseau privé par l'intermédiaire d'Internet ou d'un autre réseau public au moyen d'une connexion à un VPN utilisant le L2TP. Ce dernier est un protocole de tunneling standard qui possède pratiquement les mêmes fonctionnalités que le protocole PPTP**[8]**.

•**IPSec *(Internet Protocol Security)* :** Est un protocole fournissant un mécanisme de sécurisation au niveau de la couche réseau du modèle OSI. Il assure la confidentialité , l'authentification et l'intégrité des données. IPSec permet de protéger les données et également l'en-tête d'une trame, en masquant le plan d'adressage grâce à l'ajout d'un en-tête IPSec à chaque datagramme IP.

IPSec est soutenu par deux protocoles de sécurité *(AH et ESP)* et un protocole de gestion *(IKE)***[13].**

- AH *(Authentication Header)*, est employé pour assurer l'authentification des machines aux deux extrémités du tunnel. Il permet aussi de vérifier l'unicité des données grâce à l'attribution d'un numéro de séquence ainsi que l'intégrité de celles-ci a l'aide d'un code de vérification des données *(Integrity Check Value)*.
- ESP *(Encapsulating Security Payload)*, répond, quant à lui, au besoin de crypter les données. Il peut toutefois aussi gérer l'authentification et la vérification de l'intégrité mais de manière moins poussée que le AH.
- IKE *(Internet Key Exchange)*, IKE négocie les algorithmes cryptographiques et les paramètres relatifs destinés à AH et ESP.

Les normes IPsec définissent deux modes distincts d'opération IPsec : le mode Transport et le mode Tunnel**[11]** :

- Le mode Transport, récupère les données provenant de la couche 4 *(TCP/transport)*, les authentifie et les chiffre puis enfin les envoie à la couche 3 *(IP/réseau)*.
- Le mode Tunnel, est généralement utilisé quand on veut relier un site à un autre *(de passerelle à passerelle)*.

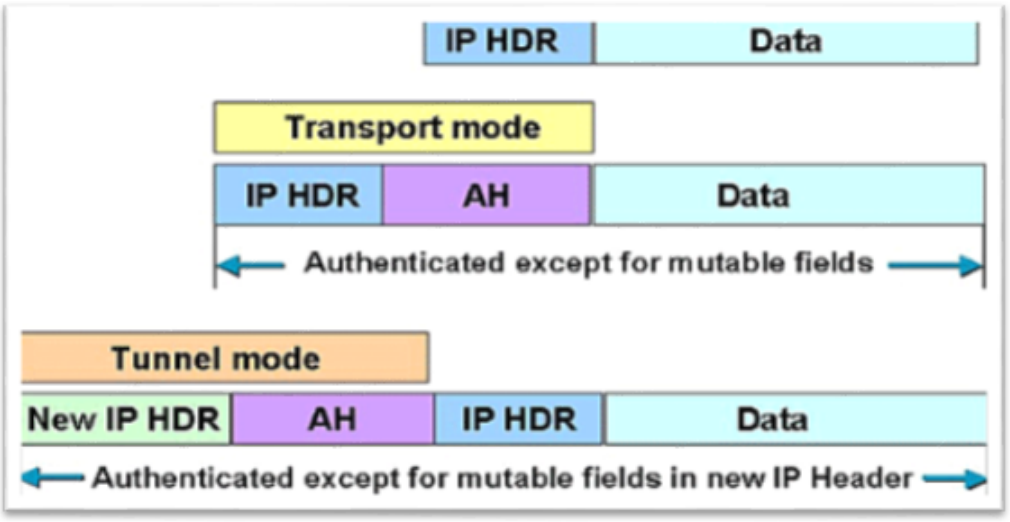


FIGURE 2.13 – *Modes Transport et Tunnel dans IPsec.*

2.5 Conclusion

Nous avons vu en premier lieu dans ce chapitres les principes de la sécurité , ses objectifs, ainsi que les différentes attaques qui la menacent. En deuxième lieux, nous avons présenté quelques solutions qui permettent d'assurer une politique de sécurité efficace tel que le firewall, la cryptographie, les VLANs, et enfin les VPNs.

A l'issue de ce chapitre, nous avons détaillé les différentes catégories et possibilités pour le déploiement d'un VLAN et d'un VPN, leur rôle et leurs différents protocoles utilisés.

Chapitre 3

Etude de l'existant

3.1 Introduction

Le port de Bejaia joue un rôle très important dans les transactions internationales vu sa place et sa position géographique. Aujourd'hui, il est classé 2èmeport d'Algérie en marchandises générales et 3ème port pétrolier. Il est également le 1erport du bassin méditerranéen certifié ISO 9001 :2000 pour l'ensemble de ses prestations, et à avoir ainsi installé un système de management de la qualité. Cela constitue une étape dans le processus d'amélioration continue de ses prestations au grand bénéfice de ses clients. L'Entreprise Portuaire a connu d'autres succès depuis, elle est notamment certifiée à la Norme ISO 14001 :2004 et au référentiel OHSAS 18001 :2007, respectivement pour l'environnement et l'hygiène et sécurité au travail**[1]**.

3.2 Missions et Activités de l'EPB

3.2.1 Ses Missions

La gestion, l'exploitation et le développement du domaine portuaire sont les charges essentielles de la gestion de l'EPB, c'est dans le but de promouvoir les échanges extérieurs du pays. Elle se doit d'assumer la police et la sécurité au sein du pays. Elle est chargée des travaux d'entretien, d'aménagement, de renouvellement et de création d'infrastructures. L'EPB assure également des prestations à caractère commercial, à savoir ; le remorquage, la manutention et l'acconage.

3.2.2 Ses Activités

Les principales activités de l'entreprise sont :

- L'exploitation de l'outillage et des installations portuaires.
- L'exécution des travaux d'entretien, d'aménagement et de renouvellement de la super structure portuaire.
- L'exercice du monopole des opérations d'acconage et de manutention portuaire.
- L'exercice du monopole des opérations de remorquage, de pilotage et d'amarrage.
- La police et la sécurité portuaire dans la limite géographique du domaine public portuaire.

3.3 Présentation des différentes structures de l'entreprise

L'EPB est organisé selon l'organigramme général suivant :

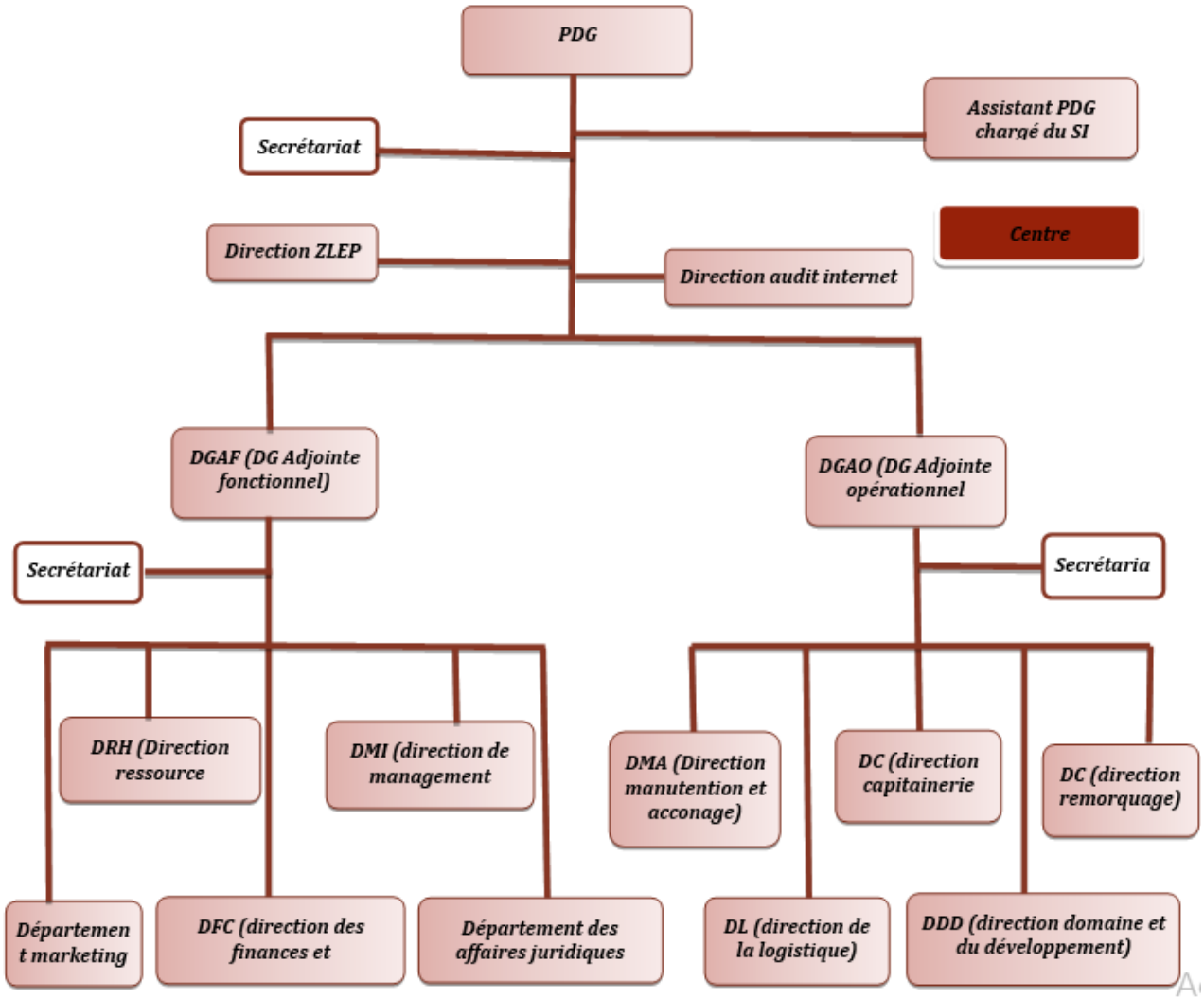


FIGURE 3.1 – *Organigramme général de l'EPB.*

3.4 Structure informatique

La structure informatique de l'EPB est un département rattaché à la direction générale adjointe ; Il a été créé en 1989 et c'est à cette époque que les premières applications de l'entreprise ont vu le jour. En 1995 la micro-informatique a été introduite à l'EPB et les premières applications sont écrites sous DBASE 5.

A partir de 2001 l'entreprise portuaire a lancé un plan pour développer les applications métiers sous PHP et DELPHI 5 et comme système de gestion de bases de données MYSQL.

- **Mission du département informatique**

Le département informatique a pour mission l'automatisation des métiers de l'Entreprise Portuaire de Bejaia, et cela en mettant en place les logiciels et l'infrastructure nécessaires pour la gestion du système d'information. L'EPB déploie des systèmes d'informations pour accroitre la productivité, automatiser les processus métiers et fournir un meilleur service aux clients. Ces systèmes intègrent de plus en plus des fonctionnalités réseau pour relier tous les utilisateurs à l'entreprise ou établir des liens avec la clientèle et les fournisseurs.

Le réseau apporte aujourd'hui une réelle valeur ajoutée en permettant d'intégrer de nouveaux partenaires, fournisseurs et clients.

3.4.1 Organisation humaine

Les différentes structures du centre informatique sont présentées dans l'organigramme ci-dessous :

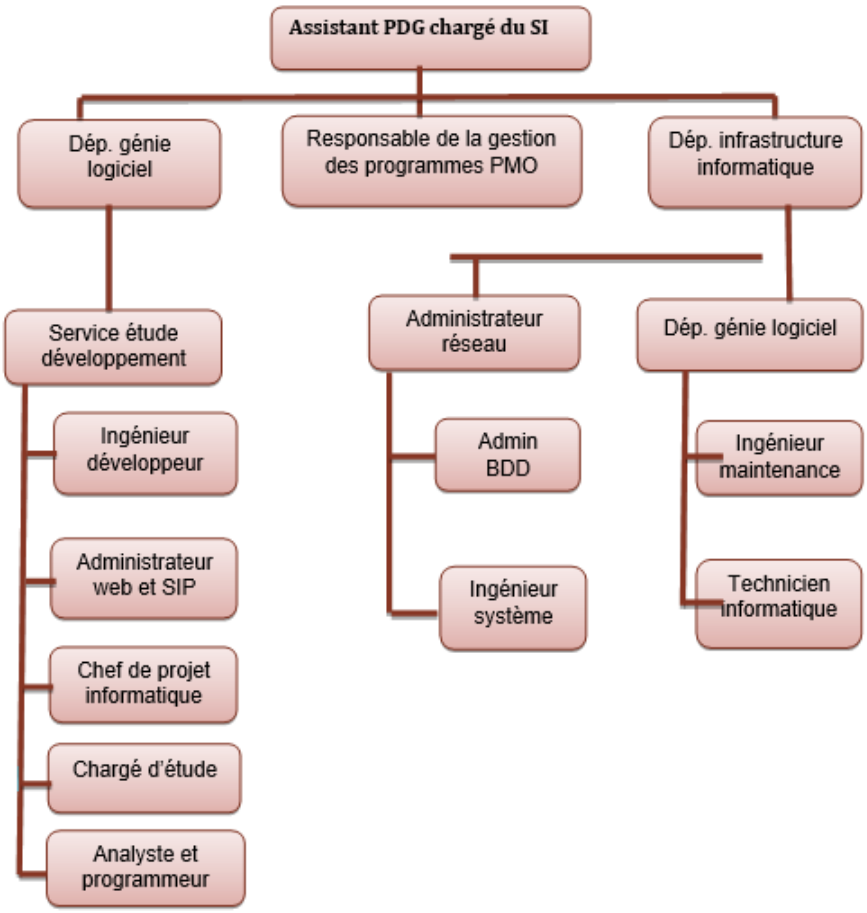


FIGURE 3.2 – *L'organigramme de la structure Informatique.*

3.4.2 Présentation du système d'information

L'EPB dispose de plus de 50 logiciels qui traitent des différentes activités du port *(Activités opérationnelles, activités de soutien...)*.

1. Réseau informatique de l'EPB

Le réseau du port de Bejaïa s'étend du port pétrolier *(no16)* aux ports 13 et 18 *(port à bois)*. La salle machine du réseau local de l'EPB contient principalement une armoire de brassage et une autre armoire optique de grande taille, éventuellement l'ensemble des serveurs, ces deux armoires servent à relier les différents sites de l'entreprise avec le département informatique par des fibres optiques de type 4, 6,8 et 12 brins. Chaque site a une armoire de brassage contenant un convertisseur(s) media, un/plusieurs Switch ou sont reliés les différents équipements par des câbles informatique.

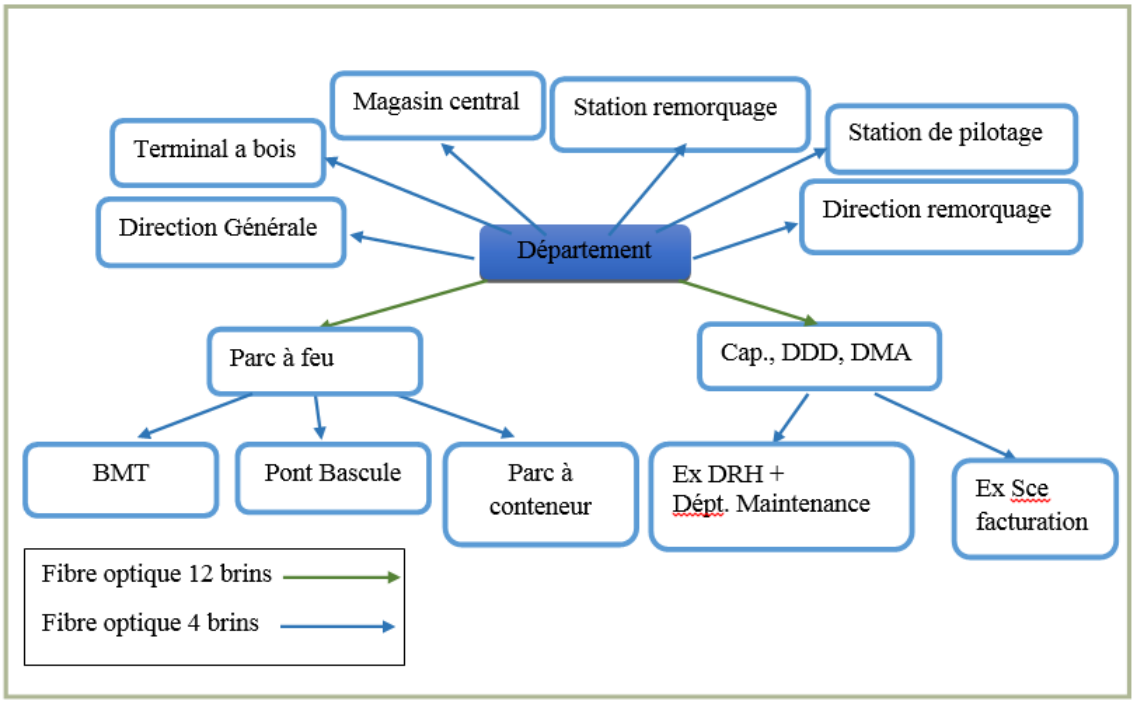


FIGURE 3.3 – *Réseau Fibre Optique de l'EPB.*

2. Architecture réseau de l'entreprise

L'architecture réseau du port de Bejaïa est comme la démontre la figure suivante :

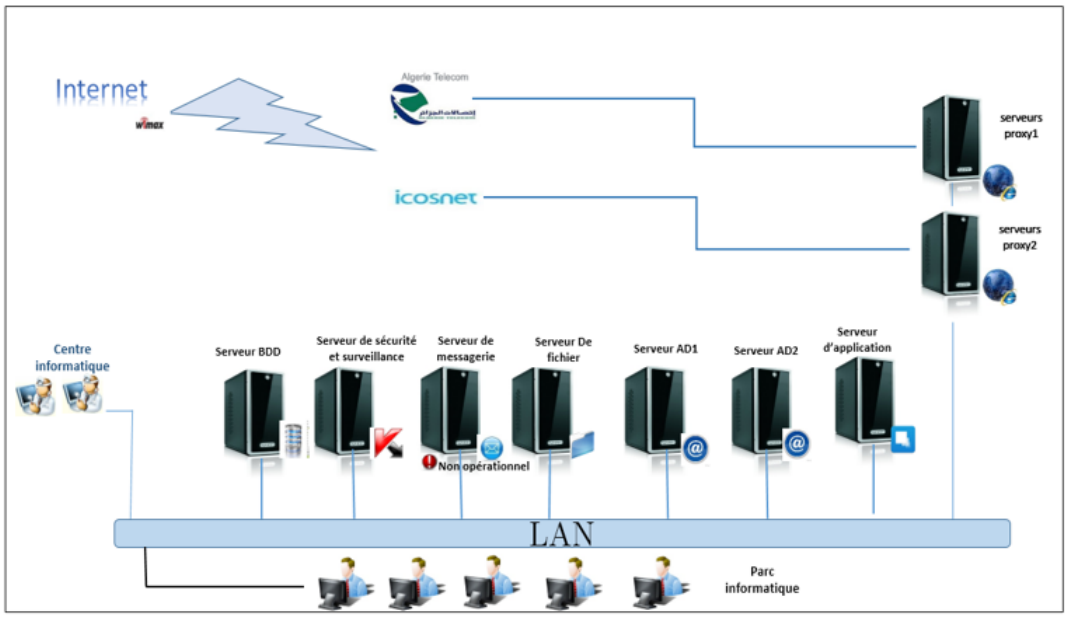


FIGURE 3.4 – *Architecture réseau de l'EPB.*

3.5 Contexte du projet à réaliser

Dans cette partie, nous allons en premier lieu présenter le projet à réaliser, suivi des objectifs issus de l'achèvement de ce dernier, en second lieu nous allons dégager la problématique associé au cahier de charges de l'organisme.

3.5.1 Présentation du projet

Le projet à réaliser, s'intitule "Etude et configuration de liaisons virtuelles (VLANs et VPNs) de l'Entreprise Portuaire de Bejaia «EPB» ".

La mise en œuvre de ce projet permet d'apporter des améliorations au réseau de l'entreprise, en mettant l'accent sur l'administration et le partage du réseau tout en assurant la fluidité et une meilleure sécurité en utilisant les réseaux virtuels VLANs et des liaisons VPNs. L'objectif de ce projet consiste à garantir une meilleure exploitation et attribution du réseau. Ainsi, assurer une communication sûre et confidentielle entre les utilisateurs au sein de l'entreprise.

En effet, proposer une segmentation sous laquelle les différents réseaux locaux des stations vont être organisés, afin de permettre la communication

et l'interconnexion entre elles en exploitant le routage.

3.5.2 Diagnostic de la situation du réseau

L'étude qu'on a mené, nous a permis de retirer et remarquer quelques faiblesses réseaux existantes dans l'entreprise et qui sont les suivantes :

- Un seul et unique domaine de diffusion ce qui implique une surcharge énorme du réseau ; des machines surchargées mais non sollicitées.
- Une mauvaise gestion et attribution d'adresse IP dû à l'utilisation de l'adressage statique, en plus, cette dernière est de classe A avec un masque sous réseau de 24 bits, donc un seul sous réseau, ce qui entraine une perte énorme d'adresses IP.
- Manque de liaisons sécurisées entre les plates-formes extra-portuaires

3.6 Solution proposée

Organiser son réseau local d'une bonne manière et adopter un bon modèle de segmentation est très important. En effet, une bonne organisation permettra une optimisation du réseau en terme d'efficacité et de performance. En outre, opter pour une solution de routage en choisissant la manière dont laquelle les données seront transitées à travers les réseaux.

L'organisation des réseaux locaux de l'Entreprise Portuaire de Bejaia, se fera en les segmentant à l'aide des VLANs et des liaisons VPNs. En effet, cette solution est la meilleure et adéquate, en vue des avantages qu'elle offre.

L'interconnexion des LANs de l'Entreprise Portuaire de Bejaia, en adoptant un routage dynamique est plus efficace par rapport à un routage statique, et cela vu la taille considérable du réseau.

3.7 Conclusion

L'étude de l'existant nous a permet de se familiariser avec le réseau actuel de l'EPB et de l'étudier assez profondément afin de voir ses lacunes et ses faiblesses. Cette étude nous a conduits à proposer des solutions pour palier à ces dernières. Après avoir choisi la solution à adopter, nous avons tracé nos objectifs ensuite nous avons défini un plan de travail pour mettre en œuvre ces solutions.

La prochaine partie va être consacrée à la description de la réalisation des étapes citées précédemment, à savoir l'installation du matériel et des logiciels ainsi que les configurations des équipements appropriées.

Chapitre 4

Configuration de liaisons virtuelles *(VLANs & VPNs)*

Partie I : Segmentation du réseau de l'EPB en VLANs

4.1 Segmentation en VLAN

La notion de VLAN est un concept qui permet de réaliser une sécurité optimal des réseaux de façon indépendante du système de câblage. Ces réseaux nous permettrons :

- D'améliorer la gestion du réseau.
- D'optimiser la bande passante.
- De Séparer les flux.
- Plus de souplesse pour l'administration.
- Augmenter la sécurité sur le réseau.
- Réduction de la diffusion du traffic sur le réseau.

4.2 Matériels et équipements utilisés

Le matériel et les équipements essentiels à la configuration des VLANs sont :

- 17 Switch Cisco 2960.
- 1 switch fédérateur optique.
- Câble RJ45 droit.
- Câble RJ45 croisé.
- Câble fibre optique.

- Des ordinateurs.

4.3 Cisco Packet Tracer 6.2

Cisco Packet Tracer est un logiciel de simulation réseau avec des équipements Cisco. Etant très réaliste, il est une bonne alternative pour ceux qui souhaitent s'entrainer sur des équipements réels. Il permet de faire du routage, de la configuration de VLAN, DHCP, NAT, ACL, etc. Cet outil est créé par Cisco Systems. Le but de packet tracer est d'apprendre les principes du réseau, tout en acquérant des compétences aux technologies spécifiques de Cisco (Cisco Networking Academy)**[24]**.

4.4 Affectation des ports aux différents Vlans

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

Département informatique	3eme étage	2eme étage		1ere étage RDC	
SW1 Vlan INF	SW2 Vlan DG	SW3 Vlan DGA	SW4 Vlan DRH	SW5 Vlan DRH – Vlan DFC	SW6 Vlan DFC
1–24 ports INF	1–24 ports DG	1–24 ports DGA	1–24 ports DRH	1–12 ports DRH 13–24 ports DFC	1–24 ports DFC

TABLE 4.1 – Affectation des ports au niveau de la direction générale.

SW7 Vlan DMA	SW8 Vlan DMA	SW9 Vlan DMA	SW10 Vlan DR	SW11 Vlan DG	SW12 Vlan DC	SW13 Vlan DL	SW14 Vlan DDD	SW15 Vlan DZ-LEP	SW16 Vlan DMI
1 – 24 ports DMA	1 – 24 ports DMA	1 – 24 ports DMA	1 – 24 ports DR	1 – 24 ports DG	1 – 24 ports DC	1 – 24port DL	1 – 24ports DDD	1 – 24ports DZ-LEP	1 - 24ports DMI

TABLE 4.2 – Affectation des ports en dehors de la direction générale.

4.5 Nomination des VLANs et attribution des adresses

Les noms et les identificateurs des VLANs à implémenter et les adresses IP seront répartis comme le démontre le tableau suivant :

Nom de Vlan	ID	Adresse réseau	1ere adresse utilisable	Dernière adresse utilisable	passerelle	Sous-interface
Vlan INF	2	172.16.128.0/22	172.16.128.1	172.16.128.254	172.16.128.1	Fa0/0.2
Vlan DG	3	172.16.132.0/22	172.16.132.1	172.16.132.254	172.16.132.1	Fa0/0.3
Vlan DR	4	172.16.136.0/22	172.16.136.1	172.16.136.254	172.16.136.1	Fa0/0.4
Vlan DMA	5	172.16.140.0/22	172.16.140.1	172.16.140.254	172.16.140.1	Fa0/0.5
Vlan DFC	6	172.16.144.0/22	172.16.144.1	172.16.144.254	172.16.144.1	Fa0/0.6
Vlan DRH	7	172.16.148.0/22	172.16.148.1	172.16.148.254	172.16.148.1	Fa0/0.7
Vlan DGA	8	172.16.176.0/22	172.16.176.1	172.16.176.254	172.16.176.1	Fa0/0.8
Vlan DC	9	172.16.160.0/22	172.16.160.1	172.16.160.254	172.16.160.1	Fa0/0.9
Vlan DL	10	172.16.152.0/22	172.16.152.1	172.16.152.254	172.16.152.1	Fa0/0.10
Vlan DDD	11	172.16.156.0/22	172.16.156.1	172.16.156.254	172.16.156.1	Fa0/0.11

TABLE 4.3 – Affectation d'adresses IP et sous-interfaces du routeur.

4.6 Configuration

Réalisation des solutions proposées sous Packet Tracer, entre l'EPB et un site distant *(ex : Aboudaou)* :

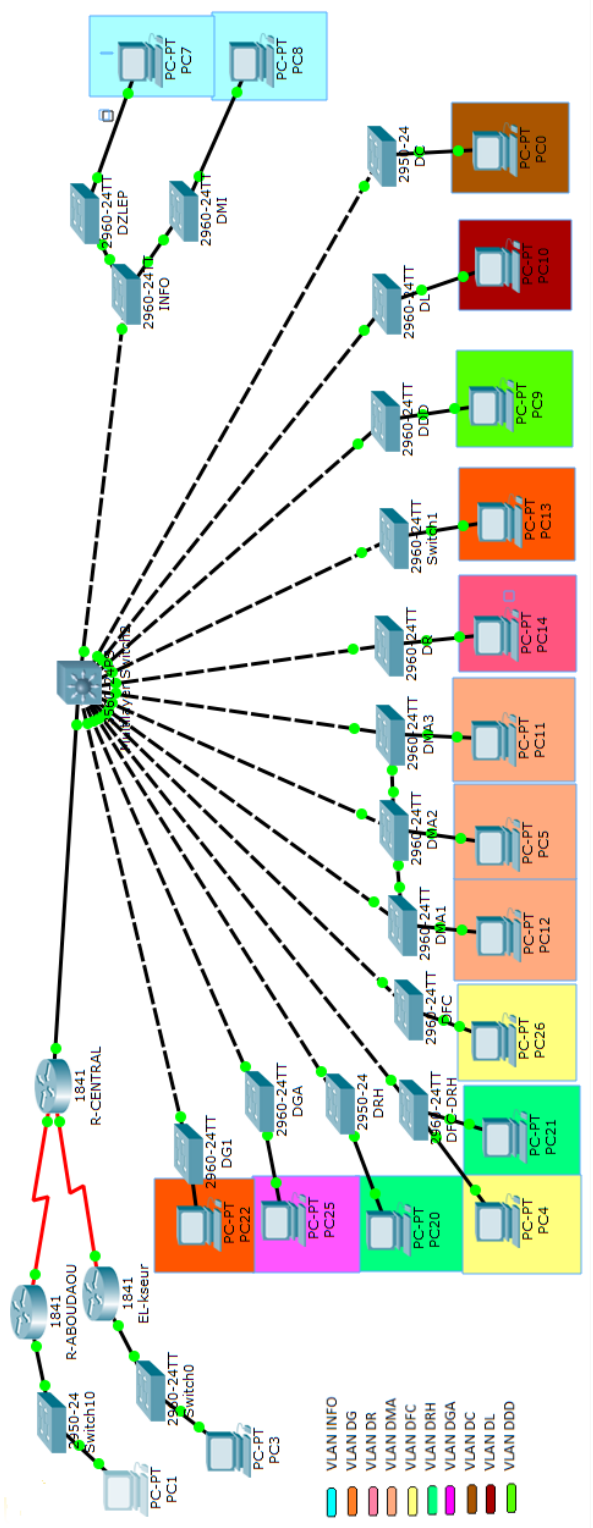


FIGURE 4.1 – *Architecture du réseau de l' EPB.*

4.7 Création des VLANs

4.7.1 Configuration de base

Nous présentons si dessous la configuration de base du switch fédérateur et le routeur central (création du nom et des mots passe) :

•Switch :

Switch>enable
Switch♯configure terminal
Switch(config)♯hostname VTPserveur

•Définir le mot de passe du mode d'exécution privilégié :

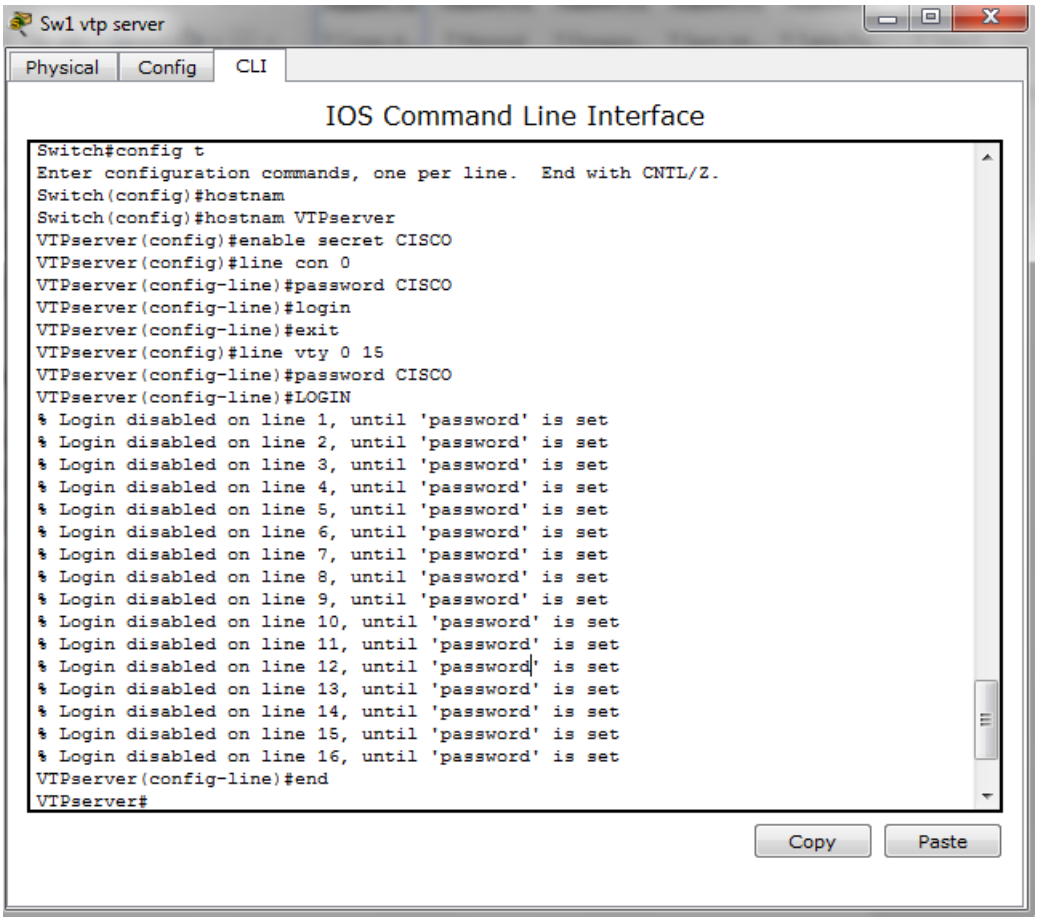
VTPserveur(config)♯enable secret CISCO

•Configurer la ligne console :

VTPserveur(config)♯line con 0
VTPserveur(config-line)♯password CISCO
VTPserveur(config-line)♯login
VTPserveur(config-line)♯exit

•Configurer le terminal virtuel (vty) :

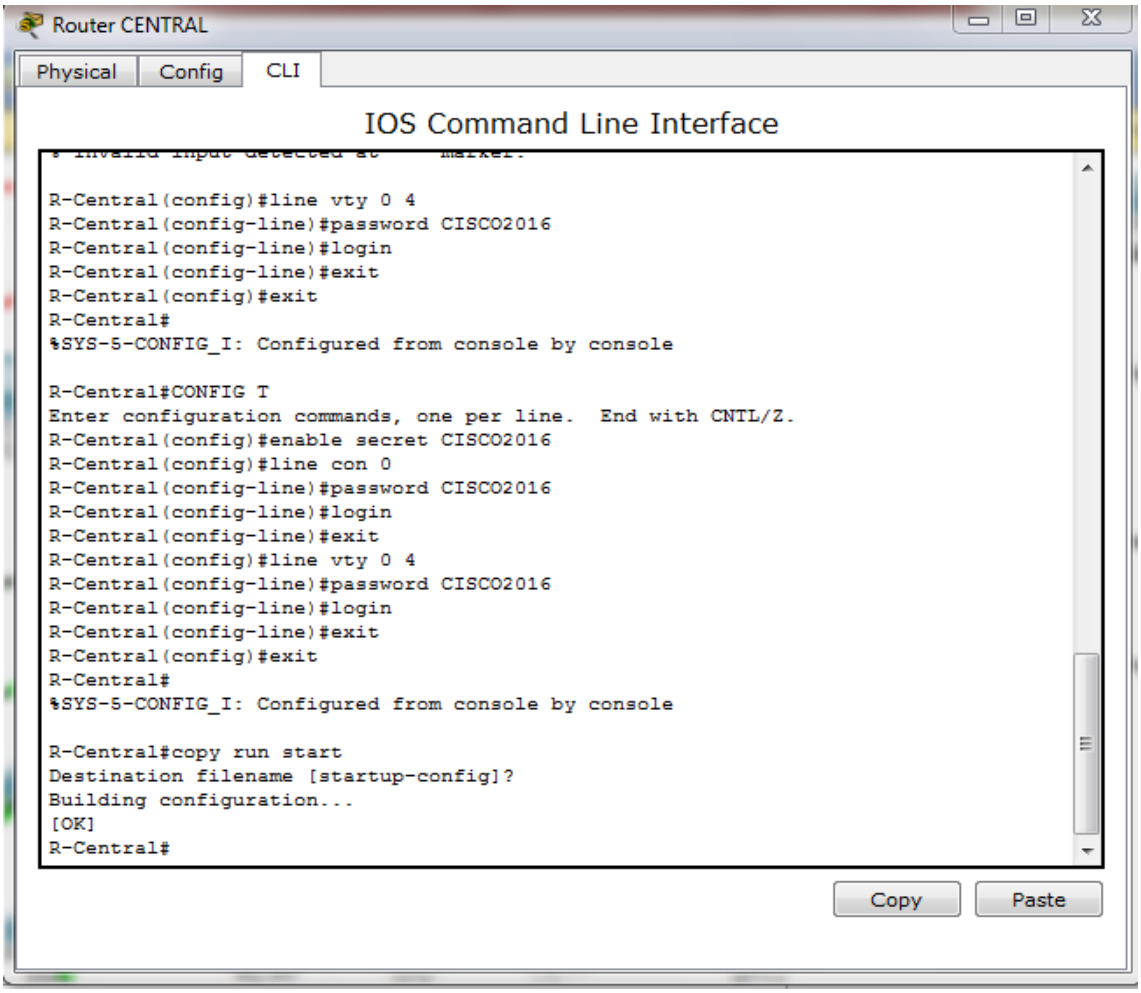
VTPserveur(config)♯line vty 0 15
VTPserveur(config-line)♯password CISCO
VTPserveur(config-line)♯login
VTPserveur(config-line)♯end



Cette configuration de base s'applique aux niveaux de tous les switchs, en prenant compte la variation des noms et des mots passe d'un switch à un autre.

•Configuration du Routeur :

Router>enable
Router♯config terminal
Router(config)♯hostname R-Central
R-Central(config)♯enable secret CISCO2016
R-Central(config)♯line con 0
R-Central(config-line)♯password CISCO2016
R-Central(config-line)♯login R-Central(config-line)♯exit
R-Central(config)♯line vty 0 4
R-Central(config-line)♯password CISCO2016
R-Central(config-line)♯login R-Central(config-line)♯end
R-Central♯copy run start

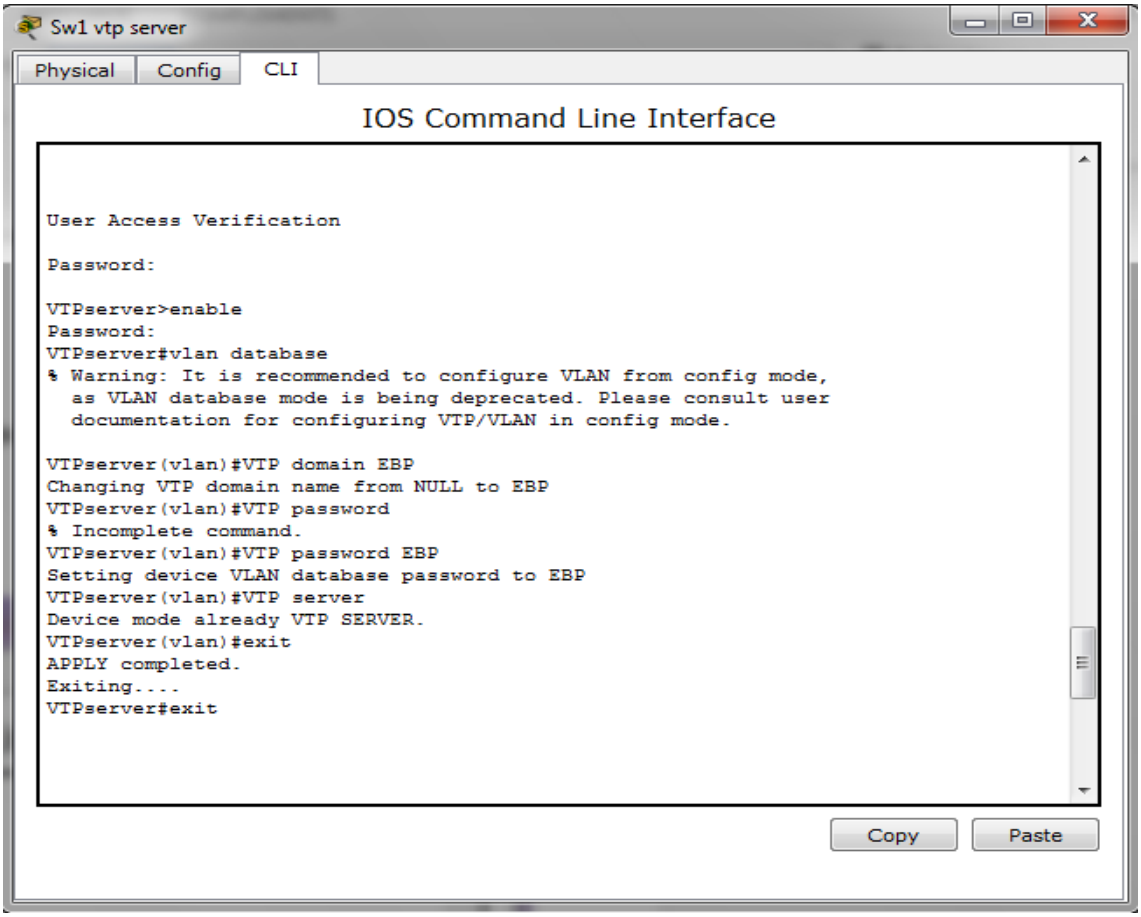


4.7.2 Configuration du VTP

Le serveur VTP diffuse ses configurations VLAN, tandis que le client VTP met à jour sa configuration VLAN en fonction des informations reçues du serveur.

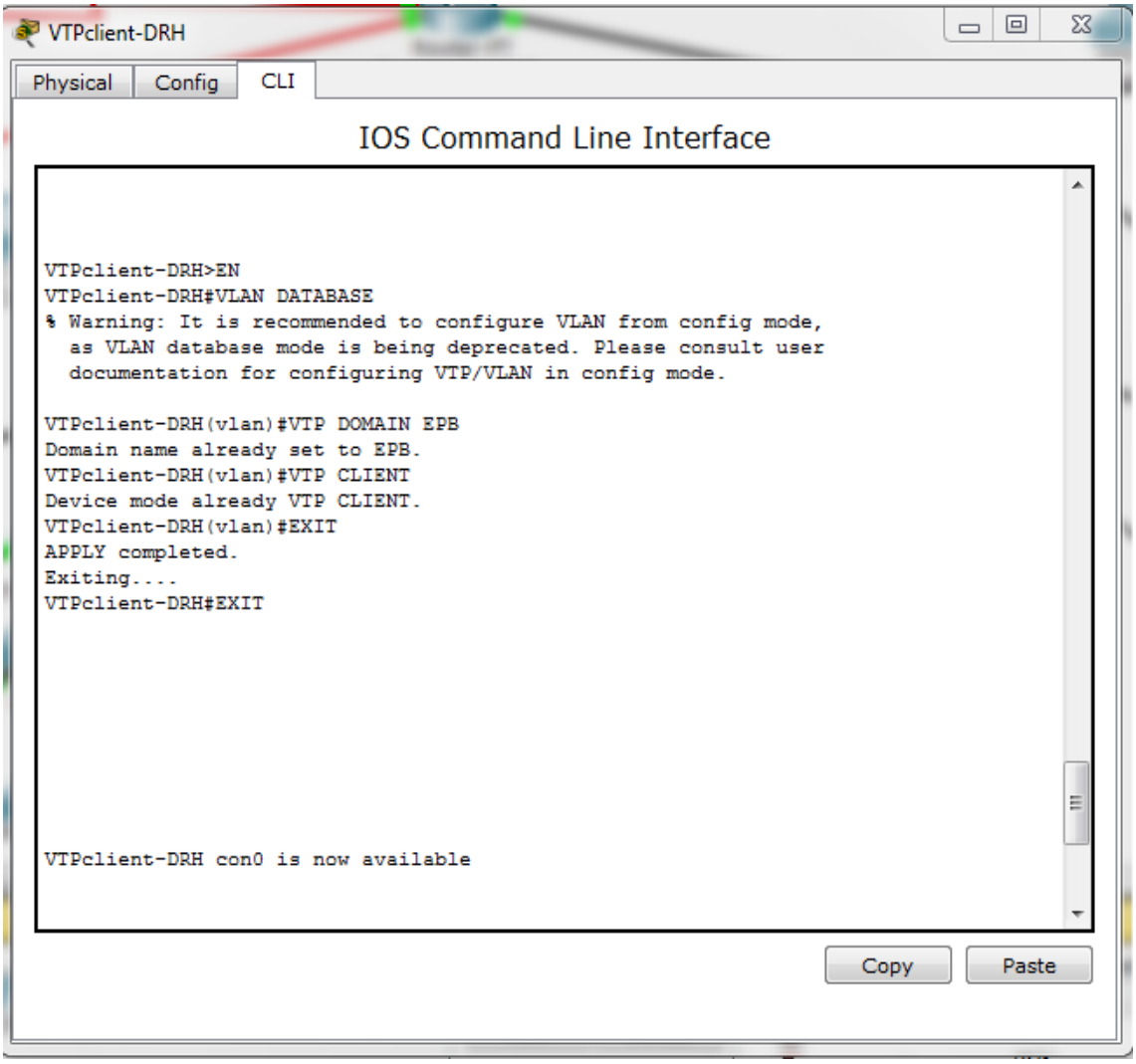
•Mode VTP serveur :

VTPserveur♯vlan database
VTPserveur(vlan)♯VTP domain EPB
VTPserveur(vlan)♯VTP password EPB
VTPserveur(vlan)♯VTP server
VTPserveur(vlan)♯exit



•Mode VTP client :

VTPclientDRH♯vlan database
VTPclientDRH(vlan)♯VTP domain EPB
VTPclientDRH(vlan)♯VTP client
VTPclientDRH(vlan)♯exit



4.7.3 Configuration et créations des VLANs sur le serveur VTP

•Créez le VLAN INF *(VLAN 2)* :

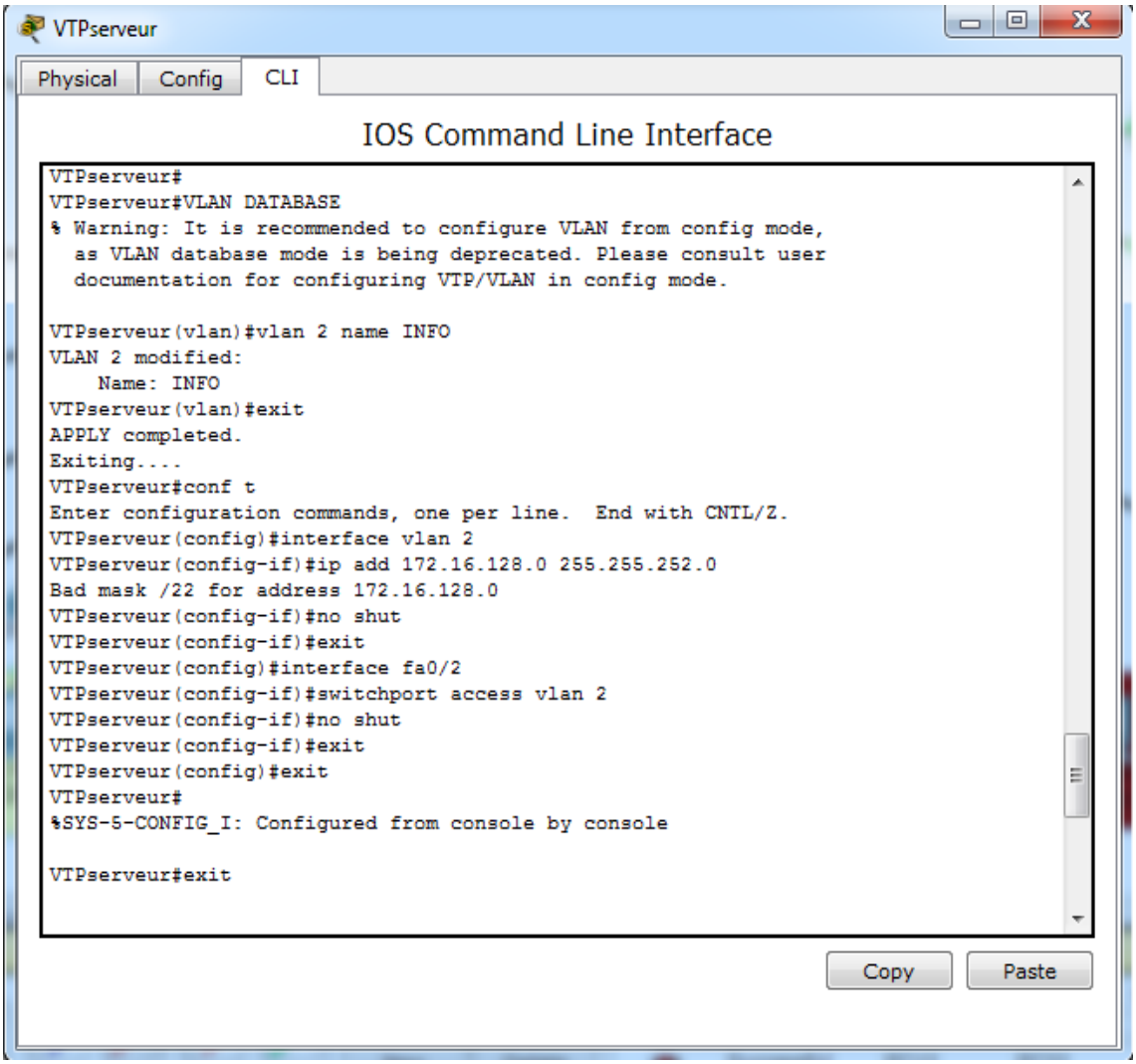
VTPserveur♯vlan database
VTPserveur(vlan)♯vlan 2 name INF
VTPserveur(vlan)♯exit

•Configurez l'adresse IP, le masque de sous-réseau du switch «VTPserveur» :

VTPserveur(config)♯interface vlan 2
VTPserveur(config-if)♯ip address 172.16.128.0 255.255.252.0
VTPserveur(config-if)♯no shutdown
VTPserveur(config-if)♯exit

•Attribution des ports du switch « VTPserveur» au VLAN2 :

VTPserveur(config)♯interface range fa0/2-20
VTPserveur(config-if-range)♯switchport access vlan 2
VTPserveur(config-if-range)♯no shutdown
VTPserveur(config-if-range)♯exit

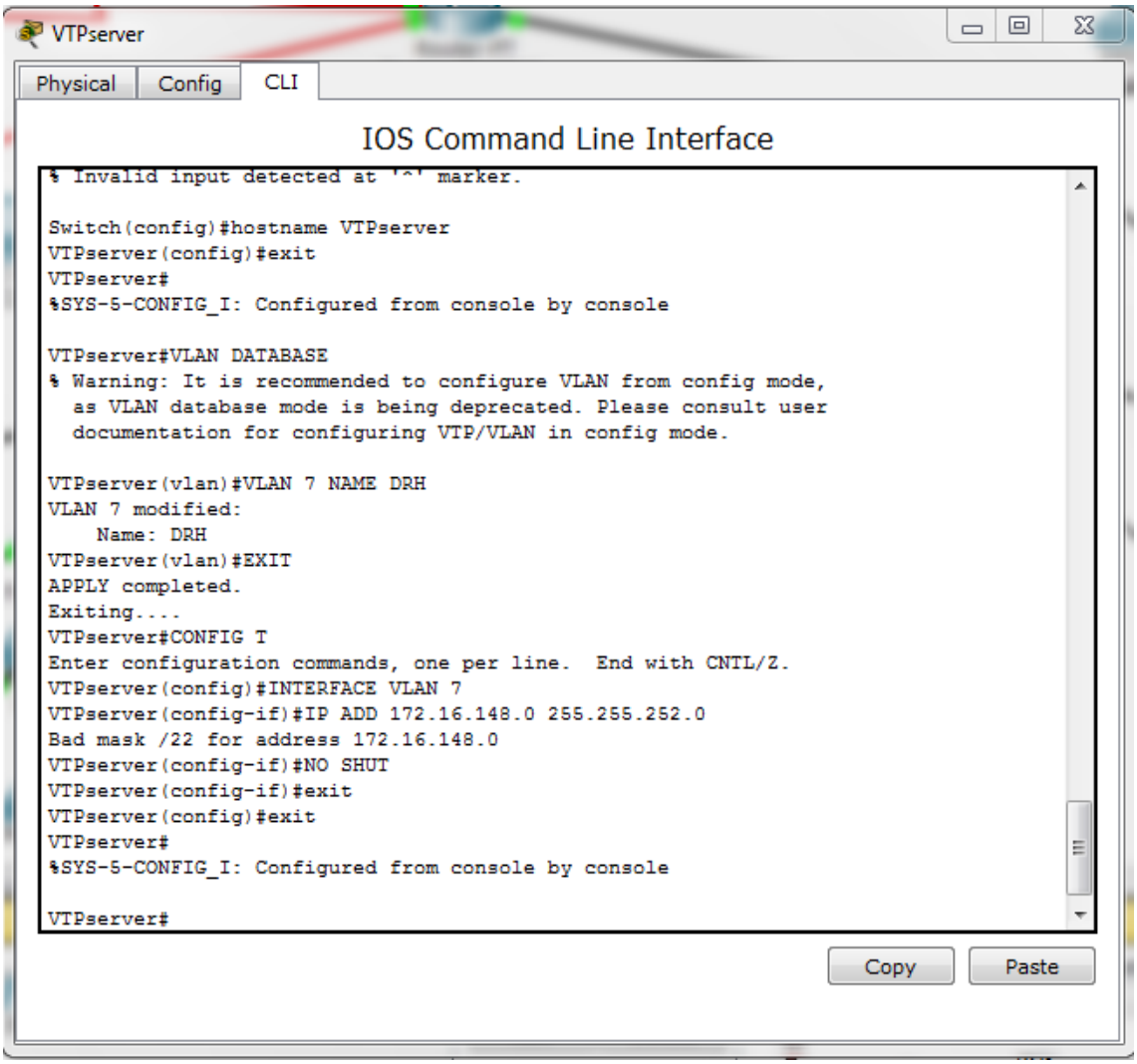


•**Créez le VLAN DRH *(Vlan 7)* :**

VTPserveur♯vlan database
VTPserveur(vlan)♯vlan 7 name DRH
VTPserveur(vlan)♯exit

•Configurez l'adresse IP, le masque de sous-réseau du VLAN 7 :

VTPserveur(config)♯interface vlan 7
VTPserveur(config-if)♯ip address 172.16.148.0 255.255.252.0
VTPserveur(config-if)♯no shutdown
VTPserveur(config-if)♯exit

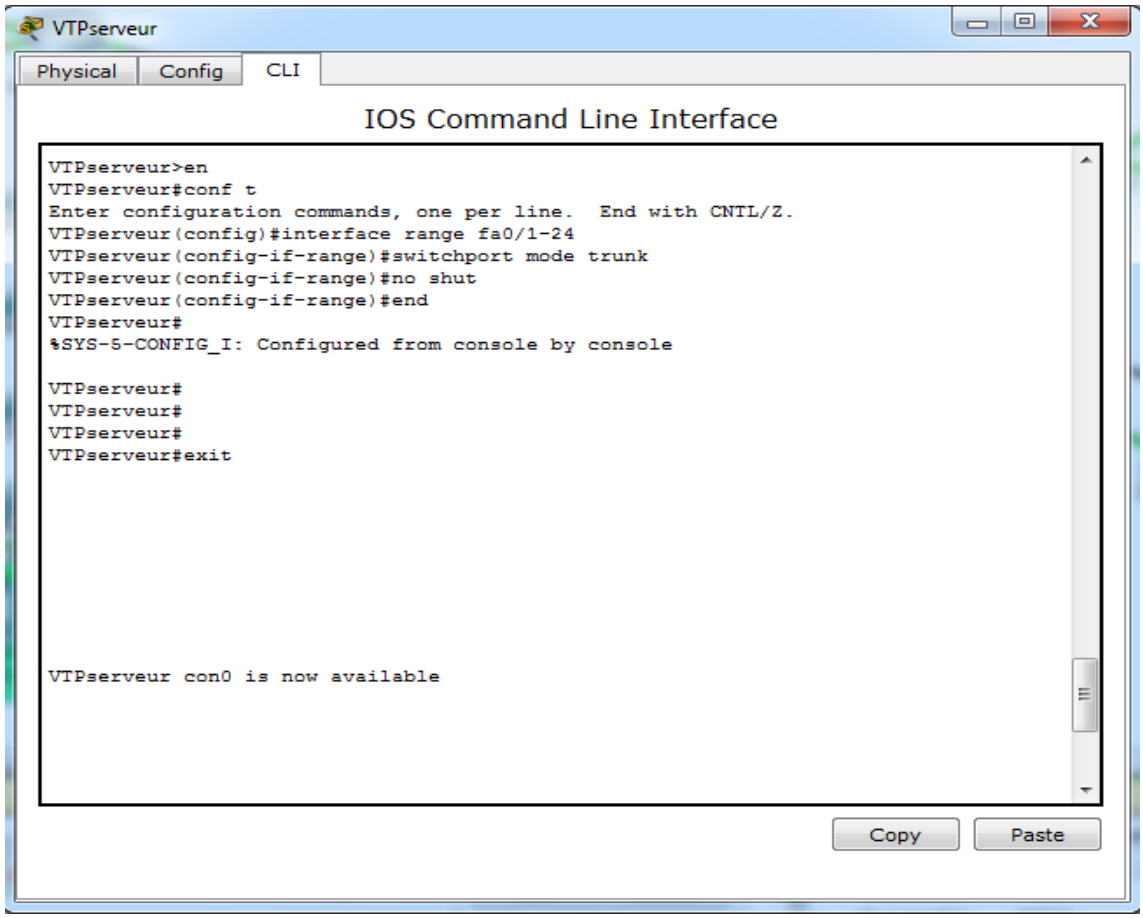


La création et la configuration de tous les VLANs s'effectue au niveau du **"VTPserveur"** d'une manière similaire ; néanmoins une variation des noms et de l'adresse IP est nécessaire.

4.7.4 Configuration des agrégations *(Trunk)*

Le lien trunk est nécessaire entre le switch serveur et les switch client. C'est en effet par celui-ci que les trames étiquetées transitent.

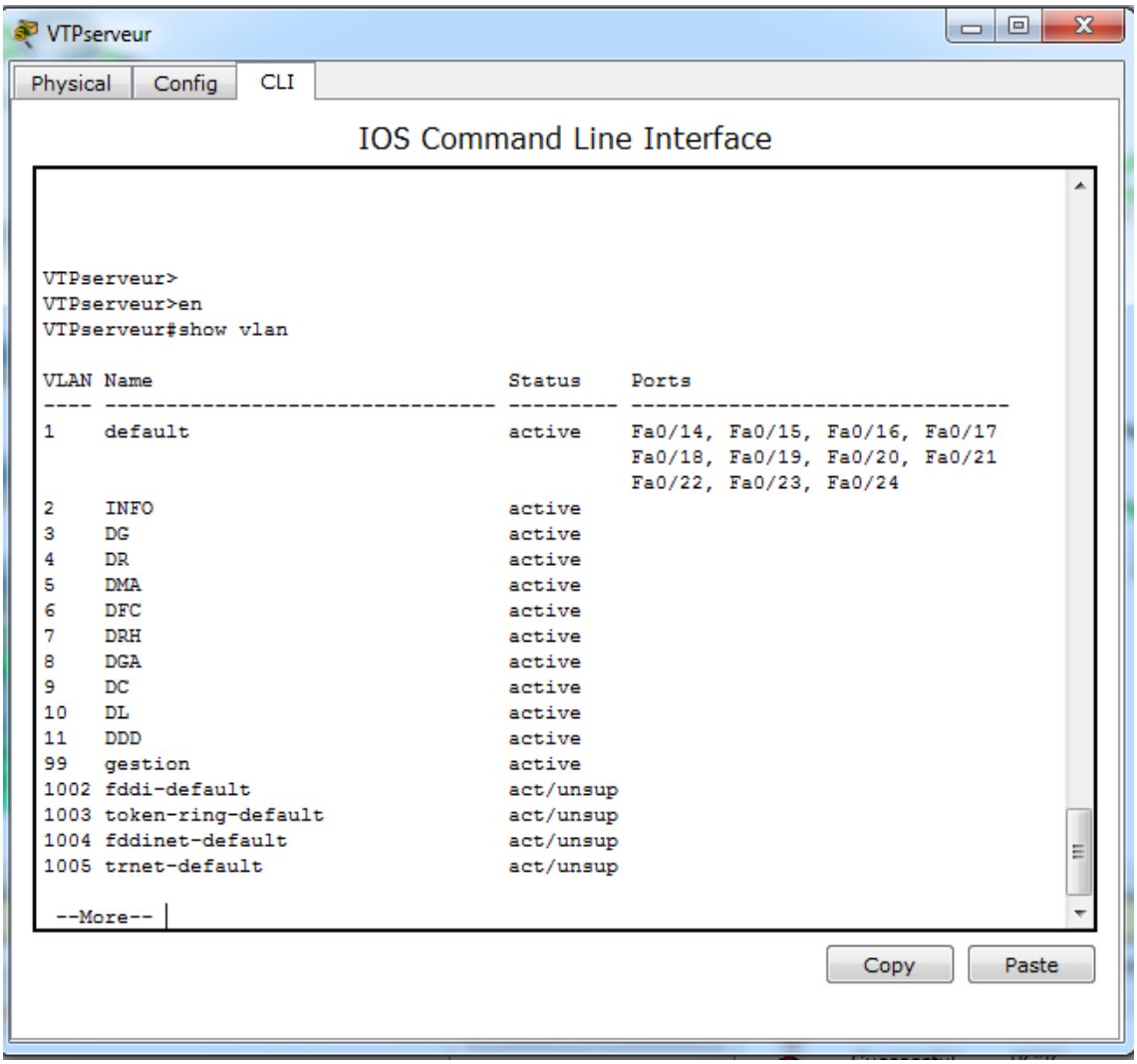
VTPserveur(config)♯interface range fa0/1-24
VTPserveur(config-if-range)♯switchport mode trunk
VTPserveur(config-if-range)♯no shutdown
VTPserveur(config-if-range)♯end



La configuration de l'agrégation trunk se fera sur le reste de tous les switchs.

Vérifiez que les VLANs ont été créés sur le switch "VTPserveur" via la commande **show vlan**.

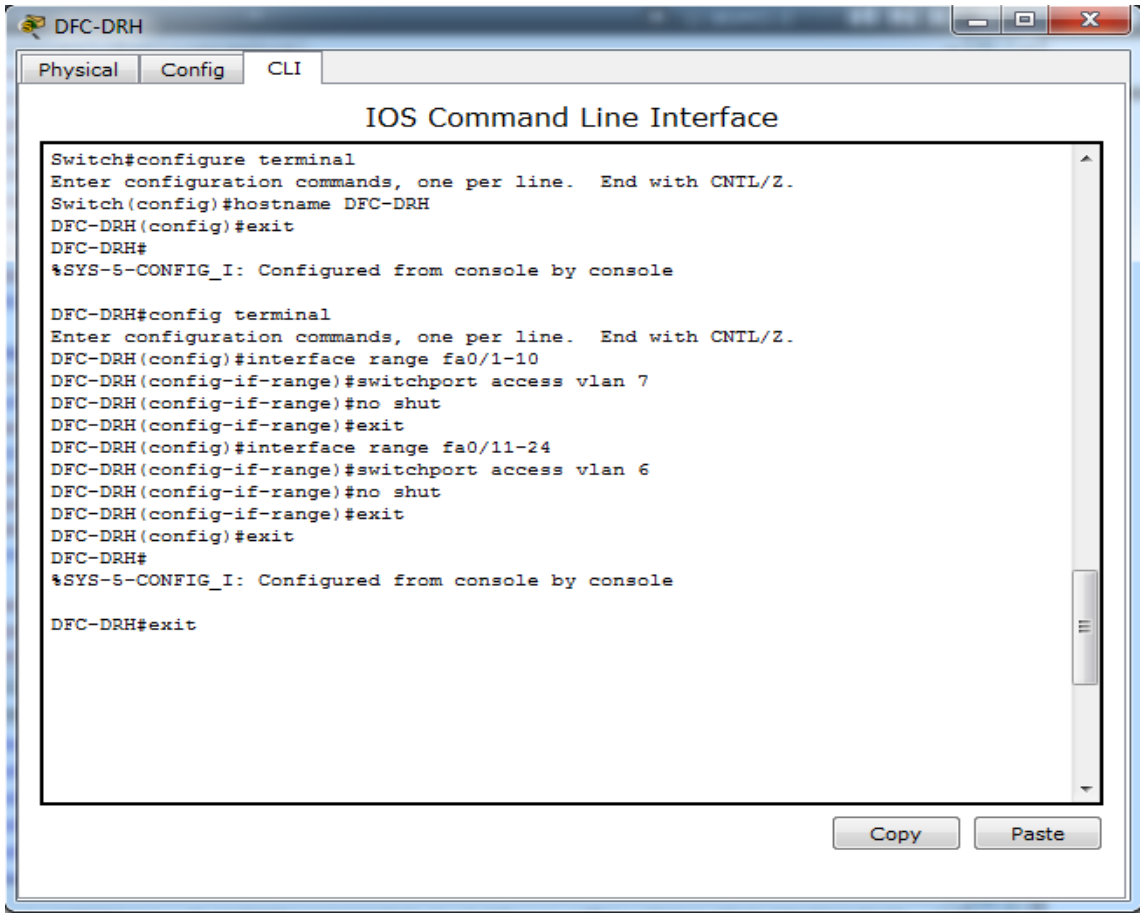
VTPserveur♯show vlan



4.7.5 Configuration des agrégations *(Access)*

- Attribution des vlan 6 et 7 aux ports du switch "DFC-DRH" :

DFC-DRH(config)♯interface range fa0/1-10
DFC-DRH(config-if-range)♯switchport access vlan 7
DFC-DRH(config-if-range)♯no shutdown
DFC-DRH(config-if-range)♯exit
DFC-DRH(config)♯interface range fa0/11-24
DFC-DRH(config-if-range)♯switchport access vlan 6
DFC-DRH(config-if-range)♯no shutdown
DFC-DRH(config-if-range)♯exit

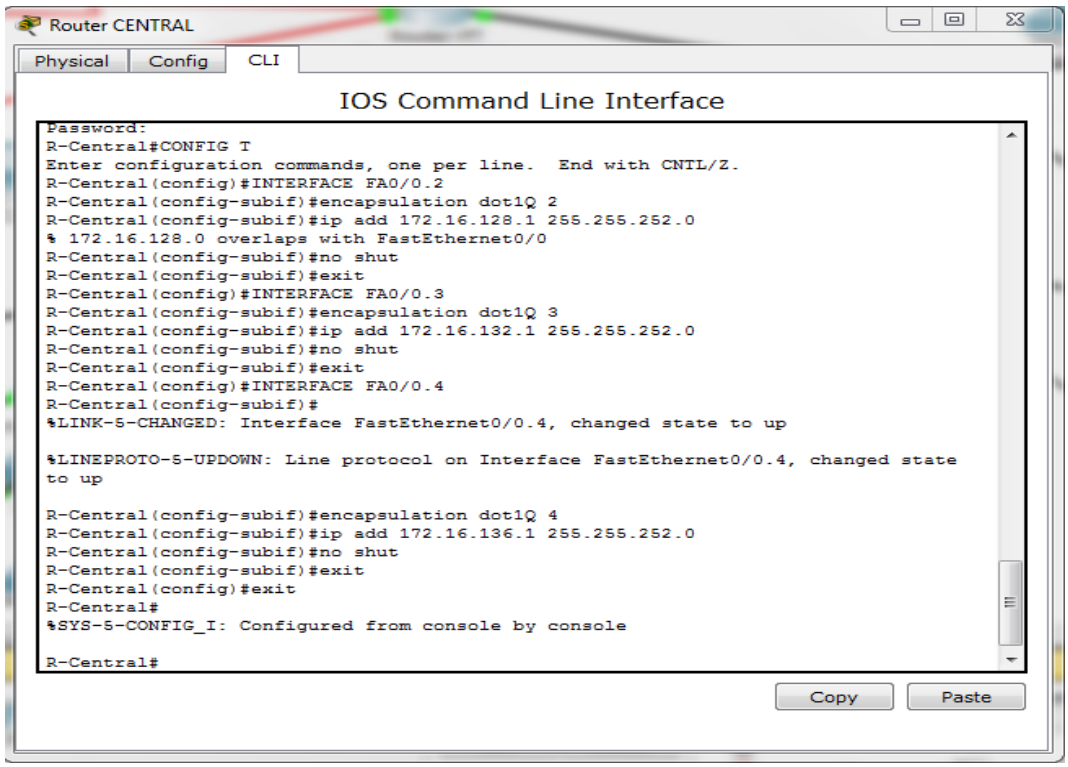


4.7.6 Routage inter-Vlans

Sur un router, une interface peut être logiquement diviser en plusieurs sous-interface virtuels. Elles fournissent une solution flexible pour le routage de plusieurs flux de données via une interface physique unique.

- Pour définir des sous-interfaces et activer des liaisons agrégées, on effectue les commandes suivantes : (ex : *switch du depINFO*)

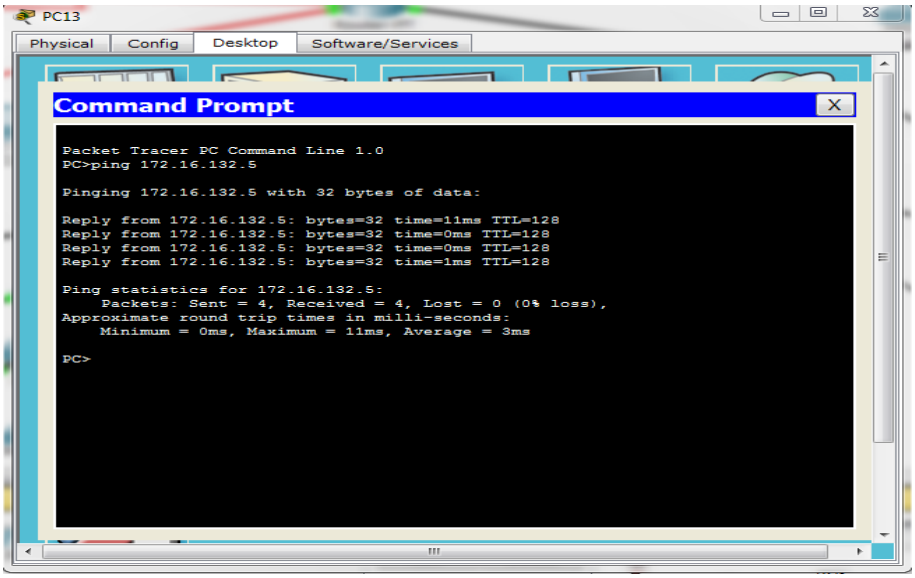
R-Central(config)♯interface Fa0/0.2
R-Central(config-subif)♯encapsulation dot1Q 2
R-Central(config-subif)♯ip address 172.16.128.1 255.255.252.0
R-Central(config-subif)♯no shutdown
R-Central(config-subif)♯exit



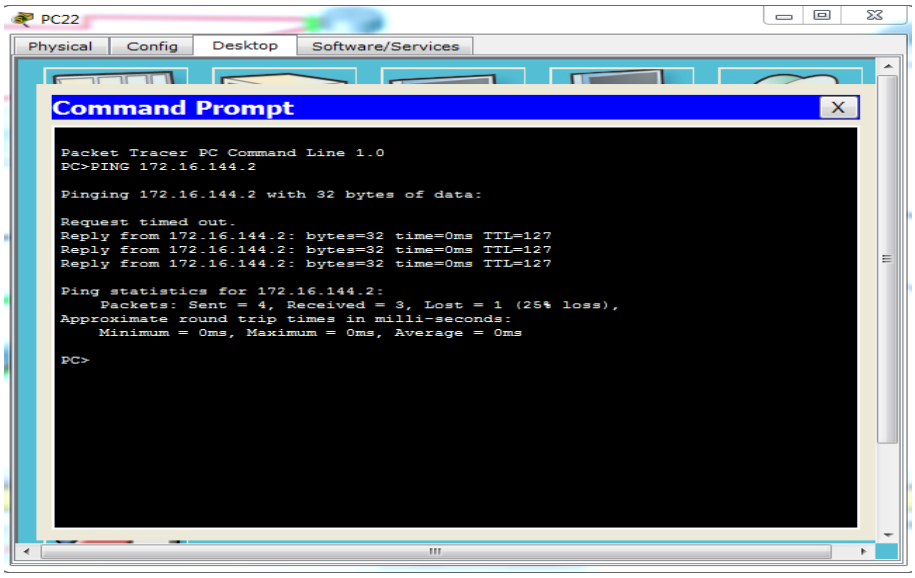
En suit les mêmes commandes avec tous les VLANs, pour configurer des sous-interfaces et activer des liaisons agrégées.

4.8 Test du réseau local de l'EPB

Testez la communication entre les différents PC du réseau local de l'EPB : **Intra-Vlan** : ex : Ping réussi entre PC13 et PC22 du VLAN DG



Inter-Vlan : Ping réussi entre PC4 du Vlan DFC et PC22 du Vlan DG.



Partie II : Configuration et mise en œuvre d'un tunnel VPN

Les tunnels VPN mis en place dans notre projet ont pour but la transmission sécurisée des données entre tous les sites distants de l'EPB. Nous avons créé deux tunnels VPN sur le réseau public internet (WiMax Ecosnet, WiMax SLC). ISAKMP et IPsec sont la base de la construction et le chiffrement des tunnels VPN. ISAKMP ou IKE, est le protocole qui permet à deux hôtes de s'accorder sur la façon de construire une association de sécurité IPsec. Cette opération s'effectue en deux étapes :

- Créer le premier tunnel, qui protège les messages de négociation ISAKMP.
- Créer le tunnel qui protège les données.

Phase 1 : Configuration du VPN

1. Schéma proposé de la solution VPN pour l'EPB
   Le schéma suivant représente une architecture pour la création de tunnels VPN, relient les 3 pole distant : l'EPB, Aboudaou et Elkseur.
2. **Configuration d'un tunnel VPN IPSec**

   Pour parfaire ce projet, il faut diviser le travail en deux phases qui sont nécessaires pour obtenir le Tunnel VPN IPSec :
   - Configuration d'ISAKMP.
   - Configuration d'IPSec (ISAKMP, crypto MAP).

   Il est noté que la politique ISAKMP de phase 1 est définie de manière globale. Cela signifie que si nous avons par exemple cinq différents sites distants (ce qui est souvent le cas vu que les entreprises ont plusieurs filiales généralement), il faut configurer cinq différentes politique ISAKMP de phase 1 *(un pour chaque routeur distant).*
   Dans ce cas, notre routeur tentera de négocier un tunnel VPN avec chaque site, et il enverra les cinq politiques puis utilisera la première correspondance reconnu par les deux extrémités.

   Notre exemple de configuration se situe entre 3 branches de l'entreprise EPB : Routeur-central de l'EPB, Routeur-Aboudaou et Routeur-Elkseur. Les 3 routeurs sont connecter à internet et ils disposent d'une adresse statique *(attribuée par le fournisseur d'accès internet)* ; comme il est indiqué sur le schéma suivant :

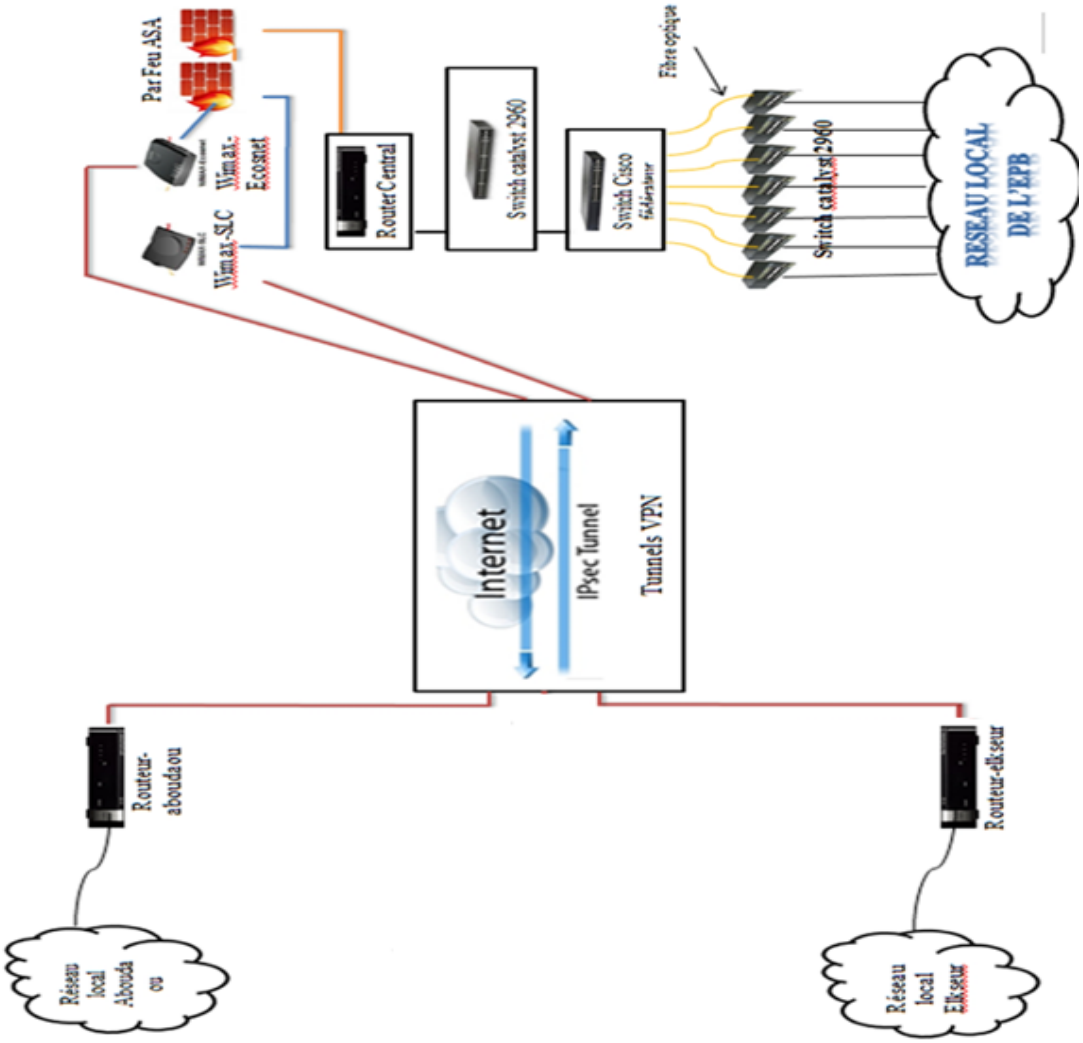


FIGURE 4.2 – *le schéma de la solution proposé pour l'EPB*

- L'adresse réseau local de l'EPB est : 172.16.100.0/22
- L'adresse réseau local d'Aboudaou est : 192.168.5.0/24
- L'adresse réseau local Elkseur est : 172.30.1.0/24
- Pour l'interface du routeur-Central l'adresse IP est : 192.168.4.9/30
- Pour l'interface du routeur-Aboudaou l'adresse IP est : 192.168.4.10/30
- Pour l'interface du routeur-Central l'adresse IP est : 172.30.2.1/24
- Pour l'interface du routeur-Elkseur l'adresse IP est : 172.30.2.2/24

⋆Table d'adressage

Périphérique	Interface	Adresse IP	Masque	Passerelle
R-Central	Fa0/0	172.16.128.1	255.255.252.0	S/0
	Seriel0/0/0	192.168.4.9	255.255.255.252	S/0
	Seriel0/0/1	172.30.2.1	255.255.255.0	S/0
PC7	Carte réseau	172.16.128.4	255.255.252.0	172.16.128.1
R-Aboudaou	Fa0/0	192.168.5.1	255.255.255.0	S/0
	Seriel0/0/0	192.168.4.10	255.255.255.252	S/0
PC1	Carte réseau	198.168.5.2	255.255.255.0	192.168.5.1
R-Elkseur	Fa0/0	172.30.1.1	255.255.255.0	S/0
	Seriel0/0/1	172.30.2.2	255.255.255.0	S/0
PC-C	Carte réseau	172.30.1.2	255.255.255.0	172.30.1.1

TABLE 4.4 – Tableau des adresses proposé

Dans notre proposition nous allons configurer le tunnel VPN IPSec entre deux sites : Routeur- central de l'EPB (R-Central) et le Routeur-Aboudaou *(R-Aboudaou)*.

Phase II : Configuration d'un VPN IPsec site à site

1. **Configuration d'ISAKMP (IKE)**
   Nous allons configurer la politique qui détermine quelle encryptions on utilise, quelle Hash quelle type d'authentification, etc.

   •Router-Central :

```
R-Central♯config ter
R-Central(config)♯crypto isakmp enable
R-Central(config)♯crypto isakmp policy 1
R-Central(config-isakmp)♯authentication pre-share
R-Central(config-isakmp)♯encryption AES
R-Central(config-isakmp)♯hash sha
R-Central(config-isakmp)♯group 2
R-Central(config-isakmp)♯exit
```

group 2 : Spécifie l'identifiant Diffie-Hellman

• **Configurer la clef :**

Nous devons définir une clé pré-partagée pour l'authentification avec le site 2 (routeur R- Aboudaou) à l'aide de la commande suivante :

R-Central(config)♯crypto isakmp key 678 address 192.168.4.10

2. **Configuration IPsec**

Configurons les options de transformations des données :

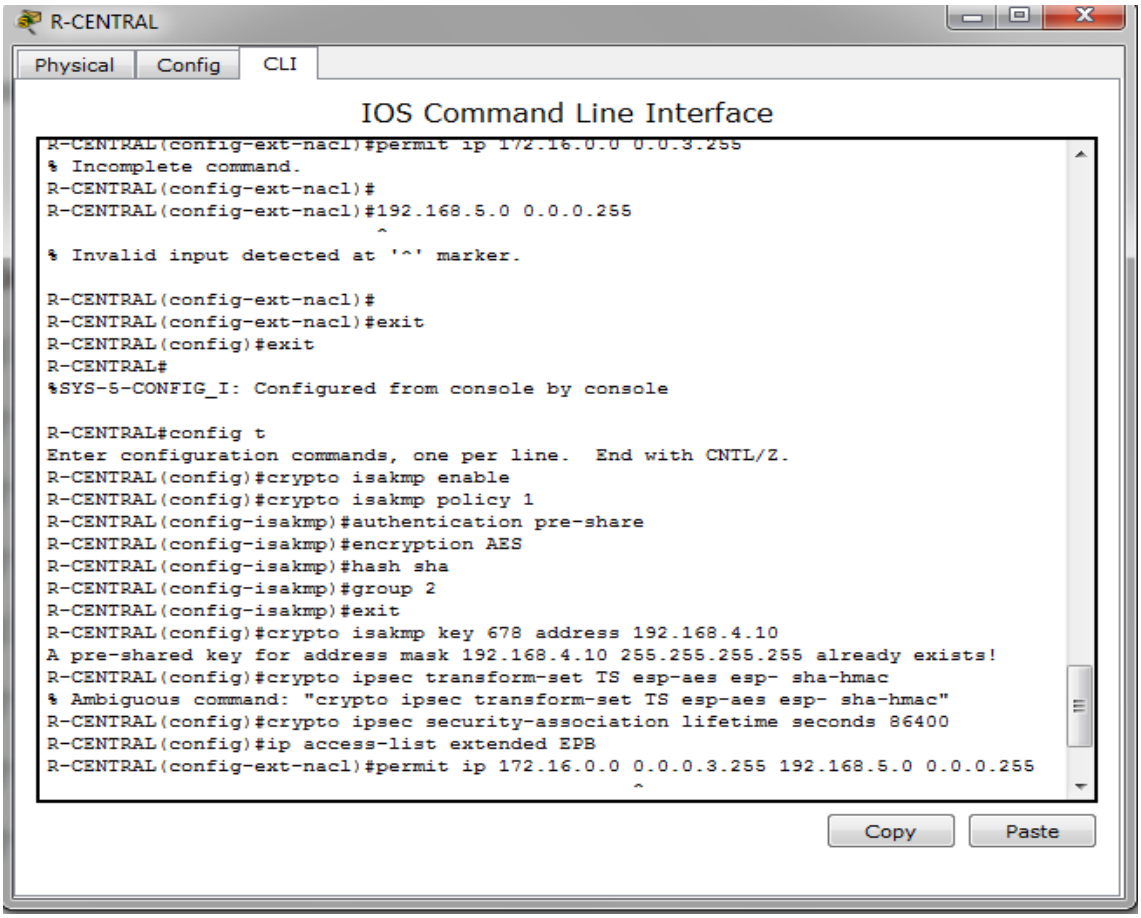
R-central(config)♯crypto ipsec transform-set TS esp-aes esp- sha-hmac
esp : Signifie Encapsulation Security Protocol

on utilise les mêmes protocoles d'encryptions et de Hash précédent :
Encryption : aes
Hash : sha
On fixe ensuite une valeur de Lifetime :
R-central(config)♯crypto ipsec security-association lifetime seconds 86400

•**Création d'ACL étendue**

Créez une ACL qui va déterminer le trafic autorisé

R-central(config)♯ip access-list extended EPB
R-central(config-ext-nacl)♯permit ip 172.16.0.0 0.0.3.255 192.168.5.0 0.0.0.255
R-Central(config- ext-nacl)♯exit



L'ACL étendue permettra de définir le trafic qui passera à travers le tunnel VPN, dans ce projet, le trafic d'un réseau à l'autre est : 172.16.0.0/22 à 192.168.5.0/24.

- **Créer crypto carte**

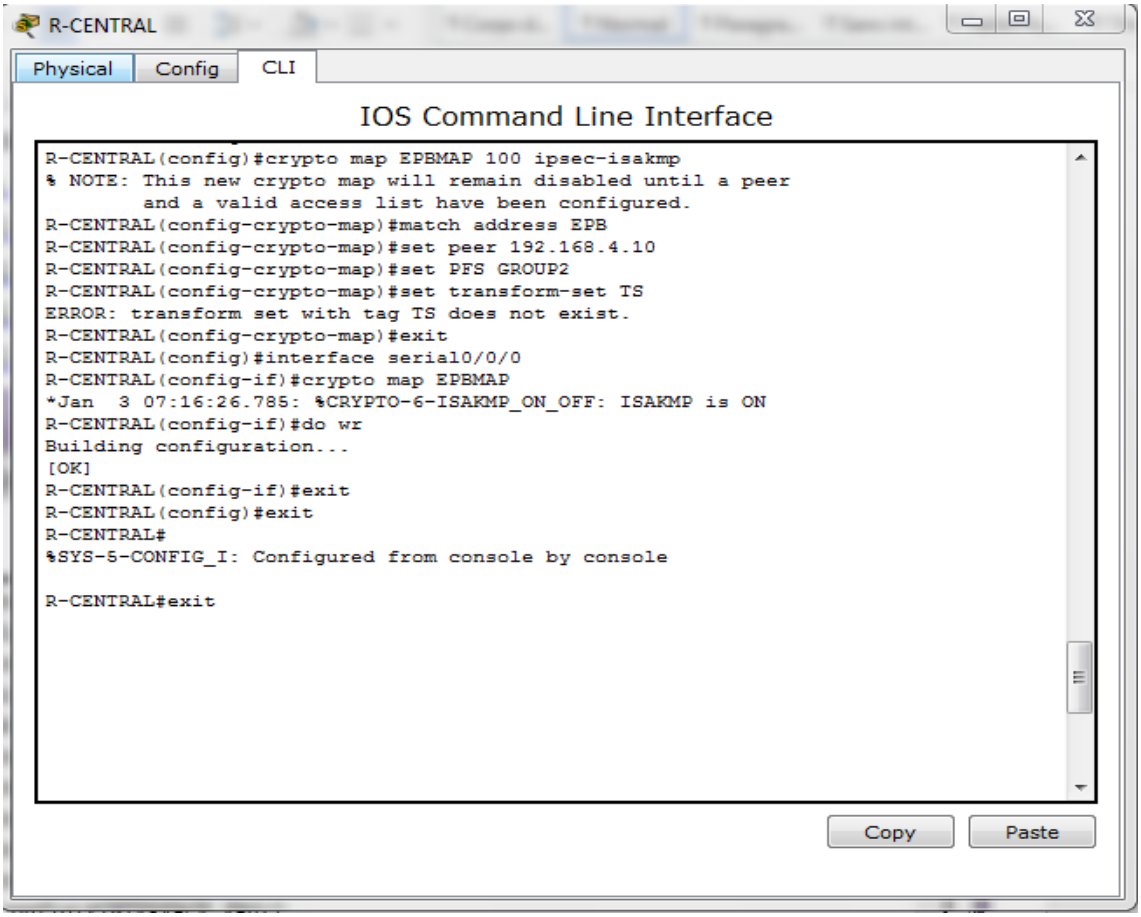
— La crypto MAP est la dernière étape de l'installation. Elle établit le lien entre ISAKMP définie précédemment et la configuration IPSec :

R-Central(config)♯crypto map EPBMAP 100 ipsec-isakmp
R-Central(config-crypto-map)♯match address EPB
R-Central(config-crypto-map)♯set peer 192.168.4.10
R-Central(config-crypto-map)♯set PFS GROUP2
R-Central(config-crypto-map)♯set transform-set TS
R-Central(config-crypto-map)♯exit

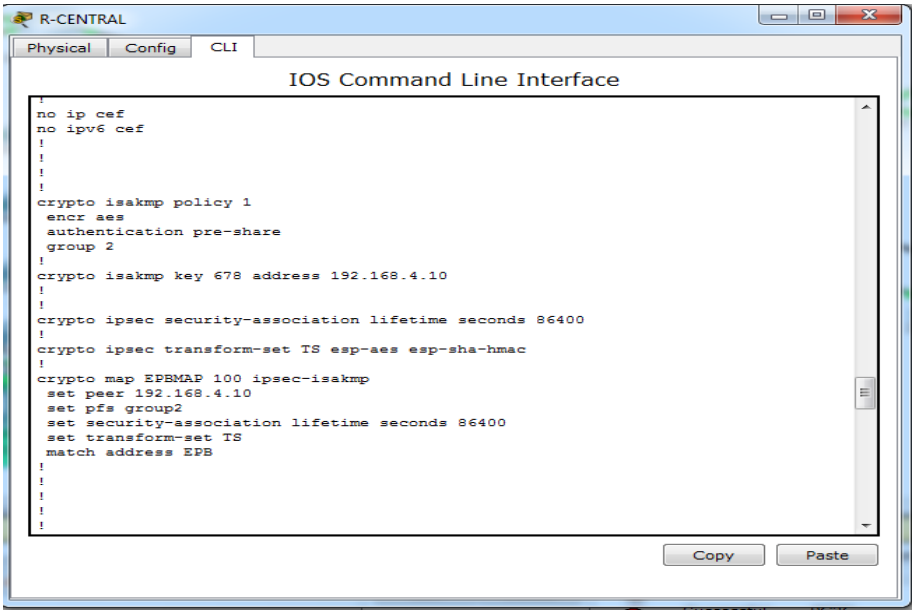
— Appliquer crypto carte à l'interface publique

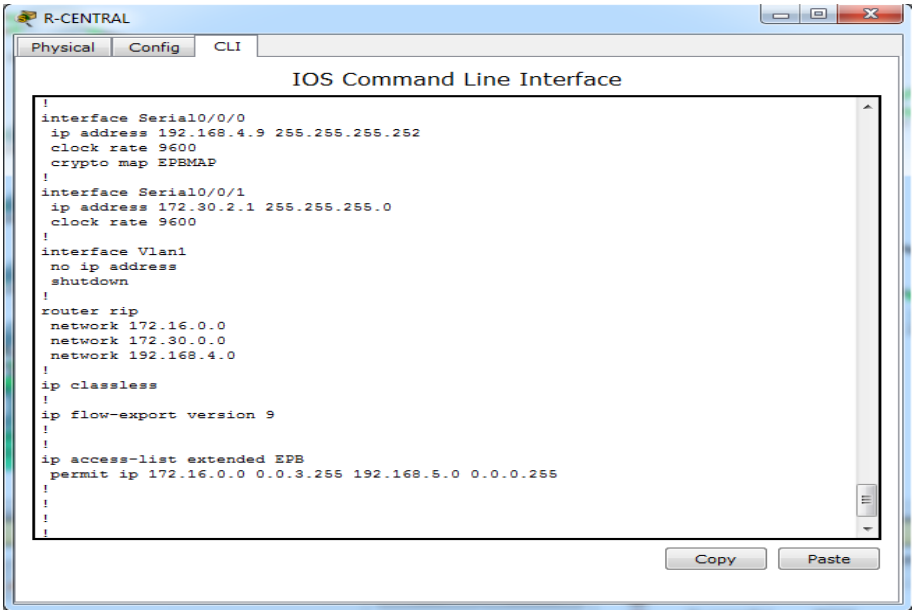
L'étape finale consiste a appliqué le crypto MAP sur l'interface de sortie de notre routeur :

R-Central(config)♯ interface Fa0/1
R-Central(config-if)♯crypto map EPBMAP
R-Central(config-if)♯do wr
R-Central(config-if)♯exit



R-Central ♯show run

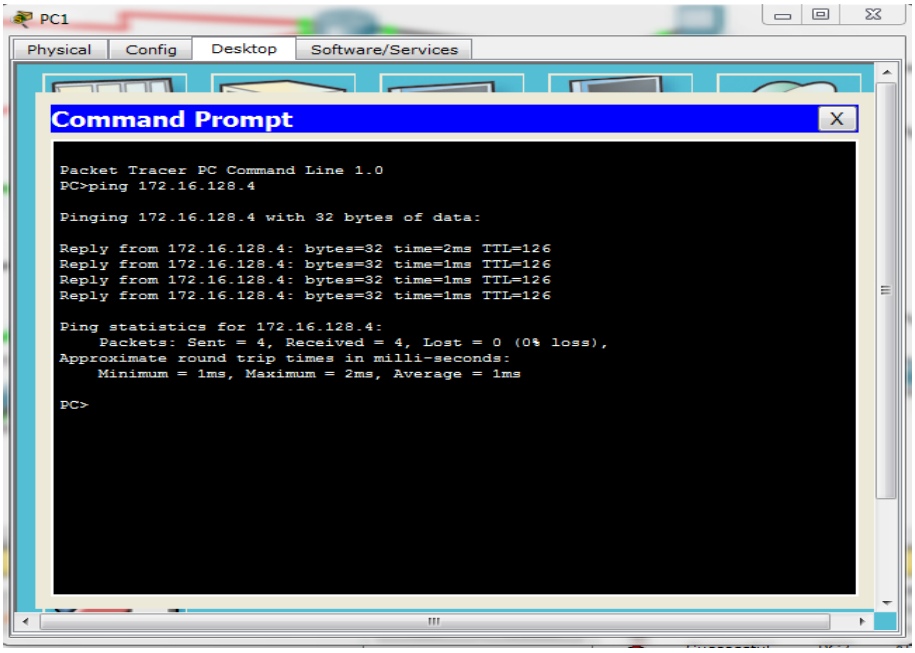


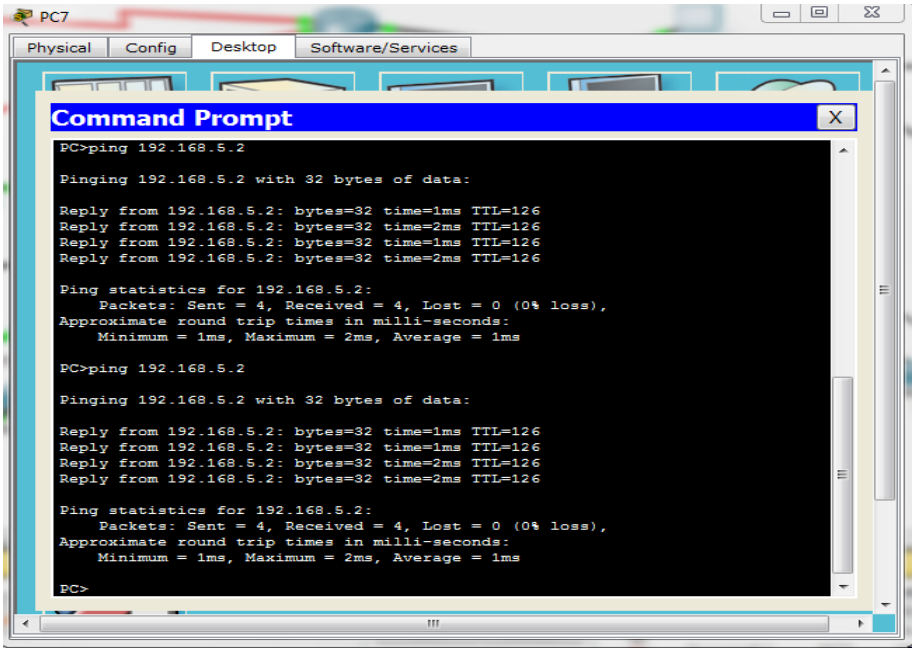


À ce stade, nous avons terminé la configuration du tunnel VPN IPSec sur le routeur du site 1 <R-Central>, les même étapes seront appliquées au routeur du site 2 <R-Aboudaou>. Les paramètres pour le routeur Aboudaou sont identiques, la seule différence étant les adresses IP par les pairs (sites) et les listes d'accès.

Phase III : Teste de Tunnel VPN IPsec

Réalisez un Ping entre le PC7 du site 1 et PC1 du site 2 et vice versa, afin de vérifier si la communication est établie :





•Vérifiez les informations retournées par le VPN sur R-CENTRAL et R-ABOUDAOU

```
R-CENTRAL#show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit


R-ABOUDAOU#show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
```

• la commande **'show crypto MAP'** pour afficher les cartes cryptographiques qui seront appliquées aux routeurs.

```
R-CENTRAL#SHOW CRYPTO MAP
Crypto Map EPBMAP 100 ipsec-isakmp
        Peer = 192.168.4.10
        Extended IP access list EPB
            access-list EPB permit ip 172.16.0.0 0.0.3.255 192.168.5.0 0.0.0.255
        Current peer: 192.168.4.10
        Security association lifetime: 4608000 kilobytes/86400 seconds
        PFS (Y/N): Y
        Transform sets={
                TS,
        }
        Interfaces using crypto map EPBMAP:
                Serial0/0/0


R-ABOUDAOU#SHOW CRYPTO MAP
Crypto Map EPBMAP 100 ipsec-isakmp
        Peer = 192.168.4.9
        Extended IP access list EPB
            access-list EPB permit ip 192.168.5.0 0.0.0.255 172.16.0.0 0.0.3.255
        Current peer: 192.168.4.9
        Security association lifetime: 4608000 kilobytes/86400 seconds
        PFS (Y/N): Y
        Transform sets={
                TS,
        }
        Interfaces using crypto map EPBMAP:
                Serial0/0/0
```

```
R-CENTRAL#show crypto ipsec transform-set
Transform set TS: {    { esp-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

```
R-ABOUDAOU#show crypto ipsec transform-set
Transform set TS: {    { esp-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

4.9 Conclusion

Au cours de ce chapitre, nous avons pu décrire la procédure de configuration concernant les VLANs et VPNs, sur le réseau local et le réseau Internet.

En effet, les résultats obtenus montrent que la segmentation du réseau local en 12 VLAN a offert une sécurisation des données échangées entre les différents départements de l'entreprise EPB, une amélioration de la gestion l'attribution d'adresses IP, ainsi qu'une meilleure organisation du réseau sans avoir eu recours au réaménagement des équipements.

L'application du VPN quant à elle, permet de sécuriser la liaison externe via le Tunnel VPN IP sec.

Ceci dit, il convient de mentionner que ces configurations restent « théoriques », car leur réalisation au sein de l'entreprise n'a pas encore pris place. Néanmoins, notre vérification et mise en œuvre à l'aide du simulateur Packet Tracer, confirment la fiabilité et l'efficacité des résultats obtenus.

Conclusion générale

Le secteur des technologies de l'information étant en constante mutation, le présent travail fait état des résultats de la mise en place d'un réseau VPN et d'une segmentation en VLAN. Grâce à ces technologies, nous permettrons aux employés de partager de façon sécurisée leurs données via le protocole IPSec qui est le principal outil permettant d'implémenter les VPNs, ce partage est possible en externe entre les utilisateurs dit « distants » situés en dehors du réseau local. L'intégration des VLANs quant à elle améliore les performances du réseau et offre une flexibilité ainsi qu'une facilité d'administration.

Notre travail est divisé en deux parties, à savoir l'approche théorique qui était subdivisé en deux chapitres dont le premier a porté sur les généralités des réseaux informatiques ; le second sur la sécurité des réseaux informatiques. La deuxième partie offre une présentation de l'organisme d'accueil et traite l'aspect pratique : la configuration des liaisons virtuelles (VPNs et VLANs).

Ce travail d'une part n'a pas été facile du point de vue conception car afin de simuler notre réseau, il fallait comprendre le fonctionnement des équipements Cisco et leurs fonctionnalités, comprendre les notions de VLANs et VPNs compliquées et apprendre à simuler avec le logiciel Pakcet Tracer.

La segmentation en VLAN simplifie l'administration et les modifications du réseau car toute l'architecture peut être modifiée par un simple paramétrage des commutateurs, elle présente aussi un gain en sécurité car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées. Comme le trafic réseau d'un groupe d'utilisateurs est confiné au sein du VLAN qui lui est associé, il en résulte une libération de bande passante, ce qui augmente les performances du réseau. Les Vlans apportent également une grande flexibilité dans la gestion des réseaux.

En effet, la mise en place de VPN permet aux réseaux privés de s'étendre et de se relier entre eux via internet. Cette solution mise en place est une politique de réduction des coûts liés à l'infrastructure réseau des entreprises. 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 et du système d'information qui progressent de façon exponentielle.

Les résultats obtenus lors des simulations effectuées sur le PACKET TRACER ont montré le bon fonctionnement du VLAN et VPN au sein de l'entreprise pour l'amélioration de la QoS, dans les réseaux informatiques.

Notons que ces résultats concordent avec les objectifs tracés au début de l'étude, à savoir, réduire la surcharge du réseau ainsi que sécuriser le partage entre les sites distants.

Ce travail a fait l'objet d'une expérience intéressante, qui nous a permis d'améliorer nos connaissances et nos compétences dans le domaine de sécurité des réseaux informatiques.

en guise de perspectives, on aimerai implémenter d'autres protocoles de sécurité tel que le AAA(Authentification, Authorization, Accounting)ou encore simuler sous une autre plate forme comme : GNS3 et Open Network.

Bibliographie

[1] *document interne de l'EPB.*

[2] BOUKRAM A. *Introduction à la Sécurité Informatique,Département Informatique, Université de Bejaia.* 2015.

[3] Steven Andrés, Brian Kenyon, and Erik Pack Birkholz. *Security Sage's guide to hardening the network infrastructure.* Syngress, 2004.

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

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

[6] TOUAZI DJ. . *Conception et réalisation d'une segmentation logique dynamique et portable du réseau intranet de l'université de béjaia.* 2012.

[7] Richard Froom, Balaji Sivasubramanian, and Erum Frahim. *Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide : Foundation Learning for SWITCH 642-813.* Cisco Press, 2010.

[8] Etienne GALLET DE SANTERRE. Protocole l2tp. *Techniques de l'ingénieur. Télécoms*, (TE7579), 2006.

[9] Didier Godart. *Sécurité informatique : risques, stratégies et solutions.* Edipro, 2002.

[10] Antoine Joux. *La réduction des réseaux en cryptographie.* Ecole Normale Supérieure (Paris). Laboratoire d'Informatique, 2004.

[11] Stephen Kent. Ip encapsulating security payload (esp). 2005.

[12] Todd Lammle and William Tedder. *CCNA Routing and Switching Deluxe Study Guide : Exams 100-101, 200-101, and 200-120.* John Wiley & Sons, 2014.

[13] Ali Larab, Pierre Gaucher, and Patrick Martineau. Intégration du protocole ipsec dans un réseau domestique pour sécuriser le bloc des sous-réseaux fan. 2010.

[14] Philippe Latu. Technologie rnis. 2000.

[15] Dale Liu. *Cisco CCNA/CCENT Exam 640-802, 640-822, 640-816 Preparation Kit*. Syngress, 2009.

[16] Philippe Mathon. *Windows Server 2003 : les services réseaux TCP/IP*. Editions ENI, 2003.

[17] Adrien Miller and Philippe Jean Dit Pannel. Sécurité avec ip : Les solutions. 2003.

[18] Jöelle MUSSET. Sécurité informatique : Ethical hacking : Apprendre l'attaque pour mieux se défendre, 2009.

[19] Guy Pujolle. *Cours réseaux et tél écoms*. Edition Eyrolles, Paris, 2004.

[20] Vincent Remazeilles. *La sécurité des réseaux avec Cisco*. Editions ENI, 2009.

[21] Ahmed ROUANE. Sécurité de réseau. 2010.

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

[23] François Santy. La virtualisation, 2013.

[24] Khaled TRABELSI and Haythem AMARA. *Mise en place des réseaux LAN interconnectés en redondance par 2 réseaux WAN*. PhD thesis, Université Virtuelle de Tunis, 2011.

[25] Andy Valencia, Morgan Littlewood, and Tim Kolar. Cisco layer two forwarding (protocol)" l2f". Technical report, 2001.

[26] L Xavier and K Thomas. Reseaux privés virtuels-vpn. frameip tcpip, 2004.

Résumé

La virtualisation du réseau permet de combiner des ressources matérielles et logicielles dans une seule unité administrative. L'objectif de notre travail consiste à implémenter une solution en utilisant les liaisons virtuelles afin de segmenter et sécuriser le réseau intranet de l'entreprise portuaire de Bejaia « EPB ». Nous avons choisis de simuler avec PACKET TRACER, afin de fournir aux différentes directions de l'EPB un partage efficace en utilisant le VTP qui permet de gérer de façon centralisé les VLANs, et d'augmenter la sécurité en créant des réseaux privés virtuels VPNs, associé au protocole de tunneling IPSEC.

Mots clés : VLAN, VPN, VTP, protocole de tunneling, IPSEC, PACKET TRACER.

Abstract

The virtualisation of the network consists in combining material and software resources in a single administrative unit. The objective of our work consists in implementing a solution by using the virtual connections to segment and reassure the intranet network of the harbour company of Bejaia " EPB". We chose to simulate with PACKET TRACER, to supply in the various directions managements of the EPB an effective division sharing by using the VTPs who allows to manage in a way centralized the VLANs, and to increase the safety security by creating a virtual private network VPN associated with the protocol of tunneling IPSEC.

Keywords : VLAN, VPN, VTP, protocole de tunneling, IPSEC, PACKET TRACER.