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

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

Mémoire de Fin de cycle

En vue d'obtention du diplôme de master professionnel en informatique spécialité : Administration et Sécurité des Réseaux Informatiques

Thème

Etude et amélioration de l'infrastructure réseau de l'EPB (VLAN, serveur de messagerie ZIMBRA)

Réalisé par :

M^elle^ **FETTOUS** Amel et M.**MADI** Lyes.

Soutenu le 28/06/2016 devant le jury composé de :

Président	M. A. BAADACHE	MAC B	U.A/Mira Bejaïa
Examinatrice	M^me^. S. BOUKERRAM	MAC A	U.A/Mira Bejaïa
Examinateur	M. F. BOUCHEBAH	Doctorant	U.A/Mira Bejaïa
Encadreur	M. A/Kamel. TARI	Professeur	U.A/Mira Bejaïa
Co-Encadreur	M. N. RAGAB	Doctorant	U.A/Mira Bejaïa

Promotion 2016/2017

Dédicaces

Je dédie mon travail à mes très chers et respectueux parents

Qui m'ont soutenu tout en long de ma vie ainsi qu'à ma sœur Sara et mon frère Toufik

À mes grands-parents, mes cousins et cousines, Oncles et tantes

À mon binôme Lyes ainsi que sa famille

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

Amel

Je dédie mon travail à mes très chers et respectueux parents,

À mes frère et sœurs, mes beaux-frères et belles sœurs et neveux,

À ma précieuse famille, mes cousins et cousines, Oncles et tantes, À mon binôme Amel ainsi que sa famille

À mes amis et collègues

Et à toutes les personnes qui m'ont aidé, un grand MERCI à tous.

Lyes

Remerciements

***N**ous 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.*

***N**ous exprimons notre reconnaissance à Monsieur **TARI A/kamel** ainsi qu'à Monsieur **EL SAKAAN Nadim** d'avoir joué pleinement leur rôle de promoteur en étant à nos côtés tout au long de l'étude de notre projet, leurs conseils et orientations nous ont guidés jusqu'à l'aboutissement de ce travail.*

***N**ous remercions également **M. HADJAL Riad** directeur de la capitainerie et **M. BETTACHE IDIR** directeur de la direction des systèmes d'informations*

*Et **M. MAKHLOUFI Hichem** ainsi qu'à **M. BONDRA Said** administrateurs réseau au niveau de la direction système d'information au sein de l'entreprise portuaire de Bejaia durant notre stage pour leur aide, leur patience et leurs remarques pertinentes qui ont apporté une amélioration certaine à notre travail.*

***N**ous remercions aussi **Dr BAADACHE Abderrahmane** d'avoir accepté de présider le jury de notre soutenance. Ainsi qu'aux membres de jury constitué de : **M. BOUCHEBAH Fatah** et **Dr. BOUKERRAM S.** d'avoir accepté de juger ce modeste travail.*

***N**os 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.*

***E**nfin, 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.*

Amel & Lyes

Liste des abréviations

ACL	Access Control List.
AD	Active Directory.
ARP	Address Resolution Protocol.
BDD	Base De Données.
BS	British Standard
DC	Direction Capitainerie.
DC	Domain Controller.
DDD	Direction Domaine et du Développement.
DFC	Direction des Finance et Comptabilité.
DGAF	DG Adjoint Fonctionnelle.
DGAO	DG Adjoint Opérationnelle.
DL	Direction de la Logistique.
DMA	Direction Manutention et Acconage.
DMZ	Zone démilitarisé.
DNS	Domain Name System.
DR	Direction Remorquage.
DRH	Direction des Ressources Humaines.
EPB	Entreprise Portuaire de Bejaia.
FAI	Fournisseur d'Accès Internet.
FTP	File Transfer Protocol.
GSM	global system for mobile
HTTP	Hyper Text Transfer Protocol.
HTTPS	Hyper Text Transfer Protocol Secure.
ICMP	Internet Control Message Protocol.
IDS	Intrusion Detection System.
IEEE	Institute of Electrical and Electronics Engineers.
IMAP	Internet Message Access Protocol.
IP	Internet Protocol.
ISO	International Organization for Standardization.
LAN	Local Area Network.
MAN	Metropolitan Area Network.
MDA	Mail Delivery Agent.
MTA	Mail Transport Agent.

MUA	Mail User Agent.
MX	Mail eXchanger.
MY SQL	Structured Query Language.
OHSAS	Occupational Health and Safety Advisory Services.
PAN	Personal Area Network.
PDA	Personal Digital Assistant.
PHP	Hypertext Preprocessor.
POP	Post Office Protocol.
POP3	Post Office Protocol Version 3.
PC	Personel Computer.
RAID	Redundation Array of Inexpensive Disks.
RJ45	Registred Jack 45.
SMTP	Simple Mail Transfer Protocol.
SSL	Secure Sockets Layer.
SSH	Secureb SHell
STP	Shielde Twisted Paire.
TCP	Transmission Control Protocol.
UTP	Unshielded Twisted Pair.
VLAN	Virtual Local Area Network.
VPN	Virtual Private Network.
VTP	VLAN Trunking Protocol.
VM	Virtual Machine
WAN	Wide Area Network.
WIFI	Wireless Fidelity.
WIMAX	Worldwide Interoperability for Microwave Access.

Table des matières

Table des figures

Liste des tableaux

Introduction générale

L'histoire de la communication est aussi ancienne que l'histoire de l'humanité. Depuis les origines, l'homme a eu besoin de communiquer. Pour cela il n'a cessé de développer la technologie afin de se procurer un réseau de communication plus vaste tout en essayant d'assurer la sécurité de cette dernière.

Toutefois la messagerie électronique est devenue le moyen incontournable pour l'échange d'informations. En effet l'e-mail est aujourd'hui une solution universelle utilisée par tous (particuliers et professionnels).

Il demeure entendu que les serveurs de messagerie locaux sont de plus en plus un élément d'infrastructure essentiel des systèmes d'information. Dans les entreprises, les bases de données prenant en charge les applications critiques des systèmes de messageries (courrier électronique, planification et gestion des calendriers) augmentent en taille et prennent une importance croissante.

Par ailleurs le réseau représente une notion évidente dans toute entreprise. Car on y effectue régulièrement des échanges d'informations véhiculées dans les réseaux. l'importance de ces données exige une bonne gestion du réseau, une souplesse d'utilisation et un certain degré de sécurité.

Les performances réseau constituent un facteur important dans la productivité d'une entreprise, l'une des technologies permettant de les améliorer consiste à diviser de vastes domaines de diffusions en domaines plus petits.

Dans un inter-réseau commuté, les VLANs permettent la segmentation et assouplissent l'organisation et offrent un moyen de regrouper des périphériques dans un LAN.

Ainsi, l'organisation et la sécurité de la hiérarchie architecturale du réseau de l'entreprise portuaire de Bejaïa (EPB) aurait un certain déséquilibre, ce qui nous a amené à mettre en place un plan commençant par l'étude de l'organisme d'accueil puis trouver les solutions possibles pour intervenir aux besoins de l'établissement.

En effet, ce plan a pour objectif d'améliorer et d'optimiser le réseau dans le but d'apporter une bonne gestion et protection aux ressources partagées de l'EPB.

Dans notre projet, on retrouvera toutes les stratégies prévues pour compléter les lacunes qu'on a pu déceler au niveau de l'organisme des réseaux informatiques, ainsi que les outils qui nous ont permis de mettre en œuvre nos solutions proposées.

CHAPITRE 1

GÉNÉRALITÉS SUR LES RÉSEAUX ET LA SÉCURITE

Introduction

De nos jours, les réseaux informatiques jouent un rôle important dans le monde plus particulièrement l'espace professionnel. En effet, il permet de relier entre un ensemble d'ordinateurs et de périphériques ainsi de faire circuler des informations entre eux.

Bien que les réseaux informatiques soient importants dans le monde du travail, mais ils restent incomplets sans sécurité. Tous les types de réseau informatiques ont besoin de sécurité afin de protéger la confidentialité des données.

Dans ce chapitre, nous allons présenter d'une manière générale les réseaux informatiques et les différentes attaques qui pourraient les affecter .Ensuite, donnerons les moyens et les stratégies qui permettront de faire face à ces menaces.

1.1 Les réseaux informatiques des entreprises

1.1.1 Définition d'un Réseau informatique

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à des lignes de communication (câbles réseaux, etc.) et des éléments matériels tels que les cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données .Tout celà, dans le but d'échanger des informations [1].

1.1.2 Les différents types de réseaux d'entreprise

Il existe différents types de réseaux qu'on caractérise selon leur divers critères tels que: leur tailles, leur vitesses de transfert des données et leur étendus [1].

- **Les réseaux personnels, ou PAN (Personnel Area Network) :**

Interconnectent sur quelques mètres des équipements personnels tels que les terminaux GSM, portables, etc. d'un même utilisateur [1].

- **Les réseaux locaux, ou LAN (Local Area Network) :**

Un réseau LAN permet de connecter deux ou plusieurs centaines de machines à l'intérieur d'une même enceinte (Entreprise, administration, etc.), sur de courte distance (quelques kilomètres au maximum). On fait généralement appel à la technologie Ethernet pour relier les postes de travail [1].

- **Les réseaux métropolitains, ou MAN (Métropolitain Area Network) :**

Interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un MAN permet à deux équipements 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) [1].

- **Les réseaux étendus, ou WAN (Wide Area Network) :**

Sont des réseaux destiné à transporter des données à l'échelle d'un pays voir même d'un continent ou de plusieurs continents. Le réseau est soit terrestre, il utilise dans ce cas une infrastructure au niveau de sol essentiellement de grands réseaux de fibre optiques, soit hertzien, comme le réseau satellitaire [1].

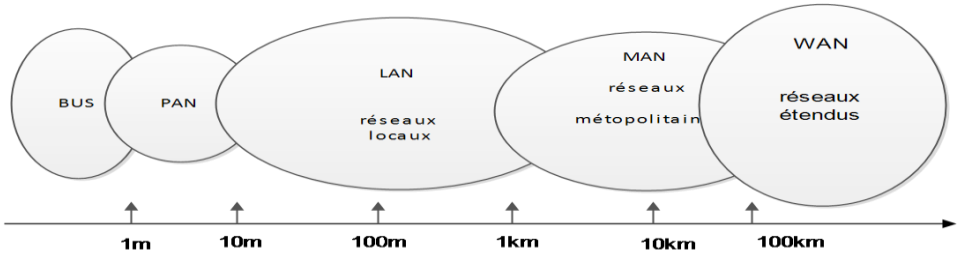

Figure 1. 1– Catégories des réseaux informatiques [1].

1.1.3 L'architecture des réseaux d'entreprise

On distingue également deux catégories de réseaux :

- **Les réseaux Post à post (peer to peer= P2P)**

Le logiciel client et le logiciel serveur sont généralement exécutés sur des ordinateurs distincts, mais un seul ordinateur peut tenir simultanément ces deux rôles. Dans le cas des réseaux de particuliers et de petites entreprises, il arrive souvent que les ordinateurs fassent à la fois office de serveur et de client sur le réseau. Ce type de réseau est appelé réseau Peer to peer [2]. voir la (Figure 1.2)

- **Les réseaux client-serveur :**

Tous les ordinateurs connectés à un réseau et qui participent directement aux communications transmises sur le réseau sont périphériques finaux. Les serveurs sont des ordinateurs équipés de logiciels leur permettant de fournir des informations, comme des messages électroniques ou des pages web, à d'autres périphériques finaux sur le réseau. Chaque service nécessite un logiciel serveur distinct. Les clients sont des ordinateurs équipés d'un logiciel qui leur permet de demander des informations auprès du serveur et de les afficher. Un navigateur web, tel que Chrome ou Firefox, est un exemple de logiciel client [2]. Voir la (Figure 1.2)

P2P Client/serveur

Figure 1. 2 : « Architecture des réseaux [2]»

1.1.4 Les topologies des réseaux

1.1.4.1 Topologie en bus

Une topologie en bus 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. Le mot « bus » désigne la ligne physique qui relie les machines du réseau.

Cette topologie a pour avantage d'être facile à mettre en œuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté [1]. (Figure1.3).

1.1.4.2 Topologie en anneau

Dans un réseau possédant une topologie en anneau, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour.

En réalité, dans une topologie anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un répartiteur (appelé MAU, Multistation Access Unit) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre-eux un temps de parole.

Les deux principales topologies logiques utilisant cette topologie physique sont Token ring (anneau à jeton) et FDDI. [1] (Figure1.3)

1.1.4.3 Topologie en étoile

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur (en anglais hub, littéralement moyen de roue). Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions.

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau. Le point sensible de ce réseau est le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est possible [1]. (Figure1.3)

1.1.4.4 Topologie en Maille

Une topologie maillée, est une évolution de la topologie en étoile, elle correspond à plusieurs liaisons point à point. Une unité réseau peut avoir (1,N) connexions point à point vers plusieurs autres unités. Chaque terminal est relié à tous les autres.

L'inconvénient est le nombre de liaisons nécessaires qui devient très élevé.
Cette topologie se rencontre dans les grands réseaux de distribution (Exemple : Internet). L'information peut parcourir le réseau suivant des itinéraires divers, sous le contrôle de puissants superviseurs de réseau, ou grâce à des méthodes de routage réparties.

L'armée utilise également cette topologie, ainsi, en cas de rupture d'un lien, l'information peut quand même être acheminée [1]. (Figure1.3).

1.1.4.5 Topologie en Arbre

Aussi connu sous le nom de topologie hiérarchique, le réseau est divisé en niveaux. Le sommet, le haut niveau, est connectée 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.

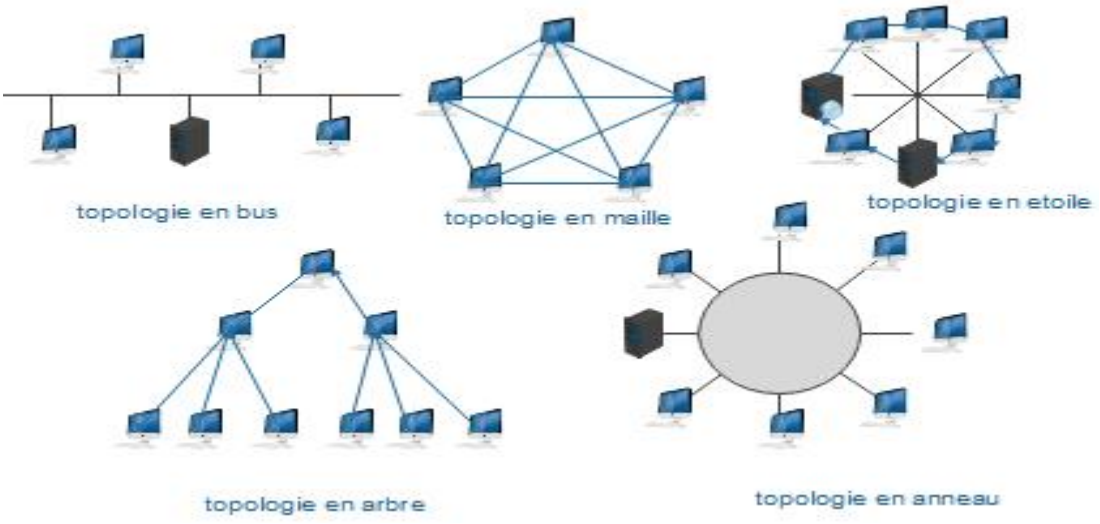

Figure 1. 3 : « Topologies réseaux [2] *»*

1.2 Composants matériels d'un réseau d'entreprise

1.2.1 Equipements d'interconnexion

Voici les équipements qui peuvent rentrer dans la composition d'un réseau d'entreprise [3] :

- **La carte réseau**

  Elle constitue l'interface physique entre l'ordinateur et le câble réseau. Les données transférées du câble à la carte réseau sont regroupé en paquets composé d'un entête qui contient les informations d'emplacement et des données d'utilisateurs. Souvent la carte réseau est intégrée dans la carte mère.

- **Le concentrateur**

  Un concentrateur (appelé Hub en anglais) est un élément matériel permettant de concentrer le trafic réseau provenant de plusieurs hôtes, et de régénérer le signal

- **Le répéteur**

Un répéteur (en anglais repeater) est un équipement simple permettant de régénérer un signal entre deux nœuds du réseau, afin d'étendre la distance de câblage d'un réseau. Le répéteur travaille uniquement au niveau physique (couche 1 du modèle OSI).

- **Les ponts**

Un pont (Bridge) est un dispositif matériel permettant de relier des réseaux travaillant avec le même protocole. Ainsi, contrairement au répéteur, qui travaille au niveau physique, le pont travaille également au niveau logique (au niveau de la couche 2 du modèle OSI).

- **Le commutateur**

Un commutateur (en anglais Switch) permet de relier plusieurs ordinateurs entre eux. C'est un pont multiport, c'est-à-dire qu'il s'agit d'un élément actif agissant au niveau 2 du modèle OSI.

- **La passerelle**

Une passerelle applicative (en anglais « gateway ») est un système matériel et logiciel permettant de faire la liaison entre deux réseaux, afin de faire l'interface entre des protocoles réseau différents.

- **Le routeur**

Le routeur est un appareil qui relie des réseaux et achemine les informations d'un émetteur vers un destinataire selon une route. Il permet de déterminer le chemin qu'un paquet de données va emprunter.

- **Le modem (modulateur démodulateur)**

Le modem est un périphérique qui permet de transmettre et de recevoir les données sous forme d'un signal. Il transforme les signaux analogiques en numériques et inversement, ces signaux sont acheminés par une ligne téléphonique.

1.2.2 Supports de transmissions

Il existe plusieurs types de support de transmission nous allons décrire quelques-uns ci-dessous [4] :

- **câble coaxial**

Un câble coaxial se compose d'un conducteur de cuivre entouré d'une couche de matériau isolant flexible.

- Un câble coaxial se compose d'un conducteur de cuivre entouré d'une couche de matériau isolant flexible.
- Vitesse et débit : 10 à 100Mbit/s.
- Cout : économique
- Taille du connecteur et du média : moyenne.
  Longueur de câble maximale : 500 m.

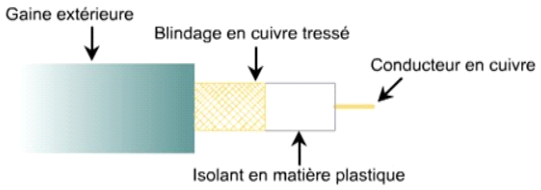

Figure 1. 4 : « câble coaxial [1]»

- **Câble à paires torsadées blindées (STP)**

Le câble à paires torsadées blindées allie les techniques de blindage, d'annulation et de torsion des fils. Chaque paire de fils est enveloppée dans une feuille métallique et les deux paires sont enveloppées ensemble dans un revêtement tressé ou un film métallique.

- Vitesse et débit : 0 à 100Mbit/s.
- Cout : modéré.
- Taille du connecteur et du média : moyenne a grande.
- Longueur de câble maximale : 100 m.

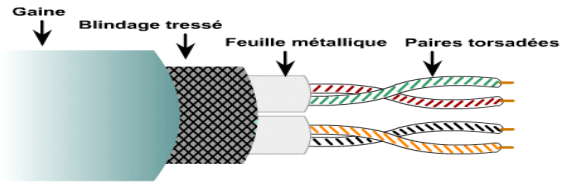

Figure 1. 5 : « Câble à paires torsadées blindées (STP) [1]» »

- **Câble à paires torsadées non blindées (UTP)**

Est un média constitué de quatre paires de fils, présent dans divers types de réseau. Chacun des huit fils de cuivre du câble est protégé par un matériau isolant. De plus, les paires de fils sont tressées entre elles. Ce type de câble repose uniquement sur l'effet d'annulation produit par les paires torsadées pour limiter la dégradation du signal due aux interférences électromagnétiques et radio.

- Vitesse et débit : 10-100-1000 Mbit/s.
- Cout : le moins onéreux.
- Taille du connecteur et du média : petite.
- Longueur de câble maximale : 100 m.

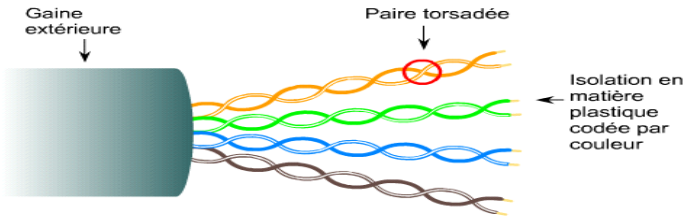

Figure 1. 6 : « Câble à paires torsadées non blindées (UTP) [1] »

- **Fibre optique**

Le cœur d'une fibre optique est la partie dans laquelle circulent les rayons lumineux. Chaque câble à fibre optique utilisé dans les réseaux comprend deux fibres de verre logées dans des enveloppes distinctes. Une fibre transporte les données transmises depuis l'équipement A vers l'équipement B. Il existe deux types de fibre monomode et multimode.

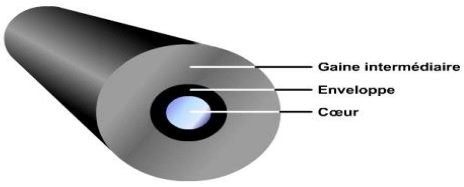

Figure 1. 7 : « *Fibre optique* [1] »

- **Transmission sans fil**

Le Wi-Fi ou wifi est un ensemble de protocoles de communication sans fil régis par les normes du groupe IEEE 802.11 (ISO/CEI 8802-11). Un réseau Wi-Fi permet de relier par ondes radio plusieurs appareils informatiques (ordinateur, routeur, smartphone, décodeur Internet, etc.) au sein d'un réseau informatique afin de permettre la transmission de données entre eux.

- **Périphériques finaux**

Les périphériques réseau auxquels les gens sont le plus habitués sont appelés périphériques finaux, ou hôtes. Ces périphériques forment l'interface entre les utilisateurs et le réseau de communication sous-jacent. Voici quelques exemples de périphériques finaux [2] :

- Ordinateurs.
- Imprimantes réseau.
- Téléphones VoIP.
- Caméras de surveillance.
- Appareils mobiles (tels que les smartphones, tablettes, PDA, les lecteurs de cartes bancaires et les scanners de codes-barres sans fil).
- Serveur (physique ou virtuel).

1.2.3 Le modèle de référence OSI

Le modèle de référence OSI (Open System Interconnexion) définit une sorte de langage commun. Ce modèle a été mis au point par l'ISO (Organisation Internationale des Standards) et il est devenu le socle de référence pour tout système de traitement de communications. Il repartit les questions relatives au domaine des communications informatiques selon sept couches classées par ordre d'abstraction croissant. Son objectif est d'assurer que les protocoles spécifiques utilisés dans chacune des couches coopèrent pour assurer une communication efficace. Décrivons succinctement le rôle de chaque couche [5] :

- **Physique** : Elle convertit les signaux électriques en bits de données et inversement, selon qu'elle transmet ou reçoit les informations à la couche liaison.
- **Liaison** : Elle est divisée en deux sous-couches :

  -La couche MAC qui structure les bits de données en trames et gère l'adressage des cartes réseaux.

  -La couche LLC qui assure le transport des trames et gère l'adressage des utilisateurs, c'est à dire des logiciels des couches supérieures.
- **Réseau** : Elle traite la partie donnée utile contenue dans la trame. Elle connait l'adresse de tous les destinataires et choisit le meilleur itinéraire pour l'acheminement. Elle gère donc l'adressage logique et le routage.
- **Transport** : Elle segmente les données de la couche session, prépare et contrôle les tâches de la couche réseau. Elle peut multiplier les voies d'accès et corriger les erreurs de transport.
- **Session** : Son unité d'information est la transaction. Elle s'occupe de la gestion

et la sécurisation du dialogue entre les machines connectées, les applications et les utilisateurs (noms d'utilisateurs, mots de passe, etc.)

- **Présentation** : Elle convertit les données en information compréhensible par les applications et les utilisateurs : syntaxe, sémantique, conversion des caractères graphiques, format des fichiers, cryptage, compression.
- **Application** : C'est l'interface entre l'utilisateur ou les applications et le réseau. Elle concerne la messagerie, les transferts et partages de fichiers, l'émulation de terminaux.

La figure illustre les couches du modèle OSI et leurs protocoles

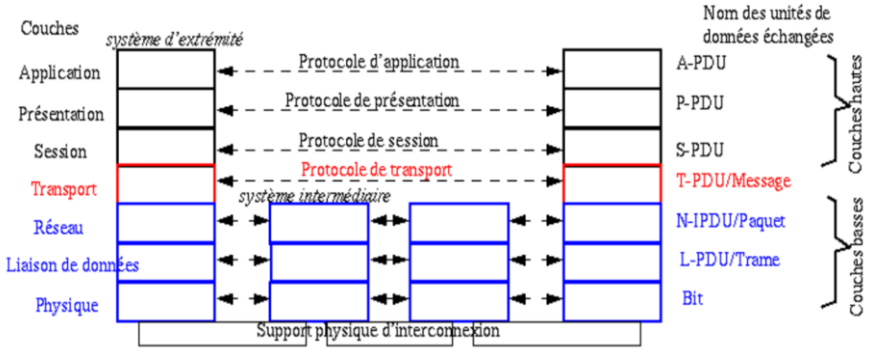

Figure 1.8: « *Les couches du modèle OSI et leurs protocoles* [5]»

1.2.4 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 il contient uniquement quatre. Les trois couches supérieures du modèle OSI sont souvent utilisées par une même application [5,6]. Le schéma de la figure 1.9 nous montre la différence entre le modèle TCP/IP et le modèle OSI.

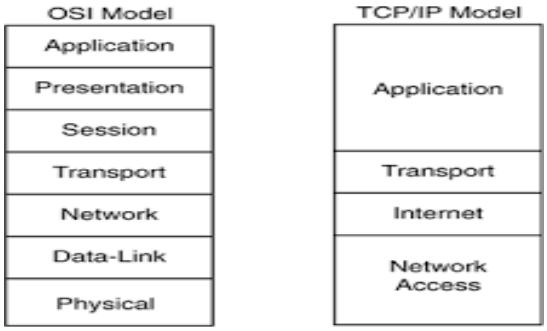

Figure 1. 9 : « *Comparaison entre le modèle TCP/IP et le modèle OSI* [5]»

1.3 La sécurité des réseaux d'entreprise

1.3.1 Définition de la sécurité informatique

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Elle s'occupe de la prévention d'actions non autorisées par les utilisateurs d'un système informatique. [5].

1.3.2 Les attaques réseaux

Les attaques réseaux s'appuient sur des vulnérabilités liées directement aux protocoles ou à leur implémentation. Il en existe un grand nombre. Néanmoins, la plupart d'entre elles ne sont que des variantes des cinq attaques réseaux les plus connues aujourd'hui.

1.3.3 Faiblesse des protocoles

Quelques protocoles réseaux n'ont pas été conçus pour tenir compte des problèmes de sécurité. Les principales attaques qui se propagent dans ce type de faiblesse sont :

- **Attaque par fragmentation**

C'est une attaque réseau par saturation exploitant le principe de fragmentation du protocole IP. En effet, le protocole IP est prévu pour fragmenter les paquets de taille importante en plusieurs paquets IP possédant chacun un numéro de séquence et un numéro d'identification commun. A la réception des données, le destinataire réassemble les paquets grâce aux valeurs de décalage qu'ils contiennent. L'attaque par fragmentation la plus célèbre est l'attaque Teardrop. Le principe de l'attaque Teardrop consiste à insérer dans des paquets fragmentés des informations de décalage erronées. Ainsi, lors du réassemblage il existe des vides ou des recoupements (overlapping), pouvant provoquer une instabilité du système. A ce jour, les systèmes récents ne sont plus vulnérables à cette attaque [7].

- **Attaque par déni de service**

C'est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou ressources d'une organisation. Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et

consultés. Les attaques par déni de service sont un fléau pouvant toucher tout serveur d'entreprise ou tout particulier relié à internet. Le principe des attaques par déni de service consiste à envoyer des paquets IP ou des données de taille ou de constitution inhabituelle, afin de provoquer une saturation ou un état instable des machines victimes et de les empêcher ainsi d'assurer les services réseau qu'elles proposent. le but d'une telle attaque n'est pas de récupérer ou d'altérer des données, mais de nuire à la réputation de sociétés ayant une présence sur internet et éventuellement de nuire à leur fonctionnement si leur activité repose sur un système d'information [7].

1.3.4 Faiblesse d'authentification

Les protocoles IP ou ICMP, manquent de système d'authentification, dès lors elles sont l'objet des attaques qui se basent sur ces faiblesses. Les principales attaques sont :

- **Attaque ARP**

C'est une technique d'attaque simple qui consiste à exploiter les lacunes du protocole ARP, c'est ce qu'on appelle couramment l'empoisonnement de cache ARP, elle exploite la lacune de non authentification des requêtes. En effet, rien n'indique à une machine qu'une requête provient effectivement d'une machine avec laquelle elle communique [8].

- **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. La plupart des attaques de type « man in the middle » consistent à écouter le réseau à l'aide d'un outil appelé sniffer [7].

- **Attaque par réflexion**

Est basée sur l'utilisation de serveurs de diffusion (broadcast) pour paralyser un réseau. Le principe de cette attaque c'est que l'attaquant va essayer de trouver une liste de serveurs de diffusion et à falsifier l'adresse de réponse afin de les diriger vers la machine cible [7].

- **Attaque par Rejeu de message**

C'est 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. Ainsi, selon le contexte, le pirate peut bénéficier des droits de l'utilisateur [7].

1.3.5 Faiblesse d'implémentation

Parmi les attaques qui exploitent ce genre de faiblesse on trouve :

- **Attaque du Ping de la mort**

«L' attaque du ping de la mort » (en anglais « ping of death ») est une des plus anciennes attaque réseau. Le principe du ping de la mort consiste tout simplement à créer un datagramme IP dont la taille totale excède la taille maximum autorisée (65536 octets). Un tel paquet envoyé à un système possédant une pile TCP/IP vulnérable, provoquera un plantage. Plus aucun système récent n'est vulnérable à ce type d'attaque [7].

1.3.6 Faiblesse de configuration

Une mauvaise configuration des équipements réseau, pare-feu, routeur...etc. est souvent exploitée pour mener des attaques. Les erreurs de configuration peuvent être de plusieurs natures, incluant l'erreur humaine, par conséquent les équipements réseau ne doivent accédés ou configurés que par des acteurs autorisés [13].

1.4 Définition d'une politique de sécurité réseau :

La politique de sécurité informatique d'une entreprise prend la forme d'un plan d'actions visant à protéger la société et ses données essentielles, en déterminant des objectifs à atteindre pour contrer les principaux risques auxquels elle est confrontée :

- Une panne du réseau interne.
- L'infiltration de virus, vers ou chevaux de Troie affectant le matériel.
- Une menace intérieure causée par l'insouciance ou la malhonnêteté [9].

1.4.1 Les différents type de politique de sécurité réseaux

Une politique de sécurité réseau couvre les éléments suivants :

- Sécurité de l'infrastructure : couvre la sécurité logique et physique des équipements et des connexions réseau, aussi bien internes que celles fournies par des fournisseurs réseau.
- Sécurité des accès : couvre la sécurité logique des accès locaux et distants aux ressources de l'entreprise, ainsi que la gestion des utilisateurs et de leurs droits d'accès au système d'informations de l'entreprise.
- Sécurité du réseau intranet face à Internet ou aux autres parties : couvre la sécurité logique des accès aux ressources de l'entreprise (Intranet) et l'accès aux ressources extérieures (Extranet) [10].

1.4.2 Champ d'application de la politique :

La présente politique s'applique sans exception au personnel, toutes les directions et à tous les tiers utilisant les installations technologiques du réseau l'EPB. La politique énonce les principes qui permettent aux utilisateurs d'obtenir les accès requis pour leur permettre d'effectuer leurs travaux [11].

1.4.3 Préparation de la politique de sécurité

La politique de sécurité informatique ne s'improvise pas à la dernière minute dans la précipitation qui suit une cyberattaque, par exemple. Elle doit être conçue sereinement en évaluant les menaces courantes et leurs conséquences prévisibles ainsi que les vulnérabilités actuelles de l'entreprise.

Le document doit contenir tous les éléments utiles à la sécurisation des données et les mesures à mettre en place pour poursuivre les activités de l'entreprise sans interruption… Ou tout au moins les reprendre le plus rapidement possible et dans les meilleures conditions.

Afin de bénéficier d'un dispositif de protection efficace, le plan d'actions ne peut se limiter à un simple mode d'emploi pour choisir des mots de passe ou sauvegarder des documents. Il doit au contraire aborder de manière globale l'ensemble des thématiques relatives à la sécurité : réseaux, applications, données, terminaux mobiles, cloud, moyens d'accès, infrastructures, etc.. [9].

1.4.4 Les objectifs d'une politique de sécurité

La définition d'une politique de sécurité n'est pas un exercice de style mais une démarche de toute l'entreprise visant à protéger son personnel et ses biens d'éventuels incidents de sécurité dommageables pour son activité.

La définition d'une politique de sécurité réseau fait intégralement partie de la démarche sécuritaire de l'entreprise. Elle s'étend à de nombreux domaines, dont les suivants :

1. audit des éléments physiques, techniques et logiques constituant le système d'information de l'entreprise;
2. sensibilisation des responsables de l'entreprise et du personnel aux incidents de sécurité et aux risques associés;

3. formation du personnel utilisant les moyens informatiques du système d'information;
4. structuration et protection des locaux abritant les systèmes informatiques et les équipements de télécommunications, incluant le réseau et les matériels ;
5. ingénierie et maîtrise d'œuvre des projets incluant les contraintes de sécurité dès la phase de conception ;
6. gestion du système d'information de l'entreprise lui permettant de suivre et d'appliquer les recommandations des procédures opérationnelles en matière de sécurité;
7. définition du cadre juridique et réglementaire de l'entreprise face à la politique de sécurité et aux actes de malveillance, 80 pour 100 des actes malveillants provenant de l'intérieur de l'entreprise ;
8. classification des informations de l'entreprise selon différents niveaux de confidentialité et de criticité.

Avant de définir une politique de sécurité réseau, il faut en connaître les objectifs ou finalités [11].

1.4.5 Principe générique d'une politique de sécurité réseau

Quelle que soit la nature des biens produit par l'entreprise, sa politique de sécurité réseau vise à satisfaire les critères suivants :

- **Identification :** information permettant d'indiquer qui vous prétendez être.
- **Authentification** : information permettant de valider l'identité pour vérifier que vous êtes celui que vous prétendez être.
- **Autorisation** : information permettant de déterminer quelles sont les ressources de l'entreprise auxquelles l'utilisateur identifié aura accès ainsi que les actions autorisées sur ces ressources.
- **Confidentialité** : ensemble des mécanismes permettant qu'une communication de données reste privée entre un émetteur et un destinataire.
- **Intégrité :** ensemble des mécanismes garantissant qu'une information n'a pas été modifiée.
- **Disponibilité** : ensemble des mécanismes garantissant que les ressources de l'entreprise sont accessibles.
- **Non-répudiation** : mécanisme permettant de trouver qu'un message a bien été envoyé par un émetteur et reçu par un destinataire.

- **Traçabilité :** ensemble des mécanismes permettant de retrouver les opérations réalisées sur les ressources de l'entreprise.
- **Continuité :** a pour but de garantir la survie de l'entreprise après un sinistre important touchant le système informatique. Il s'agit de redémarrer l'activité le plus rapidement possible avec le minimum de perte de données [11].

1.5 Stratégie de sécurité réseau

1.5.1 Méthodologie pour élaborer une stratégie de sécurité réseau

Il existe plusieurs méthodes permettant d'élaborer des stratégies de sécurité, nous pouvons citer :

- Prédiction des attaques potentielles et analyse de risque.
- Analyse des résultats et amélioration des stratégies de sécurité.

1.5.2 Proposition de stratégies de sécurité réseau

Les parties qui suivent détaillent un ensemble de stratégies de sécurité focalisées sur des domaines spécifiques, ces stratégies doivent être considérées comme des briques de bases pour avoir une bonne politique de sécurité [12] :

- **Authentification**

  L'authentification selon le contexte utilise des informations contextuelles pour vérifier si l'identité d'un utilisateur est authentique ou non. Grâce aux profils de risque, les entreprises ont les moyens de restreindre l'accès à des systèmes spécifiques ou à des éléments de contenu selon les critères d'un utilisateur.

- **Cryptographie (chiffrement et signature)**

  Le chiffrement des données fut inventé pour assurer la confidentialité des données. Il est assuré par un système de clé (algorithme) appliqué sur le message. Ce dernier est décryptable par une clé unique correspondant au cryptage. Dans toute transaction professionnelle, La signature numérique est un moyen d'identification de l'émetteur du message.

- **Contrôles d'accès aux ressources**

  Méthode pour restreindre l'accès à des ressources. On n'autorise que certaines entités privilèges.

- **Firewalls**

  Afin d'éviter que des attaques puissent venir d'Internet par le routeur, il convient d'isoler le réseau interne de l'entreprise. La méthode la plus connue est le firewall et le serveur proxy ; Le firewall, placé à l'entrée du réseau, constitue ainsi un unique point d'accès par où chacun est obligé de passer. Le serveur Proxy, lui, permet de faire le relais au niveau des applications pour rendre les machines internes invisibles à l'extérieur.

- **Audit**

  L'audit de sécurité permet d'enregistrer tout ou partie des actions effectuées sur le système. L'analyse de ses informations permet de détecter d'éventuelles intrusions. Les systèmes d'exploitation disposent généralement de systèmes d'audit intégrés, certaines applications aussi. Les différents évènements du système sont enregistrés dans un journal d'audit qui devra être analysé fréquemment, voire en permanence. Sur les réseaux, il est indispensable de disposer d'une base de temps commune pour estampiller les évènements.

- **Logiciels anti-virus**

  Deux tiers des attaques se font par virus : chaque poste doit disposer d'un logiciel anti-virus mis à jour régulièrement ! Les virus se transmettent principalement par flash disk (clé USB), mais peuvent aussi se faire par mail. Les fichiers les plus susceptibles d'en contenir sont bien sûr les exécutables (.com, .exe).

- **Programmes de tests de vulnérabilité et d'erreurs de configuration**

  Utiliser des logiciels permettant de façon automatique de chercher les erreurs de configuration ou les vulnérabilités du système tel que Cops et Satan.

- **Détection d'intrusion**

  Utiliser un logiciel de détection des comportements anormaux d'un utilisateur ou des attaques connues. Ce logiciel émet une alarme lorsqu'il détecte que quelqu'un de non-autorisé est entré sur le réseau.

- **Les réseaux privés virtuels (VPN : Virtual Private Network)**

  Permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Avec le développement d'Internet, il est intéressant de permettre un transfert de données sécurisé et fiable. Grâce à un principe de tunnel (tunnelling) dont chaque extrémité est identifiée, les données transitent après avoir été chiffrées.

- **Les DMZ (zone démilitarisé)**

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur Web, serveur de messagerie, serveur FTP public,...etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau a part, accessible aussi bien du réseau interne que de l'extérieur sans pour autant risquer de compromettre la sécurité de l'entreprise. On parle ainsi de zone démilitarisé (noté DMZ pour Demilitarized zone) pour designer cette zone isolée hébergeant des applications mises à disposition du public [13].

1.6 Les Certificats

Ce sont des structures de données qui sont numériquement signés par une autorité de certification (CA: Certification autorité) en qui les utilisateurs peuvent faire confiance. Il contient une série de valeurs, comme le nom du certificat et son utilisation, des informations identifiant le propriétaire et la clé publique ainsi que la clé publique elle-même, la date d'expiration et le nom de l'organisme de certificat. La CA utilise sa clé privée pour signer le certificat. Si le récepteur connait la clé publique du CA, il peut vérifier que le certificat provient vraiment de l'autorité concernée et est assuré que le certificat contient une clé publique valide [18].

- **Définition de l'autorité de certification :** une autorité de certification qui est une autorité de confiance reconnue par une communauté d'utilisateurs. Elle délivre et gère les certificats (clefs publiques + identités signées), maintient une liste des certificats révoqués [18].

1.7 Conclusion

Ce chapitre, a mis en avant les premiers concepts des réseaux informatiques, ainsi qu'une analyse des besoins de sécurité et les étapes primordiales qui précèdent la mise en place des stratégies de sécurité dans un réseau d'entreprise.

Le chapitre suivant sera consacré à l'étude de l'existant de l'infrastructure réseau de l'entreprise portuaire de Bejaia afin d'en soulever les problématiques de cette dernier, ainsi définir nos objectifs pour apporter les solutions nécessaires.

CHAPITRE 2

PRESENTATION DE L'ORGANISME D'ACCUEIL ET ETUDES DE L'EXISTANT

Introduction

Ce chapitre sera consacré à l'étude du réseau existant dans l'EPB ainsi qu'aux améliorations proposées pour cette dernière, en premier lieu donner un aperçu sur l'ensemble de l'entreprise en terme de structure et ses objectifs , puis faire le point sur le réseau et ses composants afin de proposer d'éventuelles améliorations.

2.1 Présentation générale de l'organisme d'accueil

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 2ème port d'Algérie en marchandises générales et 3ème port pétrolier. Il est également le 1er port du bassin méditerranéen certifié par ISO 9001 pour l'ensemble de ses prestations et pour avoir ainsi installé un système de management d'une grande qualité. Cela est très important pour le processus d'amélioration des prestations, pour le bénéfice de ses clients. L'Entreprise Portuaire a connu d'autres succès depuis, elle est notamment certifiée à la Norme ISO 14001 et au référentiel BS OHSAS 18001, respectivement pour l'environnement et l'hygiène et sécurité au travail [14].

2.1.1 Missions et activités de l'entreprise

- **Missions :**

La gestion, l'exploitation et le développement du domaine portuaire sont les charges essentiels de l'entreprise dans le but de promouvoir les échangés extérieurs du pays les missions de l'EPB [14]:

- Le traitement dans les meilleures conditions de délais, le coup de la sécurité l'ensemble des passages, des marchandises et des navires
- La gestion et l'exploitation des infrastructures et des super structures portuaire
- La manutention et l'aconage de marchandise en transite par le port de Bejaia

- Le transite des passagers et leur véhicule par la gare maritimes du port Bejaia
- La mise à disposition d'infrastructures nécessaire aux activités relatives aux hydrocarbures (exportation pétrole et du cabotage nationale des produits raffinés et gaz du pétrole liquéfie).
- Pilotage, et remorquage et le lamanage des navires dans les limites de la zone de pilotage dans le port de Bejaia.

- **Activités :**

Les principales activités 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.
- La police et la sécurité portuaire dans la limite géographique du domaine public portuaire.

S'avèrent indispensable de renforcer les mesures de la sécurité dans le but de maintenir la confidentialité intégrité et le contrôle d'accès aux réseaux pour réduire les risque d'attaque [14].

2.1.2 L'organisation de la structure générale de l'EPB

L'EPB est organisée selon des directions fonctionnelles et opérationnelles dirigées par une direction générale qui est chargée de concevoir, coordonner et contrôler les actions liées a la gestion et au développement de l'entreprise (figure2.1)

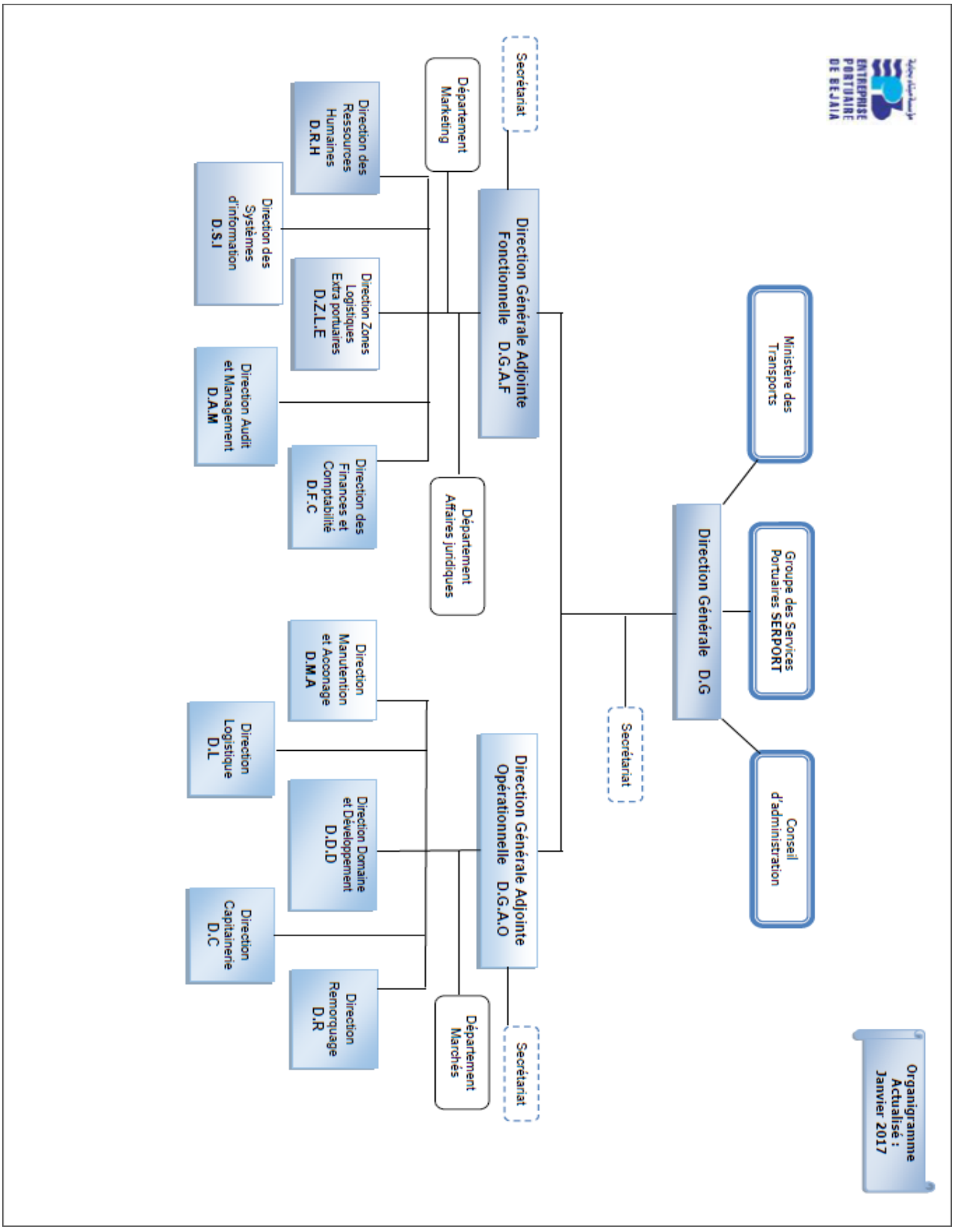

Figure 2. 1 : « *Organigramme de l'EPB [14]*»

2.2 Présentation de la DSI

La structure informatique de l'EPB est un département rattaché à la direction générale adjointe fonctionnel ; 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.

2.2.1 Organisation humain de la DSI

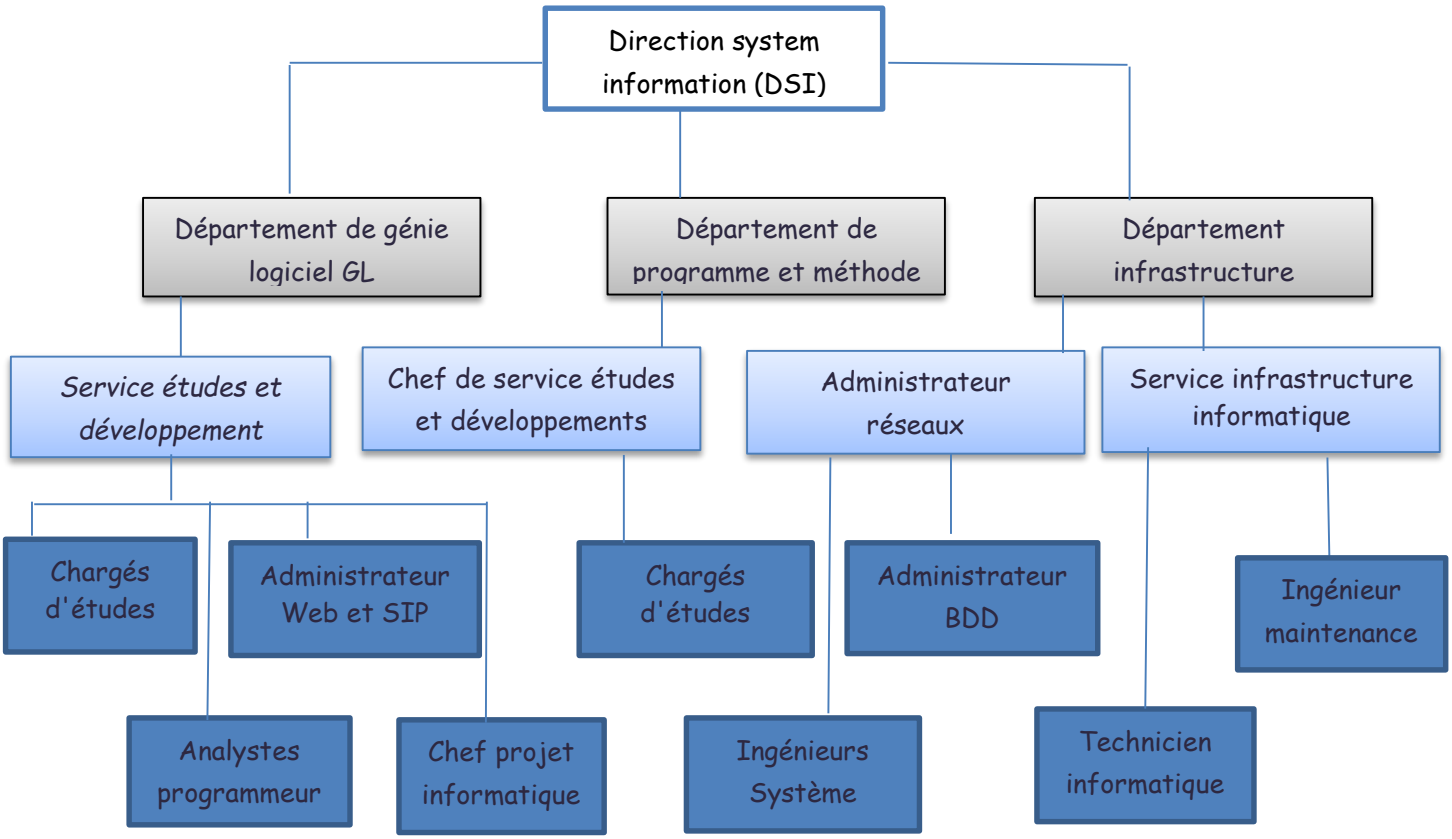

Figure 2. 2 : « représente l'organisation humaine du DSI [14] »

2.2.2 Les missions de la DSI

L'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.

2.3 Infrastructure informatique

Le réseau du port de Bejaia s'étend du port pétrolier (n°16) aux ports 13 et 16 (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 (voir figure 2.4). Chaque site a une armoire de brassage contenant un/des convertisseur(s) media, un/plusieurs Switch où sont reliés les différents équipements par des câbles informatiques [14].

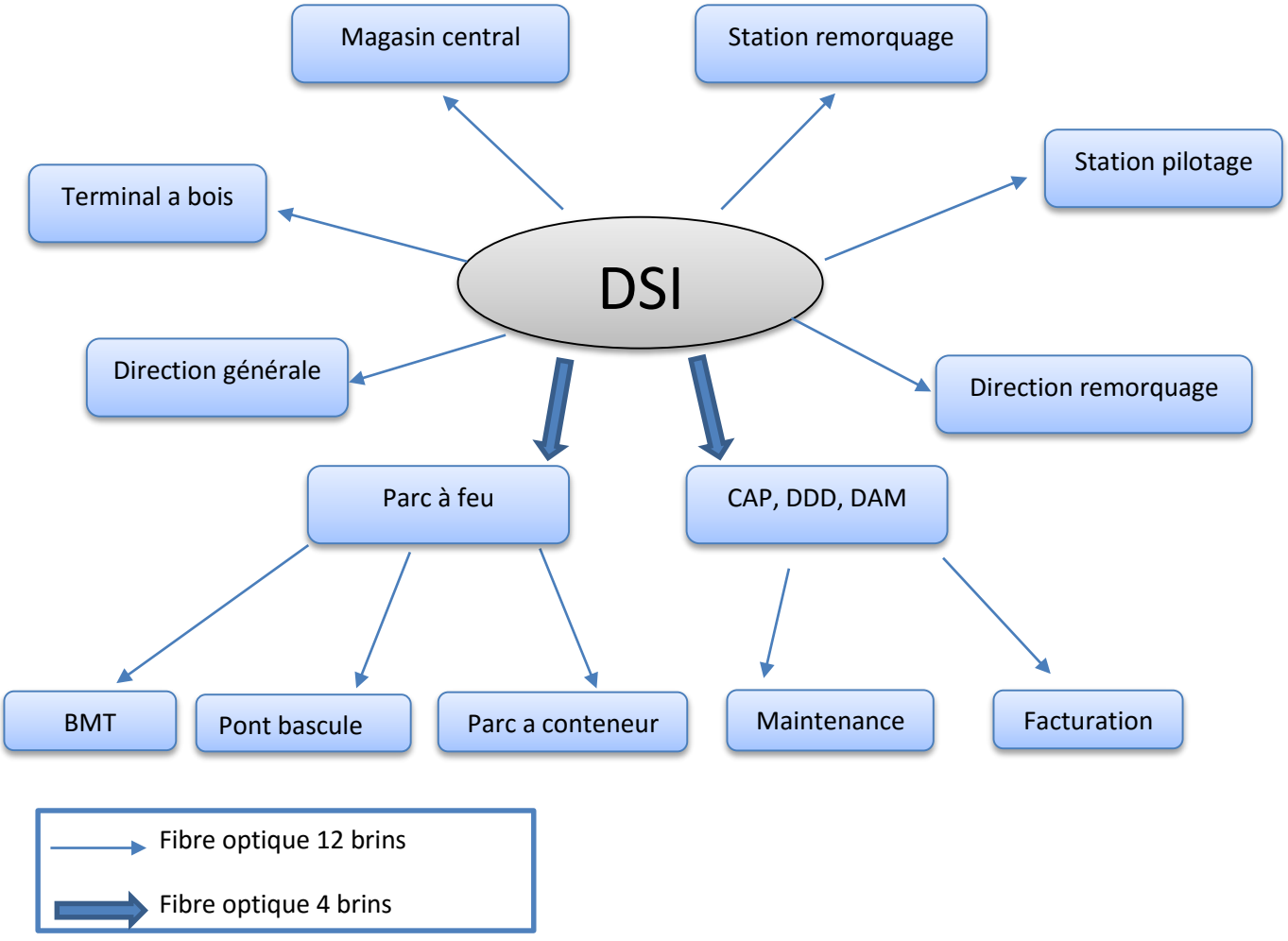

Figure 2. 3 : « réseau fibre optique de l'EPB [14]»

2.3.1 Présentation de l'architecture de l'EPB

Dans cette partie nous allons présenter les différents composants de l'architecture de l'EPB (figure2.4)

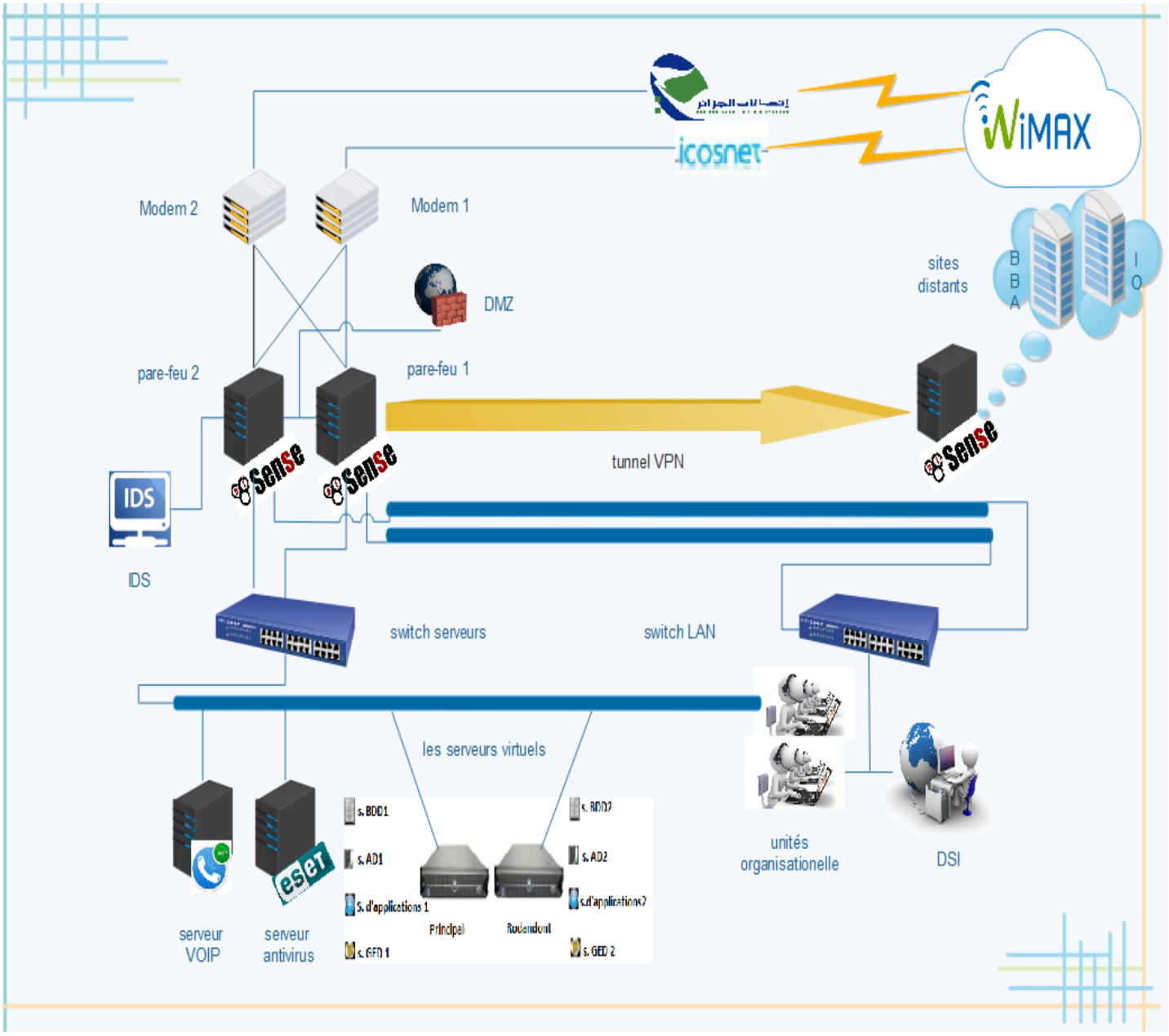

Figure 2. 4 : « architecture de l'EPB »

2.3.2 Etude de l'architecture

- **Connexion internet :**

  L'entreprise portuaire de Bejaia s'est dotée de deux connexions Wimax à savoir icosnet et Algérie télécom. Ce type de connexions permet de se connecter à

Internet haut débit grâce à une antenne outdoor qui communique par des ondes hertzienne via une station de base située au mont Gouraya, d'une très grande fiabilité permettant ainsi d'éviter l'usage du câble et le risque d'une panne physique par conséquent.

- **Sécurité :**

Un point essentielle dans une entreprise d'une telle envergure, en effet elle se doit d'assurer la protection externe et interne du système d'information. Mais aussi garantir en tout temps la confidentialité des communications, et pour cela l'EPB s'est muni de différents outils dont on retrouve :

- **Pfsense (pare-feu) :** La sécurité est assurée par deux serveurs virtuel pare-feu qui agissent comme un filtre afin de définir les règles d'accès à un réseau comme Internet à cause des risques que peut représenter une connexion normal dans certain cas.
- **DMZ :** une zone démilitariser terme réseau qui consiste un « tampon » de tel sorte que l'échange entre le réseau interne et le réseau externe transite par ce tompon dont l'objectif principale et que tous les échanges passe par cette zone qui offre différents services de sécurité tels le filtrage réseaux entre les différents réseaux ainsi interconnecter mais aussi des serveurs relais dans la dmz pour gérer tout le trafic interne et externe, on retrouve aussi des antivirus ou analyseurs de contenus pour journalier les échanges et décontaminer les données entrantes ou sortante conformément à une politique de sécurité. Ajouter a cela qu'elle assure aussi des services publics et des serveurs relais permettant de masquer les services de topologie du réseau interne, comme elle rentre aussi dans la sécurisation du serveur web.
- **System de detection d'intrusion IDS (intrusion Detection System) : (snort):** tout comme son nom l'indique, un système de détection permet de détecter différentes tentatives d'intrusion et ce en se basant sur une base de signatures des attaques connues.
- **VPN (Virtual Private Network):** pour répondre aux besoins d'interconnexion de l'Entre- prise Portuaire de Bejaia aux différents sites distants (bordj bou aririje et Ighil ouberouak tala hamza).
- **Eset smart Remote** : est un outil de gestion de protection contre les programmes malveillants dans une entreprise. Quelle que soit la taille de

l'organisation, il permet de surveiller et de contrôler chaque aspect de l'infrastructure de sécurité. Eset smart remote augmente le niveau de protection et réduit le coût total de propriété des produits de eset Lab. C'est la démarche de haute valeur adoptée par ESET.

- **Salle machine :** La salle machine est le cœur du réseau toutes les activités du port reposent sur cette salle, elle regroupe en un seul endroit les ressources nécessaires au bon fonctionnement du LAN, en plus des switchs elle comporte les différentes équipements :

- **Onduleur** : trois onduleurs qui jouent un rôle important dans la sécurité des systèmes en cas de coupures de courant, l'administrateur aura le temps de sauvegarder le travail en cours.
- **armoire optique** : une armoire de fibre optique qui relie les douze câbles de fibre optique sortant elle contient des convertisseurs optique, analogique des jarretières optiques et des cordons.
- **armoire de brassage** : une armoire qui contient tous les serveurs tel que :
- **Plateforme utilisé Windows serveur 2008r2 2012 r2 :**

- **Serveur de contrôleur de domaine DC1** (Active Directory) : sous Windows Server 2012 r2 l'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateur utilisant le système Windows. Il répertorie les éléments de ce réseau administré tel que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes...etc.
- **Serveur de contrôleur de domaine redondant DC2** (Active Directory) : il permet de conserver des réplicas de données de l'annuaire sur un autre contrôleur de domaine, cela garantie la disponibilité et la continuité.
- **Serveur DHCP :** pour un adressage dynamique (des adresses de classe B), dans le but d'avoir une configuration sure et fiable des paramètres de connexion et d'assurer la réduction de gestion de configuration.
- **serveur DNS (domaine Name System).**
- **Serveur de base de données** (SQL server 2008 and My SQL) : un serveur de base de données répond à des demandes de manipulation de données stockées dans

une ou plusieurs base de données. Il s'agit de demande de recherche, de tri, d'ajout, de modification ou de suppression de données. Ces données sont utilisées par des serveurs web et des utilisateurs.

- **Serveur application/fichier** : c'est un serveur sur lequel sont installées les applications utilisées par les utilisateurs. ces applications sont chargées sur le serveur d'application pour y accéder à distance. Un serveur d'application peut être un serveur qui centralise toutes les applications utilisées par les postes clients.
- **Serveur de sauvegarde** : il a pour rôle de sauvegarder en continue les données générées par l'entreprise. Si un employé efface par erreur un document, ou qu'il y a un dysfonctionnement d'un ordinateur, le serveur est en mesure de récupérer le fichier perdu.
- **Serveur GED :** Le terme GED désigne les logiciels permettant la gestion de contenus documentaires, qui est un point important pour l'entreprise **EBP** permettant l'organisation ainsi que la gestion des informations et des documents électroniques au sein de cette dernière. En effet c'est un logiciel de Gestion Électronique de Documents (GED) fonctionnant sur un serveur en mode Intranet, Extranet, il est simple à installer et à utiliser. Les utilisateurs accèdent à la GED avec un navigateur web (Internet Explorer, Firefox, Safari, Chrome...). Il n'y a aucune installation sur les postes des utilisateurs.
- **Serveur VoIP :** Un système téléphonique VoIP/IPBX (Voice over IP) (Internet Protocol Branch eXchange) est constitué d'un ou de plusieurs téléphones SIP/VoIP, d'un serveur IPBX et facultativement d'une passerelle VoIP. Le serveur IPBX est similaire à un serveur proxy : les utilisateurs SIP, étant soit des softphones ou des téléphones matériels, enregistrés auprès d'un serveur IPBX de l'EPB, et quand ils veulent passer un appel, ils demandent à l'IPBX d'établir la connexion. L'IPBX possède un registre de tous les téléphones/usagers et de leur adresse SIP respectives et il peut ainsi connecter un appel interne ou router un appel externe soit par le biais d'une passerelle VoIP ou d'un opérateur de service VoIP mais dans le cas du serveur de l'epb est pour l'usage interne
- **Serveur web**

- **Serveurs en redondance :** un serveur redondant pour chaque serveur pour assurer les tolérances aux pannes ainsi que pour augmenter la capacité totale de ce fait les performances du système.
- **Technologie de stockage avec les RAID :** (Redundant Array of Independent Disk) pour une meilleure gestion de stockage et une garantie de disponibilité des données l'entreprise EPB s'est dotée de la technologie RAID et plus précisément le RAID de niveau 5.

- **Et on trouve dans chaque direction une armoire de brassages contenant :**
  - Switch cisco 24 ports 2950
  - Switch micro net 16ports
  - Convertisseurs media

2.4 Diagnostique de l'architecture de l'EPB

L'étude que nous avons menée sur l'architecture nous a permis de retirer des faiblesses réseaux et qui sont les suivantes.

❖ **Un seul domaine de diffusion**

- Un seul et unique domaine de diffusion ce qui implique une surcharge du réseau de l'entreprise, les machines communiquent sans cesse entre elles, le trafic réseaux devient congestionné, ce qui ralenti nettement la communication sur le réseau et engendre une lourdeur mêmes sur les applications et machines clients.

❖ **Architecture plate**

- Besoin de segmentation du réseau en plusieurs VLANs.
- Changements et Configuration des Switch au niveau des armoires pour mettre à niveau le réseau VLAN de l'entreprise.

❖ **Messagerie non opérationnelle**

- L'EPB dispose d'une messagerie externe qui dépond entièrement d'Internet. Dans le cas de coupure de connexion Internet les utilisateurs ne pourront plus s'envoyer des e-mails.
- L'entreprise ne dispose pas de serveur de messagerie interne.
- Relais de messagerie ouvert, cependant il peut être utilisé pour envoyer ou recevoir des e-mails commerciaux non sollicités ou des Spams, également appelé courriers indésirables.

2.5 Problématique

Aujourd'hui, la plupart des organisations et entreprises dépendent considérablement de leurs réseaux locaux pour leurs processus métiers critiques. En d'autres termes, leur efficacité opérationnelle et l'amélioration continuelle de leur productivité et réactivité reposent en grande partie sur la qualité de leurs infrastructures réseaux. Ceci a causé une véritable émergence de systèmes sophistiqués dédiés à la gestion de réseau, et grâce auxquels on gère très facilement des réseaux de plusieurs dizaines voire centaines d'équipements.

Apres avoir étudié le réseau de l'EPB en prenant en considération les exigences auxquelles doit répondre un réseau performant, stable, et sécurisé. Ce dernier répond à la plupart de celles-ci cependant reste à améliorer les faiblesses et les manques d'infrastructure qu'on a pu soulever.

L'entreprise Portuaire de Bejaïa (EPB) possède une architecture réseau plate où tout le monde se trouvent dans le même domaine de diffusion car la plage d'adresse IP bien qu'adaptée au début du temps où le nombre des machines n'était pas considérable, de nos jours ce nombre s'accroit de plus en plus.

La messagerie électronique de l'EPB dépend entièrement d'internet (externe) dans le cas de coupure de cette dernière les utilisateurs ne peuvent plus s'envoyer des e-mails l'utilisation d'un serveur de messagerie externe on risque de compromettre la confidentialité des e-mails échangé entre les utilisateurs les limites de cette architecture commencent désormais à se faire sentir.

En termes de Performance, cette architecture est loin d'être Optimale à cause du nombre très important broadcast transmis, des plateformes sont devenues obsolète avec l'arrivée de nouvelles technologies, par conséquent de nouvelles méthodes d'approche on était déployer par la DSI active directory sous Windows server 2012 r2 et pour la gestion des domaine mais la segmentation reste un point prioritaire à présent, Pour pallier à ces problèmes de nouvelle stratégies et outils sont nécessaires à mettre en œuvre pour une meilleure gestion de la plage d'adresse mettre en place une solution d'optimisation de la bande passante du réseau par la segmentation des domaines de broadcast du réseaux de l'EPB , La solution VLAN reste toutefois la première étape du processus d'amélioration des performances du réseau contre les surcharges rencontrées par les utilisateurs du réseaux de l'entreprise .

Tous ces phénomènes entrainent la dégradation du réseau. La segmentation et la configuration d'un serveur de messagerie devient alors nécessaire afin d'améliorer la réactivité, et augmenter les performances globales du réseau et sa sécurité.

Comment donc assurer la disponibilité en permanence d'un serveur de messagerie électronique sûr ? Comment procédé à la mise de la solution Vlan au sein du réseau l'entreprise EPB ?

2.6 Objectifs de l'étude

L'identification de nos objectifs, constitue un moyen d'évaluation des résultats de notre étude. Ces objectifs se résument à deux niveaux que sont : L'objectif général et les objectifs spécifiques.

2.6.1 - Objectif principal

Le but recherché est de montrer la nécessité de ces deux solutions qui actuellement jouent un rôle très important au sein du réseau de l'entreprise EPB, et qui sont définies comme suit :

En premier lieu, mettre en place des VLANs a tout de suite semblé une éventuelle solution qui assurerait :

- la segmentation et assouplissement de l'organisation.

- la mise en œuvre des stratégies d'accès et de sécurité en fonction de groupes d'utilisateurs précis

En deuxième lieu, tout aussi importante serait de la mise en place d'une messagerie répondant aux exigences de l'entreprise, à savoir :

- Permettre au personnel de naviguer et communiquer.

- Lui permettre aussi d'utiliser plus efficacement l'outil informatique.

2.6.2 -Objectifs spécifiques

Ce projet s'inscrit dans une politique globale de modernisation des télécommunications et de l'informatique, tout comme aussi de la sécurité et optimisation du réseau.

Pour les VLANs :

Cette organisation devra d'abord permettre aux utilisateurs de bénéficier de façon plus qualitative mais aussi quantitative des potentialités réseau offertes par les équipements (bande passante, rapidité de traitement) ou de pouvoir appartenir à des groupes de travail indépendamment de l'endroit où se situent les systèmes.

Ensuite elle devra permettre de contrôler et de sécuriser les échanges à l'intérieur d'un domaine et entre les domaines de réseaux virtuels locaux, ce qui est une solution au problème de la confidentialité des données.

Enfin La réalisation de VLANs devra permettre une certaine centralisation, d'où un meilleur contrôle du réseau et des procédures de reconfiguration plus facile pour les administrateurs.

Afin de parvenir à la réalisation effective de ce projet nous devons passer par plusieurs étapes:

- Premièrement nous procéderons à une étude suivie d'une analyse de l'existant afin de prendre connaissance des plans déjà réalisés, des équipements disponibles et de leurs potentialités.
- -deuxièmement, nous examinerons des propositions de solutions, puis nous en retiendrons une.
- -Troisièmement nous passerons à la simulation de configuration des équipements.

Pour la messagerie :

Il doit permettre la mise en place d'un système de transmission des données (fichiers testes, images..) fiable, sécurisé, à moindre coût, rapide et accessible à tous les Bureaux en temps réel.

Nous décrivons ce que l'interface doit offrir comme fonctions sans pour autant spécifier les détails de leurs fonctionnements :

Il consiste à concevoir et à réaliser un système d'envoi de messages. Précisément notre tâche peut être résumée comme suit :

- Présenter le serveur de la messagerie et décrire les différents protocoles.
- Description et fonctionnement de l'architecture de la messagerie électronique.
- Mettre en œuvre et élaborer le projet de la messagerie décrit.

2.7 Architecture proposée pour le réseau de l'EPB

Nous pouvons regrouper les améliorations proposées dans l'architecture suivante

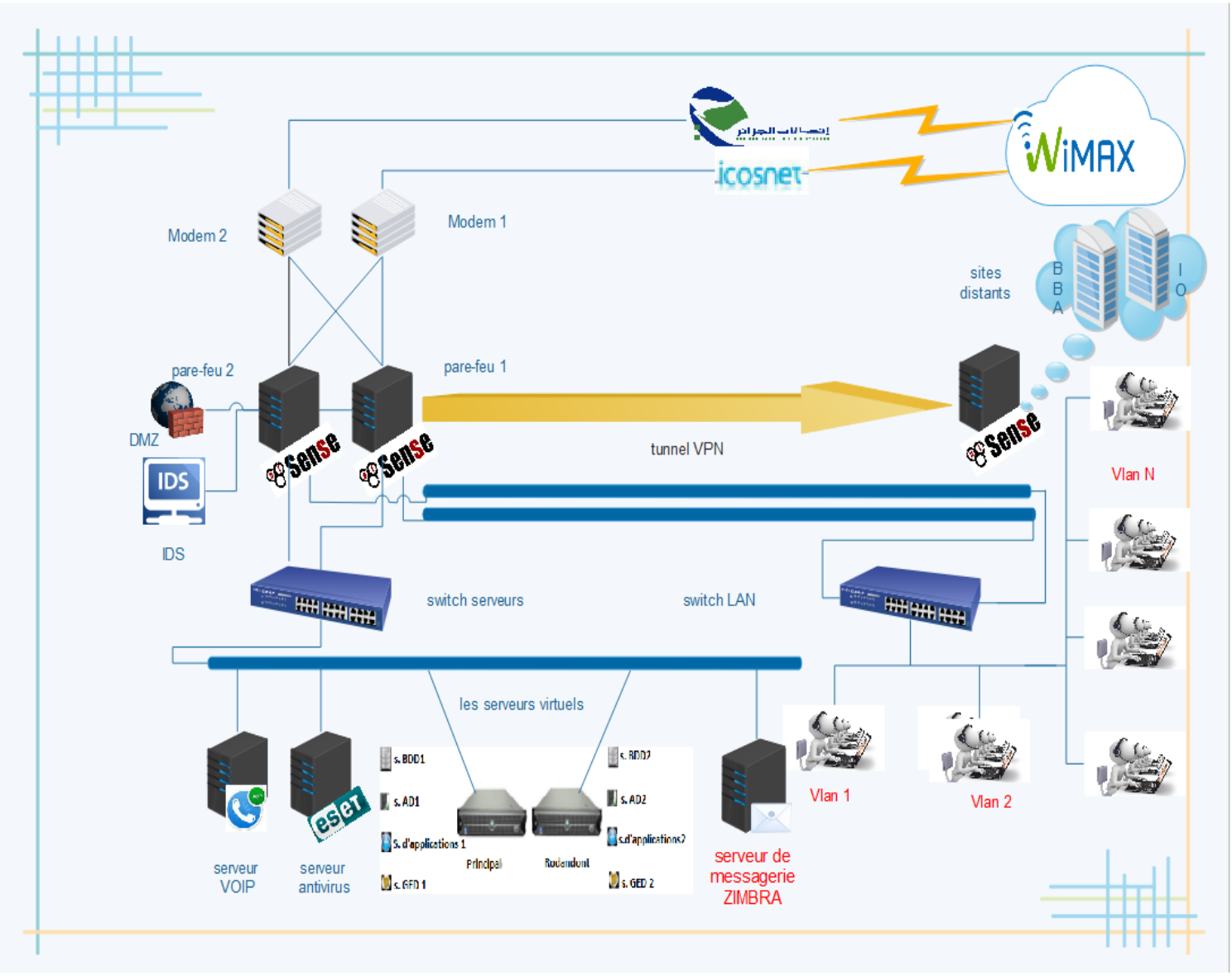

Figure 2. 5 : « *Architecture proposé pour les réseaux l'EPB* »

2.8 Conclusion

A l'issue de ce chapitre, l'étude de l'existant nous a permis de se familiariser avec le réseau actuel de l'Entreprise Portuaire de Bejaïa, de ce fait en retirer certaines lacunes et faiblesses du réseau de cette dernière, dans le chapitre qui suit nous allons proposer certaines solutions, suite à ça définir nos objectifs en adoptant un plan de travail afin de les mettre en œuvres. Pour remédier à ces problèmes.

CHAPITRE 3

ETUDES DES SOLUTIONS PROPOSEES

Introduction

Après avoir soulevé les différents problèmes et lacunes liées à l'organisation de l'architecture réseau de l'EPB, ce chapitre sera exclusivement consacré aux solutions proposées pour pallier à ces problèmes ainsi que les matériels et équipements utilisés pour les réaliser.

3.1 Solution VLAN

3.1.1 Définition des réseaux virtuels

Un réseau local virtuel (VLAN) est un réseau local (LAN) distribué sur des équipements de niveau 2 du modèle OSI .C'est l'une des technologies permettant d'améliorer et de diviser de vastes domaines de diffusion en domaines plus petits [15].

3.1.2 L'intérêt d'avoir des VLANs

Il existe plusieurs intérêts à avoir des VLAN dans un réseau, voici quelques exemples de besoins qui nécessitent l'utilisation des réseaux virtuels :

- ✓ **La sécurité :** Les groupes contenant des données sensibles sont séparés du reste du réseau, ce qui diminue les risques de violation de confidentialités.
- ✓ **Réduction des couts :** Des économies sont réalisées grâce à l'utilisation plus efficace de la bande passante et des liaisons ascendantes existantes.
- ✓ **Meilleures performances :** Le fait de diviser des réseaux linéaires de couche 2 en plusieurs groupes de travail logiques (domaines de diffusion) réduit la quantité de trafic inutile sur le réseau et augmente les performances.
- ✓ **Atténuation des tempêtes de diffusion :** Le fait de diviser un réseau en plusieurs réseaux VLAN réduit le nombre de périphériques susceptibles de participer à une tempête de diffusion.

- ✓ **Efficacité accrue du personnel informatique** : Les VLAN facilitent la gestion du réseau, car les utilisateurs ayant des besoins réseaux similaires partagent le même VLAN.
- ✓ **Gestion simplifiée de projets ou d'applications** : La séparation des fonctions facilitent ka gestion d'un projet ou l'utilisation d'une application.

3.1.3 Les différents types de VLANs

Il existe plusieurs types de VLAN définis selon le critère de commutation et le niveau auquel il s'effectue :

❖ **VLAN de niveau 1 par port**

Chaque port du commutateur est affecté à un VLAN donné. L'affectation des ports est statique, donc l'administrateur peut connaitre directement le VLAN d'appartenance d'un équipement. Cette technique est efficace dans les réseaux où les déplacements sont rares et contrôlés. En effet, une source externe ne peut y accéder au réseau, sauf si elle se branche sur le port appartenant au VLAN voulu à accéder, donc, un renforcement de la sécurité. Par contre, son inconvénient est sa lourdeur d'administration. En effet, si un matériel est déplacé et que l'on désire qu'il soit toujours dans le même VLAN, il faudra alors configurer le nouveau port [34]. (Voire la figure 3.1)

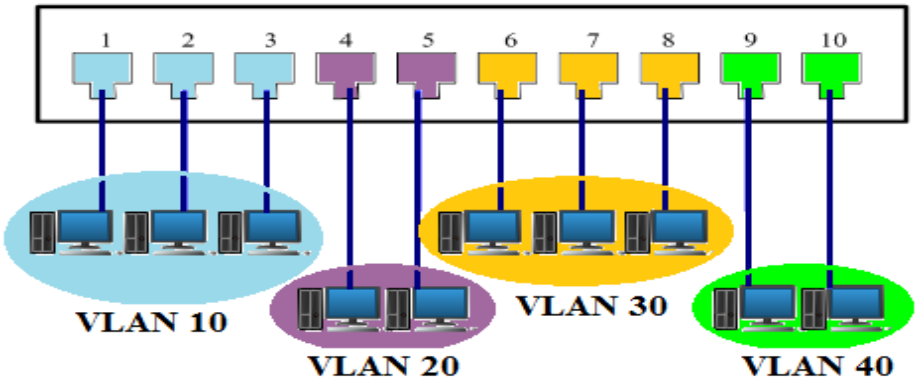

Figure 3. 1 : « VLAN par port [34]»

❖ **VLAN de niveau par adresse MAC**

Consiste à définir un réseau virtuel en fonction des adresses MAC des stations. L'intérêt principal de ce type de VLAN est l'indépendance vis-à-vis de la localisation géographique. Si une station est déplacée sur le réseau physique, son adresse physique ne changeant pas, elle continue

d'appartenir au même VLAN (ce fonctionnement est bien adapté à l'utilisation de machines portables) [34].

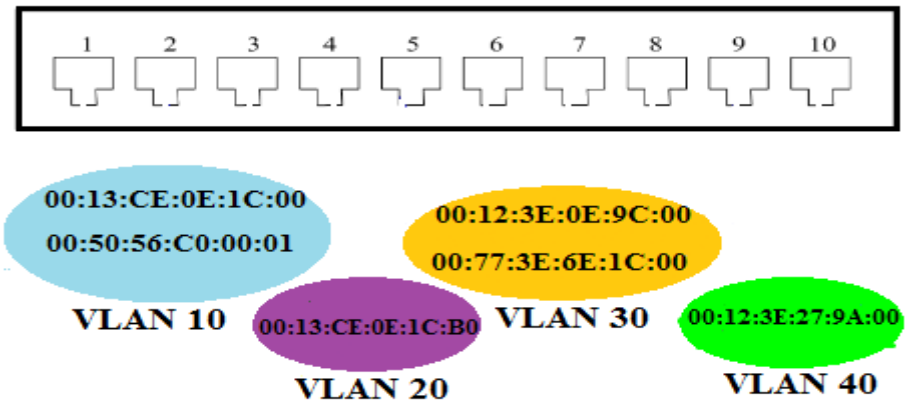

Figure 3. 2 : « VLAN par adresse MAC [34]»

❖ **VLAN de niveau 3**

On distingue 2 types de VLAN de niveau 3:

1. **Le VLAN par sous-réseau :** Associe des sous-réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de déplacements d'une station. En contrepartie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.

2. **Le VLAN par protocole :** Permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un réseau [34].

3.2 Les protocoles de transport des VLANs

Afin d'assurer les transports des VLANs certains protocoles ont été mis en place :

3.2.1 La norme 802.1q

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

Le principe consiste à ajouter dans l'en-tête de la trame Ethernet un marqueur qui va identifier le VLAN. Il existe quelques solutions propriétaires pour réaliser ceci, mais le système s 'est avéré tellement intéressant qu'une norme a été définie, il s'agit de la norme802.Iq. [16].

❖ **Description de la norme**

Le tableau suivant illustre la modification de la trame Ethernet et de l'ajout d'un champ sur 4 octets par la norme 802.1Q :

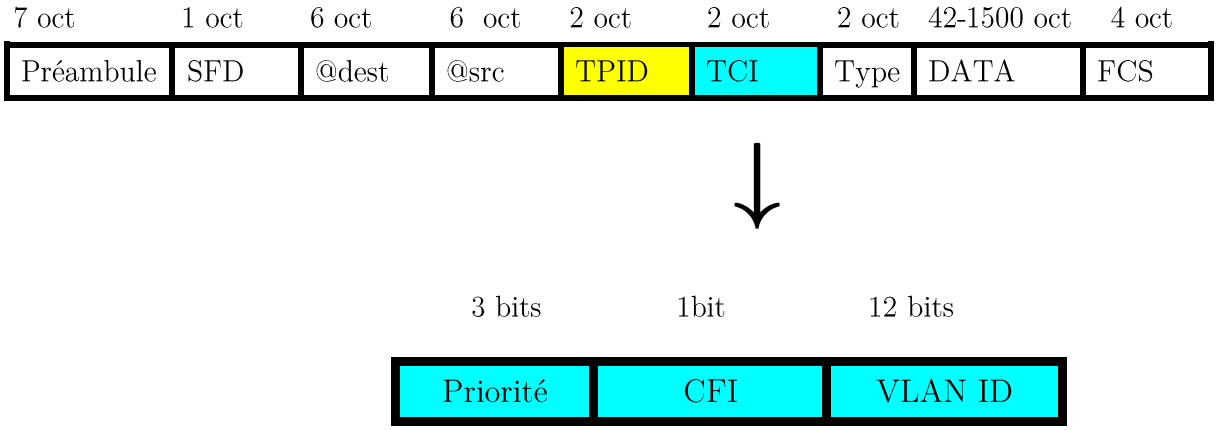

Tableau 3. 1 : « Extension de la trame Ethernet modifiée par la norme 802.1Q [15]»

2) Tag Protocol Identifier (TPID)

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

3) Tag Control Information (TCI)

Cette partie se compose de trois champs :

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

b) Canonical Format Identifier (CFI) Ce champ d'un bit assure la compatibilité entre adresse MAC Ethernet et Token Ring. Un commutateur Ethernet fixe cette valeur à 0[16].

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

2 octets	2 octets TCI		
TPID 16 bits	USER Priority 5 bits	CFI 1 bit	VLAN ID 12 bits

Tableau 3. 2 : « Détails du champ 802.1Q [15]»

3.2.2 La notion des trunks

Pour distribuer le réseau local virtuel on utilise des trunks. Un trunk est en fait la connexion physique sur laquelle transitent les trames de plusieurs VLANs. Ces trames sont identifiées par le VID afin d'arriver à bon port. On peut placer un trunk entre deux commutateurs, entre un commutateur et un hôte supportant le trunking et enfin entre un commutateur et un routeur pour effectuer un routage inter-VLAN. Il ne faut pas oublier que les VLANs transitant sur un même trunk se partagent la bande passante, c'est pourquoi il est recommandé d'utiliser des connexions à débit important, comme du Gigabit Ethernet ou de la fibre optique dans le meilleur des cas [15].

3.2.3 Spanning-Tree

Le protocole Spanning Tree (STP) est un protocole de couche 2 (liaison de données) conçu pour les commutateurs. Le standard STP est défini dans le document IEEE 802.1D-2004. Il permet de créer un chemin sans boucle dans un environnement commuté et physiquement redondant. STP détecte et désactive ces boucles et fournit un mécanisme de liens de sauvegarde. Le standard a été amélioré en incluant IEEE 802.1w Rapid Spanning Tree (RSTP). Le protocole STP a pour but d'éviter les cycles (et donc des trames qui se baladent) et doit être recalculé à chaque modification de la topologie d'un réseau. Un effet visible de l'utilisation de cette technologie est les blocages de quelques secondes voire dizaines de secondes que les utilisateurs peuvent observer lorsqu'une machine est insérée dans un réseau sur lequel il y a un arbre de recouvrement (débranchez une machine d'un commutateur, rebranchez-la et observez : si votre réseau se bloque

quelques temps c'est peut-être que votre commutateur recalcule son arbre de recouvrement) [17].

3.3 Quelques protocoles d'administration et de gestion des VLANs

Il est possible de configurer le 802.1q à la main pour permettre le transport des VLANs.

Pour cela, il faut configurer chaque port se trouvant sur le chemin d'un port tagué d'un VLAN à un autre. Il faut de plus répéter l'opération pour chaque lien défini.

On peut comprendre que le processus s'avère long et fastidieux. La norme prévoit donc des mécanismes pour taguer les ports automatiquement et administrer les VLAN d'une manière plus simple, plus abrégée et plus embryonnaire. Pour cela plusieurs protocoles ont été défini tels que le VTP, GVRP, DTP.

Dans ce qui suit, nous n'allons définir que le protocole VTP propriétaire CISCO, lequel nous allons utiliser par la suite dans le chapitre réalisation.

3.3.1 Le protocole VTP (VLAN Trunking Protocol)

Afin de ne pas redéfinir tous les VLANs existant sur chaque commutateur, CISCO a développé un protocole permettant un héritage de VLANs entre commutateurs. C'est le protocole VTP. Ce protocole est basé sur la norme 802.1q et exploite une architecture client-serveur avec la possibilité d'instancier plusieurs serveurs [16].

- **Comprendre le VTP (VLAN Trunking Protocol)**

Un commutateur doit alors être déclare en serveur, on lui attribue également un nom de domaine VTP. C'est sur ce commutateur que chaque nouveau VLAN devra être défini, modifie ou supprimé. Ainsi chaque commutateur client présent dans le domaine héritera automatiquement des nouveaux VLANs créent sur le commutateur serveur.

La mise en place d'un domaine VTP permet de centraliser la gestion des VLANs, ce qui peut s'avérer plus que plaisant dans un environnement abondamment commuté et comprenant de multiples VLANs.

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

a) **Mode serveur**, dans lequel le commutateur est chargé de diffuser la configuration aux commutateurs du domaine VTP.

b) **Mode client VTP**, dans lequel le commutateur applique la configuration émise par un commutateur en mode serveur.

c) **Mode transparent**, dans lequel le commutateur ne fait que diffuser, sans prendre en compte, la configuration du domaine VTP auquel il appartient.

- **Exemple d'utilisation des VTP**

Pour comprendre le fonctionnement des VTP, nous allons l'illustrer dans cet exemple ci-dessous (Figure 3.3).

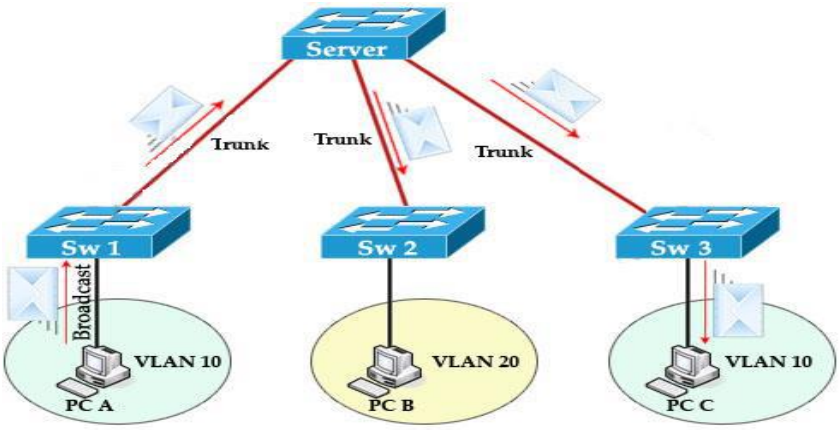

Figure 3. 3 : « Fonctionnement du protocole VTP [15]»

Les administrateurs peuvent changer les informations des VLAN sur les switchs fonctionnant en mode serveur uniquement. Une fois que les modifications sont appliquées, elles sont distribuées à tout le domaine VTP au travers des liens "trunk". En mode transparent, les modifications sont locales mais non distribuées. Les switchs en mode client appliquent automatiquement les changements reçus du domaine VTP.
Les configurations VTP successives du réseau ont un numéro de révision. Si le numéro de révision reçu par un switch client est plus grand que celui en cours, la nouvelle configuration est appliquée. Sinon, elle est ignorée. Quand un nouveau switch est ajouté au domaine VTP, le numéro de révision de celui-ci doit être réinitialisé pour éviter les conflits.

3.4 Procédure suivie pour l'élaboration de la solution VLANs

Les performances réseau représentent l'un des points principaux dans la productivité d'une entreprise. En effet, afin d'organiser la hiérarchie de l'architecture réseau de l'entreprise EPB, nous avons opté pour cette procédure qui débutera par :

- La sélection des matériels nécessaires à savoir :

  - Câble RJ45 droit croisé.
  - 2 switchs de niveau 3 (1 switch L3 – 1 switch L3 redondant).
  - 3 switchs cisco 2950.
  - Les ordinateurs.
  - Un serveur.
  - Un point d'accès (WiFi).
  - Un dispositif VoIP.

- L'organisation des directions et celà en utilisant le type VLAN de niveau 1 par port (c'est-à-dire attribuer chaque port d'un des trois switchs un VLAN qui représentera une des dix directions de l'entreprise).
- Elle se poursuivra en ajoutant 3 VLANs du même type (VLAN de niveau 1 par port) reliés à un autre switch qui représentera : VLAN Serveur, VLAN VoIP et VLAN point d'accès.

3.4.1 Nomination des VLAN et attribution des adresses IP

Tableau descriptif des noms attribuer aux VLANs : leurs numéros, adresses réseau, et le masque correspondant ainsi que l'adresse passerelle (voir le tableau ci-dessous)

Nom du VLAN	Numéro du VLAN	Adresse réseaux	Masque du réseau	Adresse passerelle
Vlan_DRH	2	172.16.2.0/24	255.255.255.0	172.16.2.1
Vlan_DSI	3	172.16.3.0/24	255.255.255.0	172.16.3.1
Vlan_DZLE	4	172.16.4.0/24	255.255.255.0	172.16.4.1
Vlan_DAM	5	172.16.5.0/24	255.255.255.0	172.16.5.1
Vlan_DFC	6	172.16.6.0/24	255.255.255.0	172.16.6.1
Vlan_DMA	7	172.16.7.0/24	255.255.255.0	172.16.7.1
Vlan_DL	8	172.16.8.0/24	255.255.255.0	172.16.8.1
Vlan_DDD	9	172.16.9.0/24	255.255.255.0	172.16.9.1
Vlan_DC	10	172.16.10.0/24	255.255.255.0	172.16.10.1

Vlan_DR	11	172.16.11.0/24	255.255.255.0	172.16.11.1
Vlan_VoIP	12	172.16.12.0/24	255.255.255.0	172.16.12.1
Vlan_p _acces	13	172.16.13.0/24	255.255.255.0	172.16.13.1
Vlan_serveur	14	172.16.14.0/24	255.255.255.0	172.16.14.1

Tableau 3. 3 : « Nomination des VLANs et attribution des adresses IP »

Ces trois switchs seront reliés à un switch principal (switch de niveau 3) ainsi qu'un autre qui n'est que le redondant de ce dernier et celà en utilisant le protocole VTP (VLAN Trunking Protocol), ainsi que le protocole STP (spanning-tree).

Switch	**Mode VTP**
SW_PRINCIPAL	Serveur
SW_PRINCIPAL_RED	Client
SW_DG	Client
SW_DGAF	Client
SW_DGAO	Client

Tableau 3.4 : « Tableau des modes VTP »

3.5 Solution messagerie

3.5.1 Définition des serveurs de messagerie

Un serveur de messagerie a pour vocation de recevoir et d'envoyer le courrier électronique à travers le réseau. Un utilisateur n'est jamais en contact direct avec ce serveur il l'utilise soit logiciel de messagerie soit un Webmail qui se charge de contacter le serveur pour envoyer et recevoir des messages via Internet [29].

3.5.2 Les différents Protocoles de la messagerie

3.5.2.1 Les protocoles de communication (de transport)

Le fonctionnement du courrier électronique repose sur une série de protocoles de communication destinés à envoyer ses messages, de serveur à serveur, à travers l'Internet. Les principaux protocoles sont les suivants : SMTP, POP3 ou encore IMAP4, chacun jouant un rôle bien précis.

- SMTP (Simple Mail Transfer Protocol) est le protocole standard permettant de transférer le courrier entre deux serveurs de messagerie: celui de l'expéditeur et celui du destinataire.
  Il spécifie aussi l'entête des courriers (from : to : etc...), les possibilités d'envoi groupé, la gestion des heures ou encore le format des adresses des utilisateurs [32].

- POP3 (Post Office Protocol) permet d'aller récupérer son courrier sur un serveur distant (le serveur POP). Ce protocole est nécessaire pour les personnes qui ne sont pas connectées en permanence à l'Internet messagerie. Mais ce protocole n'est, en revanche, pas sécurisé. Dans un logiciel de courrier, il faut toujours donner l'adresse de son serveur POP qui prendra généralement la forme suivante : pop. Nom_de_domaine [33].

Exemple : pop.yahoo.fr.

- IMAP4 (Interactive Mail Access Protocol), moins utilisé que POP, offre plus de possibilités. Cependant, de plus en plus de FAI utilisent ce protocole [33].

IMAP4 pourrait, à terme, remplacer progressivement POP3. La principale innovation d'IMAP4 réside dans la possibilité de gérer son courrier directement sur le serveur de son FAI. Tous les courriers et dossiers de messages restent sur le serveur.

3.5.2.2 Les Services de la messagerie

- MUA (Mail User Agent ou Agent de Gestion du Courrier `AGC') est un programme qui permet à un client de LIRE, ECRIRE un message électronique et de l'envoyer à l'Agent de routage qui va l'injecter dans le système de messagerie via le protocole SMTP [30].

- MTA (Mail Transfer Agent ou Agent de Transfert de Courriers `**ATC**') est un programme qui sert à transférer des messages électroniques entre des ordinateurs qui utilisent le protocole SMTP [30]. Il est composé de deux agents :

  - Un agent de routage des messages
  - Un agent de transport de messages

- MDA (Mail Delivery Agent ou Agent de Distribution de Courriers) : C'est un programme utilisé par l'Agent de Transfert de Courriers ATC pour acheminer le courrier vers la boite aux lettres du destinataire spécifié. Il distribue le courrier dans les boîtes des utilisateurs spécifiés [30].

3.5.3 Les étapes de l'envoi et de la réception des emails

- *Envoi*

Entre l'utilisateur et son serveur, l'envoi d'un courrier électronique se déroule généralement via le protocole SMTP. Puis c'est au serveur d'envoyer le message au serveur du destinataire, cette fonction est appelée Mail Transfer Agent en anglais, ou MTA.

- *Réception*

La réception d'un courrier électronique s'effectue elle aussi en deux temps. Le serveur doit recevoir le message du serveur de l'expéditeur, il doit donc gérer des problèmes comme un disque plein ou bien un engorgement de la boîte aux lettres et signaler au serveur expéditeur toute erreur dans la délivrance. Il communique à ce dernier par l'intermédiaire des canaux d'entrée-sortie standard ou bien par un protocole spécialisé comme LMTP (Local Mail Transfer Protocol). Cette fonction de réception est appelée Mail Delivery Agent en anglais, ou MDA. Le serveur doit renvoyer le message au destinataire final lorsque celui le désire, généralement via le protocole POP3 ou IMAP.

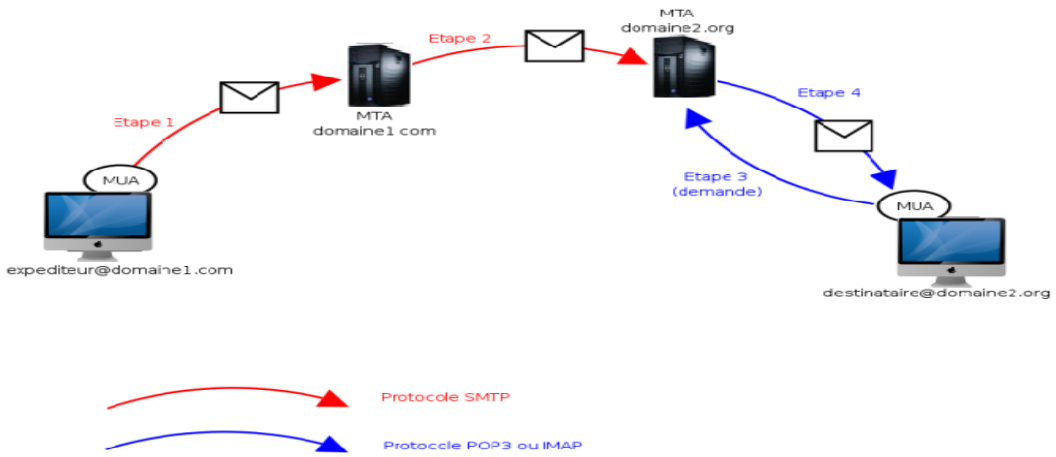

Figure 3. 4 : « les quatre étapes d'envoi d'emails »

3.5.4 Les Clients de messagerie

3.5.4.1 Les Clients lourds

Un client de messagerie de type lourd, est un logiciel qui permet de lire, d'écrire et d'expédier des courriers électroniques. Il s'installe sur un poste client qui se connecte au serveur de messagerie.

Le client lourd a l'avantage de récupérer nos messages et de les copier sur notre poste local, en mode connecté au serveur. Ainsi en mode hors connexion, nous avons accès à nos messages.

- Thunderbird de Mozilla
- Zimbra Desktop

3.5.4.2 Les Clients légers ou Web mail

Un client de messagerie de type léger est un logiciel qui est installé sur un poste client, permet de se connecter au serveur de messagerie via un navigateur web (Internet explorer, Firefox). Il fonctionne uniquement en mode connecté et ne copie pas en local les messages stockés sur le serveur. Ainsi, en mode hors connexion nous n'avons plus accès à nos courriers.

- MS Outlook Web Access
- Web mail Ajax de Zimbra
- Round cube

3.5.5 Le choix du serveur de messagerie

La messagerie est devenue un outil de travail à part entière. Son rôle aujourd'hui dépasse souvent les fonctionnalités d'envoi et de réception d'emails. Entre les différentes solutions propriétaires et open source, clients riches ou clients légers… il n'est pas facile de choisir. Quelle est la solution la mieux adaptée à votre société et à votre utilisation ? Avez-vous intérêt à externaliser ? Quels sont les contraintes sur la sécurité, et comment

me protéger des virus et des spams ? Les logiciels open source de messagerie électronique sont-ils une réponse satisfaisante ?

3.5.6 Les messageries collaboratives Open Source

Les logiciels open source de messagerie électronique sont depuis longtemps utilisés par la plupart des opérateurs et des ISP (Internet Service Provider), notamment pour leurs performances et leur disponibilité exemplaires, capables d'héberger un nombre très important de boîte aux lettres sur des configurations matérielles accessibles. Néanmoins, dès qu'on s'approche des besoins de messagerie collaborative (mobilité, agenda, …), ils ont longtemps accusé un retard important, soit sur le plan fonctionnel, soit sur le plan ergonomique.

Aujourd'hui, l'éventail de technologies et de solutions est plus large, et des clients de messagerie comme Thunderbird, de la fondation Mozilla, progresse à grande vitesse. Les alternatives au couple Exchange/Outlook sont donc de plus en plus intéressantes, et toujours aussi accessibles.

Outre les possibilités d'échange d'emails et de gestion des boites aux lettres, les solutions open source intègrent désormais les services d'annuaire d'entreprise, les meilleures protections par antivirus et antispam, et les fonctionnalités d'agenda et de calendrier partagé. Ils intègrent aussi un Webmail de grande qualité pour donner accès à la messagerie à vos utilisateurs nomades et à vos clients légers. Le mail server supporte la plupart des protocoles de messagerie. Il permet une grande capacité de stockage des messages et supporte la gestion des quotas. Les fonctionnalités d'alias, de forward et de mailing list facilitent la distribution d'emails à un groupe de destinataires. Pour choisir une solution plutôt qu'une autre il est important d'avoir une vision d'ensemble des interactions qu'offrent chaque solution avec des clients de messagerie tels qu'Outlook ou Thunderbird. Les plus importantes sont regroupées dans le tableau ci-dessous [31] :

		Calendrier					Contact			
		Lect./Écr.	Gestion des partages	Free/Busy	Hors-ligne		Lect./Écr.	Gestion des partages	Hors-ligne	
					Lect.	Écr.			Lect.	Écr.
Zimbra	Thunderbird	✓	✗	✓	✓	✗	✓	✗	✓	✓
	Outlook	✓(1)	✓(1)	✓(1)	✓(1)	✓(1)	✓(1)	✓(1)	✓(1)	✓(1)
	Zimbra Desktop	✓	✓	✓	✓	✓	✓	✓	✓	✓
SOGo	Thunderbird	✓	✗	✓	✓	✗	✓	✗	✓	✓
	Outlook	✗	✗	✗	✗	✗	✗	✗	✗	✗
eGroupware	Thunderbird	✓	✗	✗	✓	✗	✓	✗	✓	✓
	Outlook	✓(2)	✗	✗	✗	✗	✗	✗	✗	✗
Horde	Thunderbird	✓	✗	✗(4)	✓	✗	✓	✗	✓	✓
	Outlook	✓(2)	✗	✗	✗	✗	✗	✗	✗	✗
Open-Xchange	Thunderbird	✗(3)	✗	✗	✓	✗	✗	✗	✗	✗
	Outlook	✓(1)	✓(1)	✓(1)	✓(1)	✓(1)	✓(1)	✓(1)	✓(1)	✓(1)
Kolab	Thunderbird	✓	✗	✗	✓	✗	✓	✗	✓	✓
	Outlook	✓(2)	✗	✗	✗	✗	✗	✗	✗	✗
Bedework	Thunderbird	✓	✗	✓	✓	✗	Fonctionnalités non supportées			
	Outlook	✓(2)	✗	✗	✗	✗	Fonctionnalités non supportées			
Apple Calendar Server	Thunderbird	✓	✗	✗	✓	✗	Fonctionnalités non supportées			
	Outlook	✗	✗	✗	✗	✗	Fonctionnalités non supportées			

(1) demande l'achat de licences
(2) avec la version 2007 d'outlook
(3) en lecture seule
(4) en cours de développement

Tableau 3. 5 : « tableau comparative des serveurs de messagerie [31] »

3.5.7 Explication de notre choix pour une messagerie Zimbra

Zimbra répond en tous points aux principales problématiques que rencontre une DSI quant au choix d'une messagerie professionnelle [33] :

Mode d'utilisation :

- Flexibilité : augmentation/baisse du nombre de licences Zimbra utilisées.
- Collaborativité : partage/superposition d'agendas, de documents, de carnets d'adresses, gestion de GAL (Global Address List), messagerie instantanée, etc.
- Utilisation intuitive.
- Nomadisme : votre messagerie Zimbra est consultable via un webmail sur votre navigateur (Microsoft Internet Explorer, Mozilla Firefox, Apple Safari), avec les mêmes fonctionnalités que sur le client lourd.
- Mobilité : synchronise en mode Push avec les principaux OS embarqués sur vos Smartphones : iOS, BlackBerry (connecteur natif BlackBerry Enterprise Server), Android, Symbian OS, Palm OS & Windows Mobile (connecteur Zimbra Mobile).
- Interopérabilité : avec MS Outlook, Thunderbird, etc.

Sécurisation des données :

- Certificat SSL pour garantir la confidentialité de vos données.
- En option, un module d'archivage légal (Zimbra Archiving&Discovery) : il s'agit d'un mécanisme d'archivage à valeur probatoire avec une durée de rétention définie, dans le cas où un courriel peut éventuellement constituer une preuve.
- Antispam et antivirus en standard.

Paramétrages :

- Evolutivité : augmentation/baisse de la volumétrie d'une BAL.
- Interface d'administration pour créer/ajouter/supprimer des BAL.
- Reporting et statistiques, pour répondre à vos besoins de supervision.
- Définition de rôles des utilisateurs : paramétrage des accès, des droits, etc.
- Personnalisation possible : logo, thème, etc.
- Intégration d'applications métiers ou d'applications tierces (Facebook, Wikipedia ou Google Translator) : grâce aux zimlets (extensions open source).

Indexation des messages et des pièces jointes (possibilité de recherche jusque dans la pièce jointe) [20].

3.6 CONCLUSION

Dans ce chapitre nous avons pu aborder en détails les différentes solutions proposées pour l'amélioration de l'architecture réseau de l'EPB, ainsi que différents outils importants pour la réalisation de ces dernières.

Dans le prochain chapitre, nous présenterons les outils avec lesquels nous avons simulé et réalisé les solutions que nous avions proposées précédemment.

CHAPITRE 4

REALISATION

Introduction

Dans ce chapitre, nous allons passer à la dernière étape qui est la réalisation. Cette phase est cruciale pour la mise en place de tout ce que nous avons vu et fait auparavant, nous implémenterons les solutions précédemment proposées et conçues, pour ce faire nous commencerons par la présentation des outils utilisés, puis nous expliquerons en détail les différentes étapes suivies pour la réalisation de l'architecture LAN et la création des VLANs, ainsi que la réalisation de la messagerie électronique.

4.1 Les outils utilisés pour la réalisation de nos solutions

Plusieurs outils sont nécessaires pour simuler et mettre en œuvre ce dont on a proposé comme solutions dans notre travail, et on citera :

4.1.1 Simulateur cisco packet tracer

Packet Tracer 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 …[25].

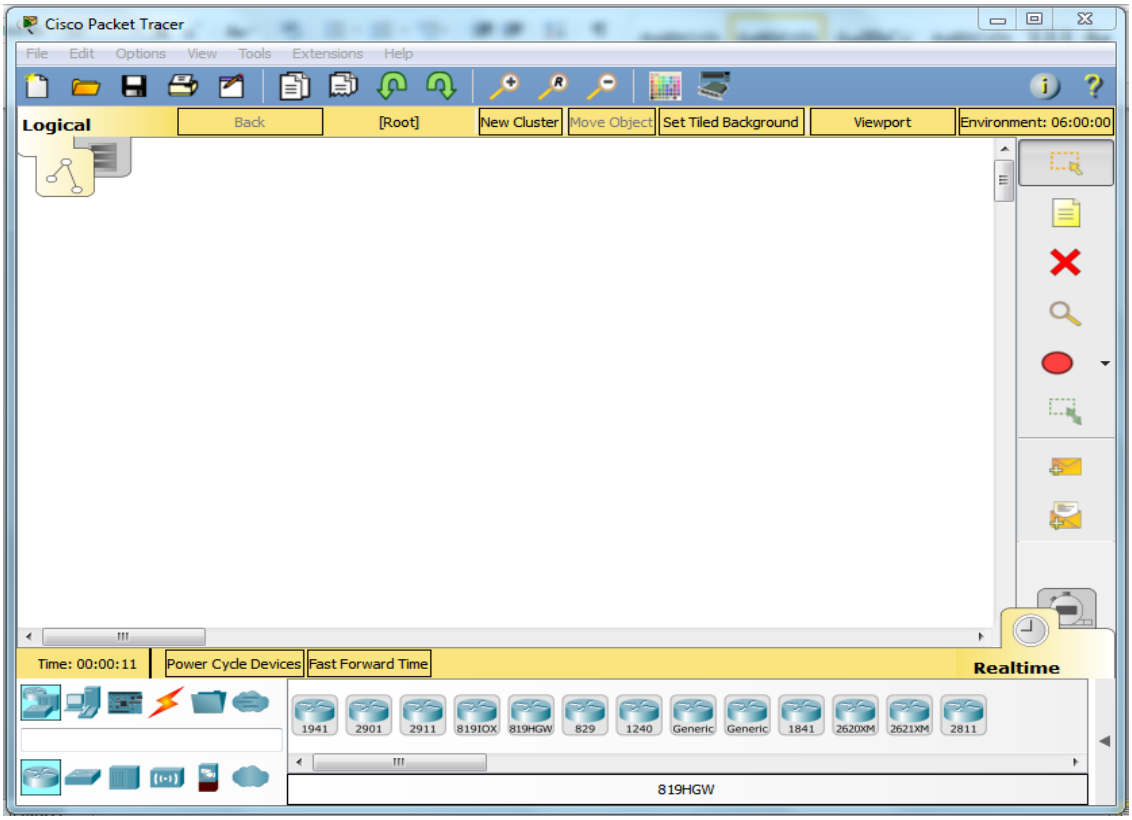

Figure 4. 1 : « Interface Packet Tracer »

4.1.2 Pfsense

Pfsense est un logiciel open source tournant sous FreeBSD. Il possède les fonctionnalités d'un pare-feu mais également d'un routeur. Il permet d'intégrer également de nouveaux services tels que l'intégration d'un portail captif, la mise en place d'un VPN, et bien d'autres [19].

- **Fonctionalité du pfsense :**

Pfsense est :

- **Un fournisseur de services** tel que :

  - Serveur de temps : NTPD ;
  - Relais DNS ;
  - Serveur DHCP ;
  - Portail captif de connexion.

- **Un routeur** entre un WAN et un LAN, différents segments, VLANs, DMZs :

  - il implémente les protocoles RIP, OLSR, BGP ;

• il permet de mettre en place des VPNS : OpenVPN,IPsec, PPTP.

- Un firewall capable de :

• faire de la traduction d'adresses : NAT, SNAT, DNAT ;

• faire du filtrage de paquets entre WAN et LAN et entre deux réseaux reliés par VPN ;

• faire de la QoS : « traffic shaper » ;

• faire du « load balanching » avec plusieurs connexions Internet [19].

4.1.3 VMware Workstation

Une version station de travail du logiciel qui permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique (machine existant réellement), et il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'ordinateur hôte. La version Linux présente l'avantage de pouvoir sauvegarder les fichiers de la machine virtuelle (* .vmsd) pendant son fonctionnement [26].

4.1.4 CentOS 6.9

CentOS (Community **ent**reprise Operating System est une distribution 100% open source, distribuée gratuitement, Et basée sur la RHEL de red_hat ,) est une distribution GNU/Linux principalement destinée aux serveurs elle est utilisée par 20 % des serveurs web Linux, elle est l'une des distributions Linux les plus populaires pour les serveurs web [21].

4.1.5 Zimbra 8.7.7

Zimbra est un serveur de messagerie avec des fonctionnalités de travail collaboratif.

La version Open Source comprend la fonction de serveur de messagerie, de calendriers partagés, de carnets d'adresses partagés, de gestionnaire de fichiers, de gestionnaire de tâches, wiki, messagerie instantanée.

La version Network (payante) comprend en plus le connecteur MAPI pour MS Outlook, un système de sauvegarde/restauration à chaud par boîte mail, un serveur de synchronisation (Zimbra Mobile) en option etc [22].

4.2 Pour la réalisation des solutions VLANs

4.2.1 Sous packet tracer

Nous allons suivre les étapes de configurations illustrées ci-dessous :

- Configuration des Hostnames: (Nomination des équipements sur « Cisco Packet Tracer »).
- Configuration des mots de passe
- Configuration de VTP.
- Configuration des VLANs.
- Configuration des interfaces.
- Configuration de Spanning-Tree.
- Test inter VLAN (ping entre le vlan_DRH et le vlan_serveur)
- Insertion des ACL.

4.2.1.1 Configuration des hostname

Cette configuration a pour but de renommer les commutateurs par des noms significatifs Nous prendrons comme exemple le switch de niveau3 (le switch fédérateur) dans la (Figure 4.2), sachant que c'est la même procédure pour les autres commutateurs

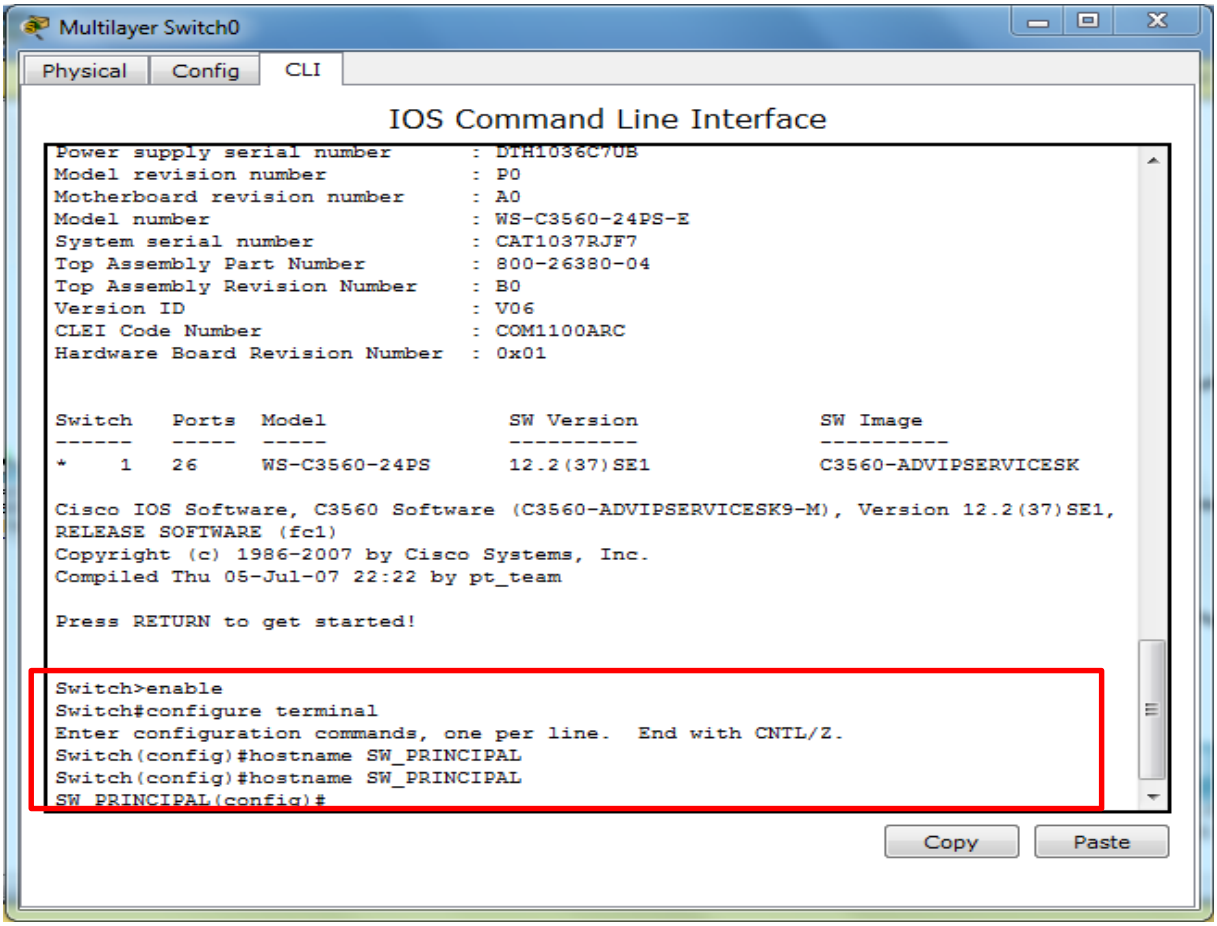

Figure 4. 2 : « Nomination d'un switch fédérateur (switch de niveau 3) »

4.2.1.2 Configuration des mots de passe

Nous allons maintenant passer à la configuration des mots de passe.

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

Notre choix c'est porté sur « epbconsole » comme mot de passe via console, l'exemple que nous prendrons est le SW_DGAF. La figure 4.3 montre les commandes de mise en place du mot de passe. La même chose sera faite pour les autres commutateurs.

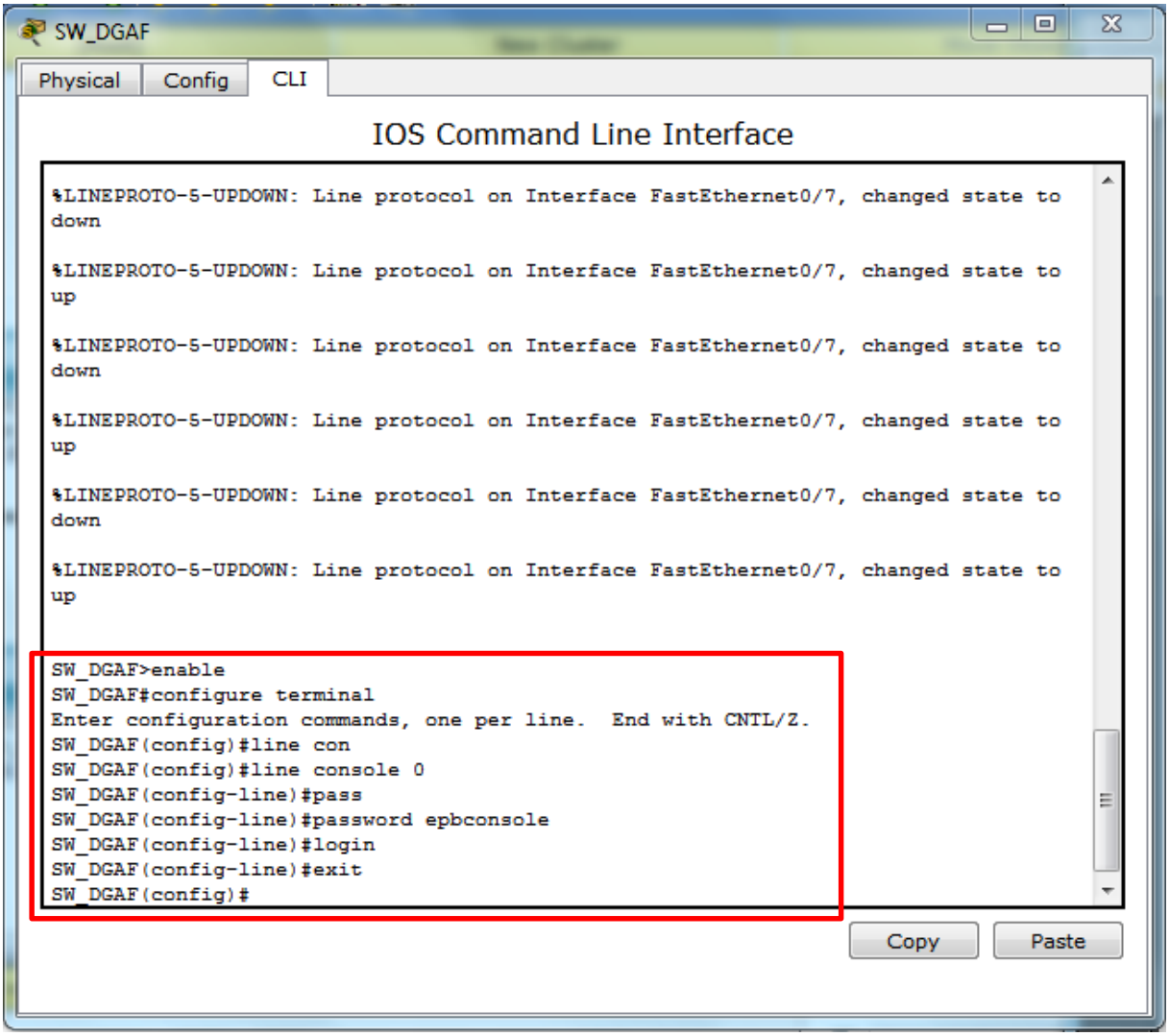

Figure 4. 3 : « Attribution du mot de passe console au SW_DGAO »

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

Pour sécuriser l'accès au mode privilégié, nous avons choisi le mot de passe epbsecret.

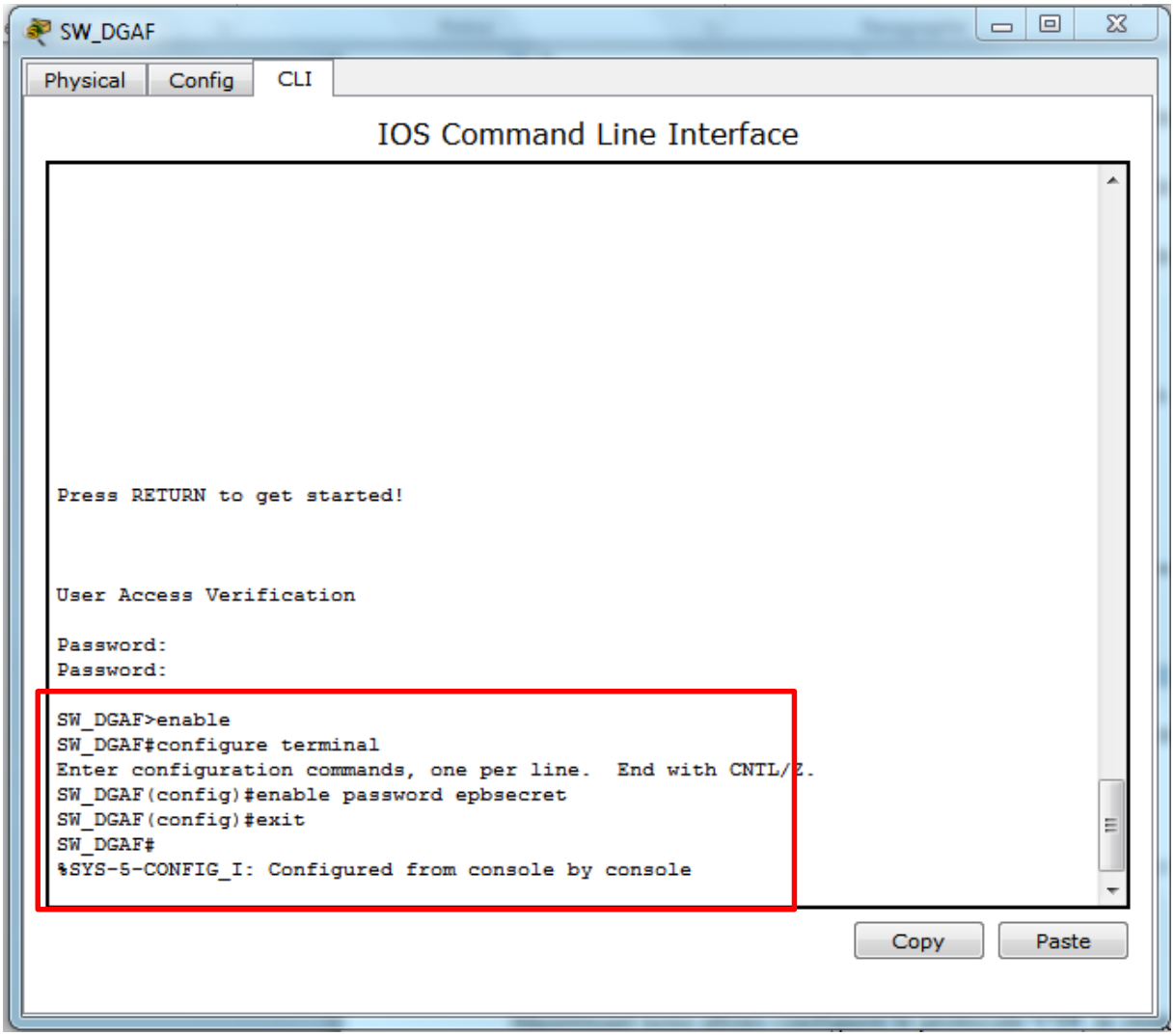

Figure 4. 4 : « Attribution du mot de passe pour le mode privilégié au SWC_DGAF »

4.2.1.3 Configuration des VLANs

Dans cette partie de configuration nous attribuons les adresses IP de passerelle pour chaque VLAN au niveau du Switch-cœur, nous prendrons comme exemple le vlan_DRH comme illustré dans la (Figure 4.5) puis par la suite continuer pour chaque VLAN.

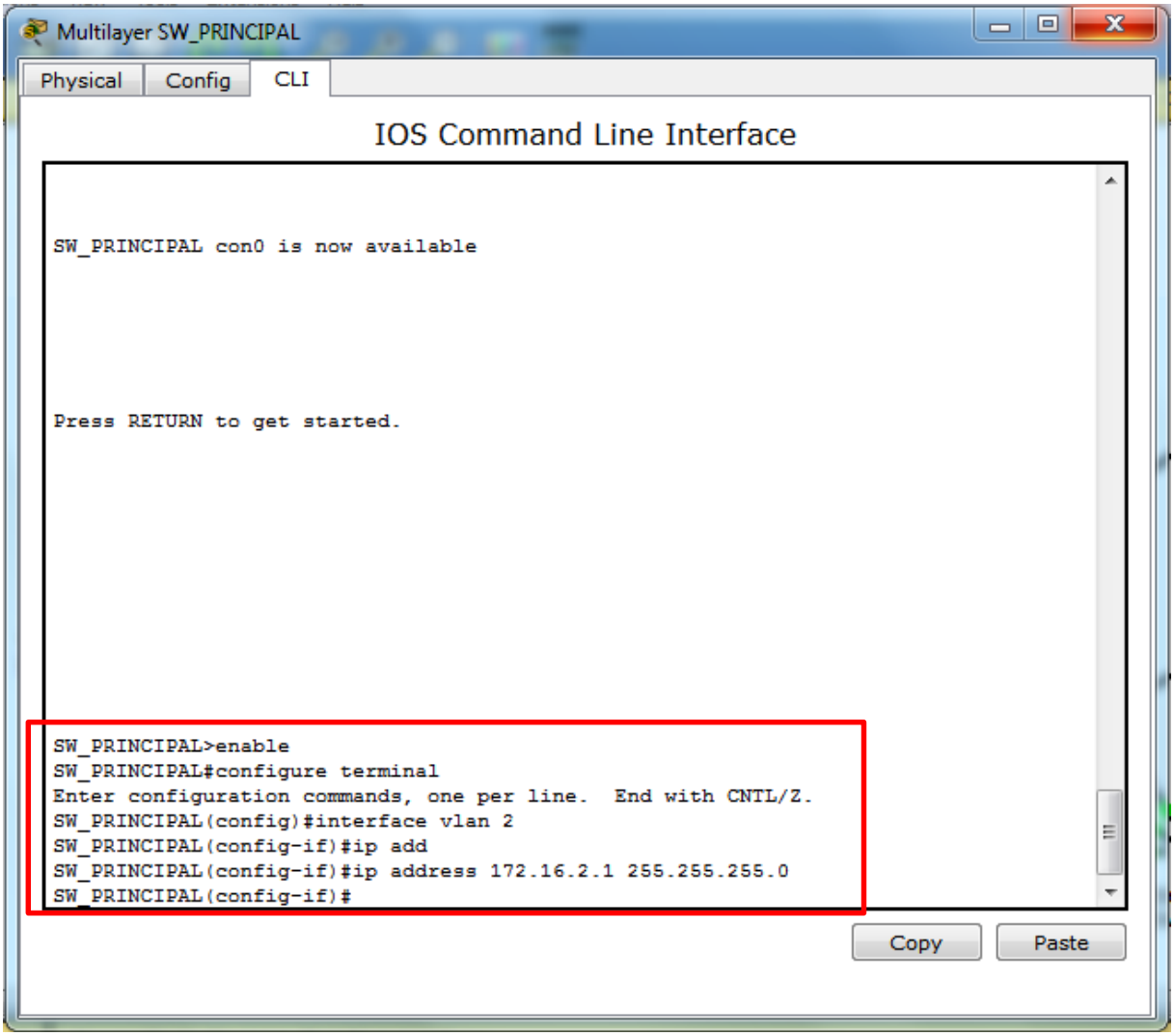

Figure 4. 5 : « Interfaces des VLANs au niveau de SW_PRINCIPAL »

4.2.1.4 Configuration du protocole VTP

Maintenant nous allons configurer le protocole VTP, le switch principal sera configuré en mode serveur (Figure 4.6) et les switchs d'accès ainsi que le switch redondant de niveau 3 en mode client. Nous prendrons le switch DGAO comme exemple (Figure 4.7), la même chose sera appliquée aux autres commutateurs.

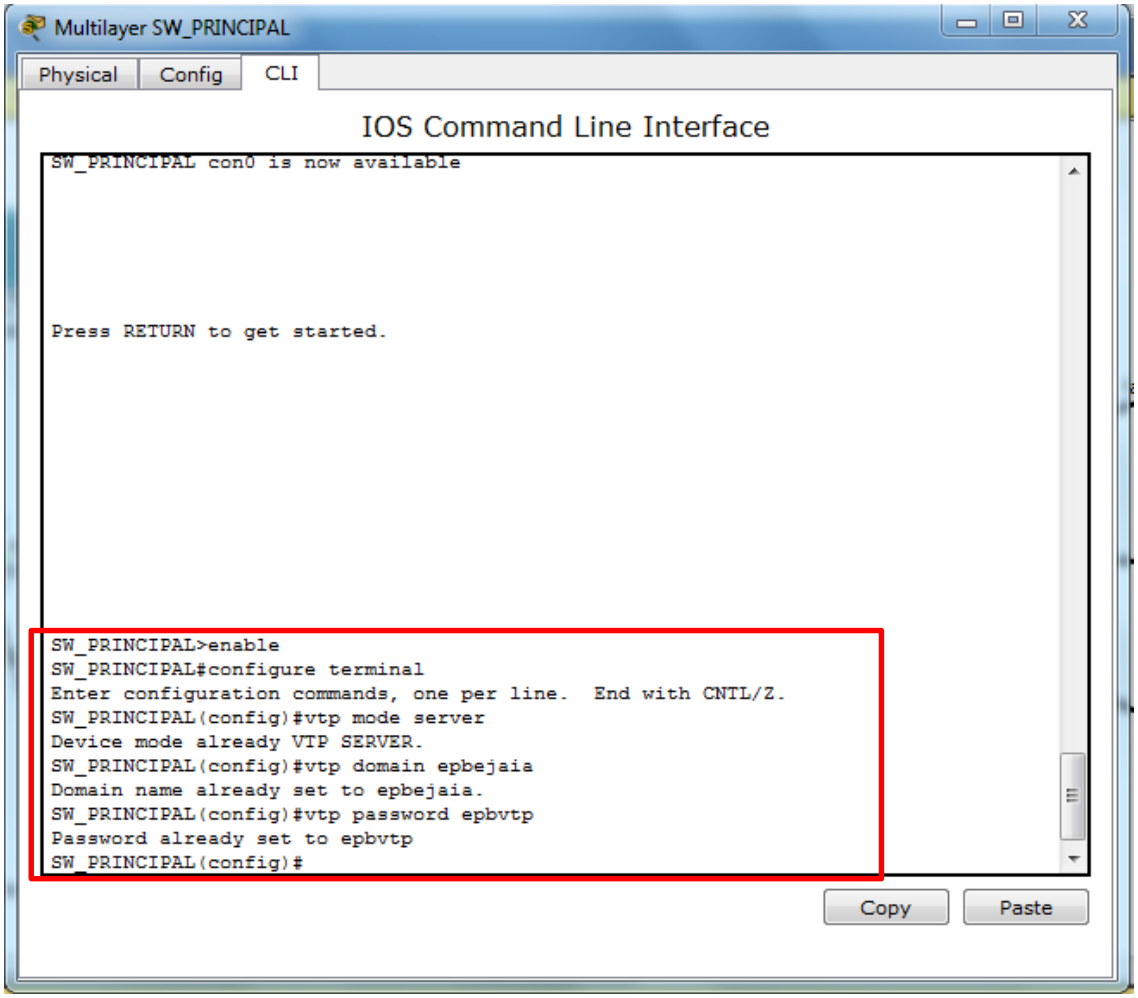

Figure 4. 6 : « configuration du protocole VTP en mode serveur du switch fédérateur »

Configuration du protocole VTP dans le switch DGAO en mode client

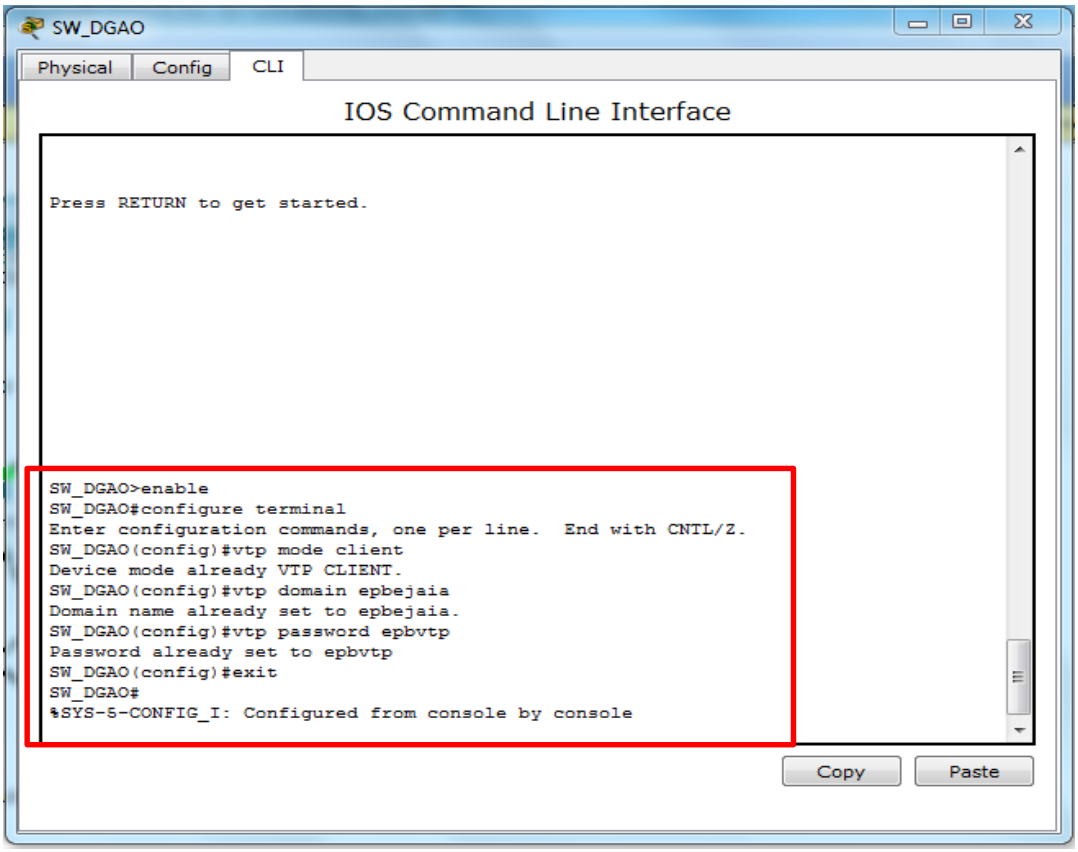

Figure 4. 7 : « configuration du protocole vtp en mode client du switch DGAO »

4.2.1.5 Configuration de Spanning-Tree

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

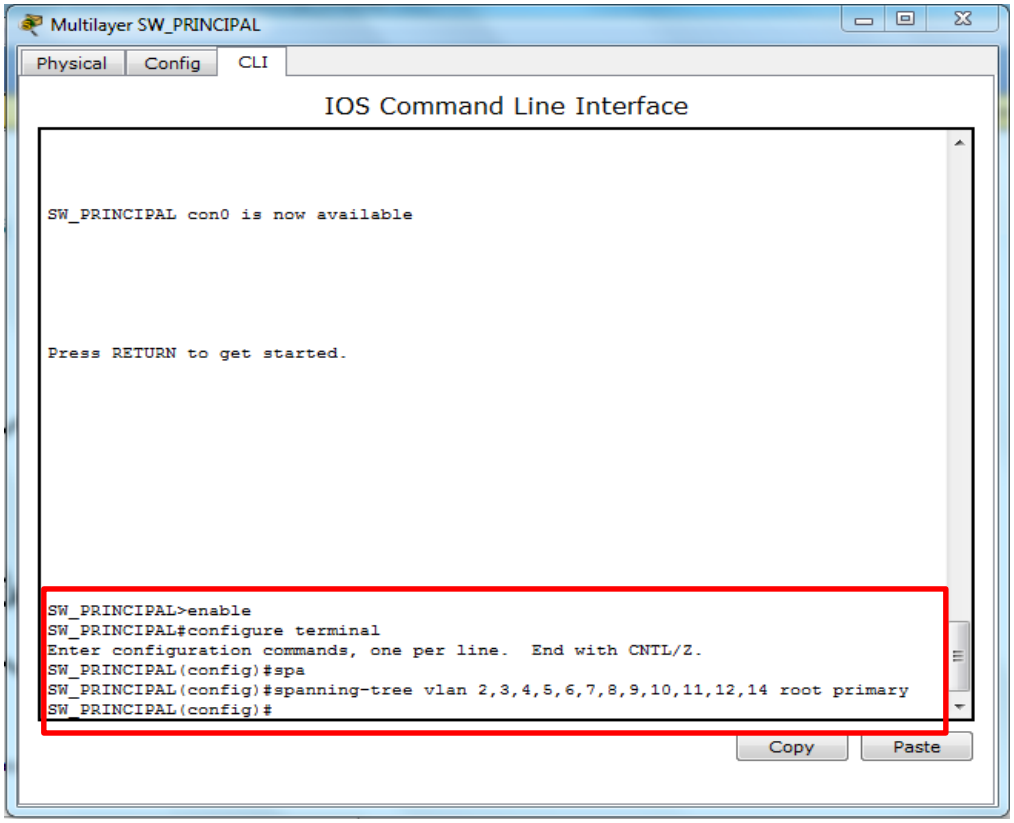

Figure 4. 8 : « configuration du Spanning Tree »

4.2.1.6 Test inter vlan (ping entre le vlan_DRH et le vlan_serveur)

Dans cette partie nous allons montrer la connectivité entre le vlan de la direction DRH et le vlan serveur dans la (figure 4. 9)

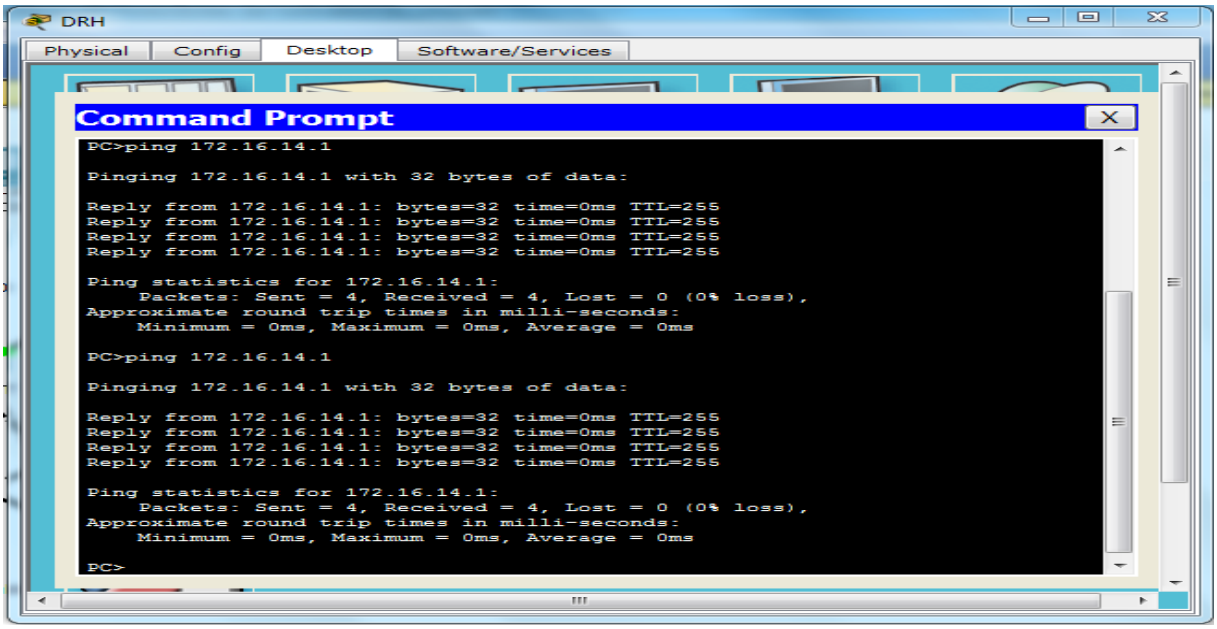

Figure 4. 9 : « ping entre le vlan_DRH et le vlan_serveur »

4.2.1.7 Insertion des ACL

Nous allons maintenant utiliser les listes des contrôles d'accès afin de limiter la communication entre certains VLANs, nous avons pris comme exemple le VLAN 2 de la direction DRH (direction des ressources humaines) auquel nous avons bloqué la communication avec d'autres VLANs tels que vlan_DSI comme le démontre la figure ci-dessous.

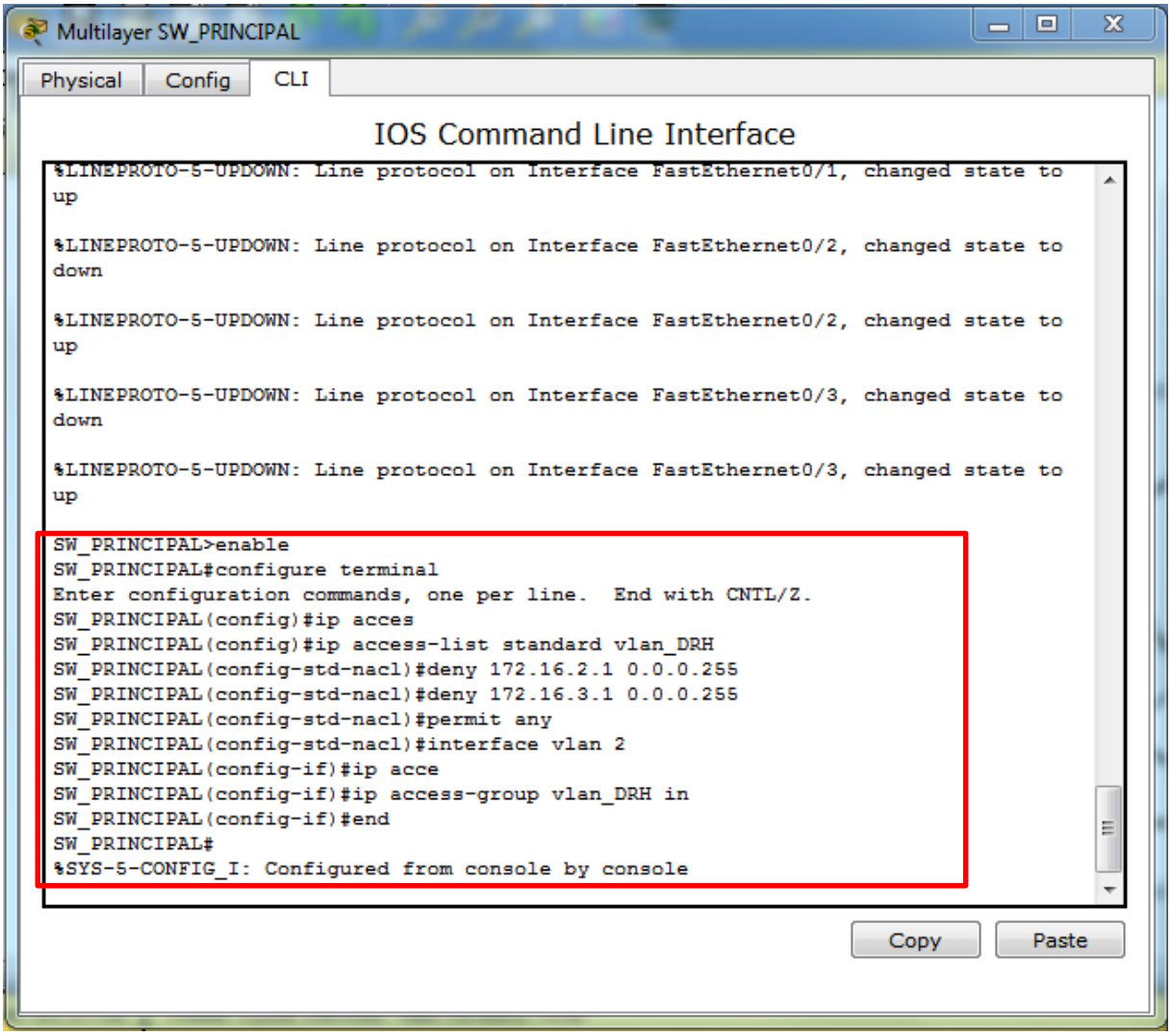

Figure 4. 10 : « ACL au niveau du VLAN de la direction des ressources humaines(DRH) »

4.2.1.8 Architecture réalisée

La Figure 4.11 représente l'architecture réalisée.

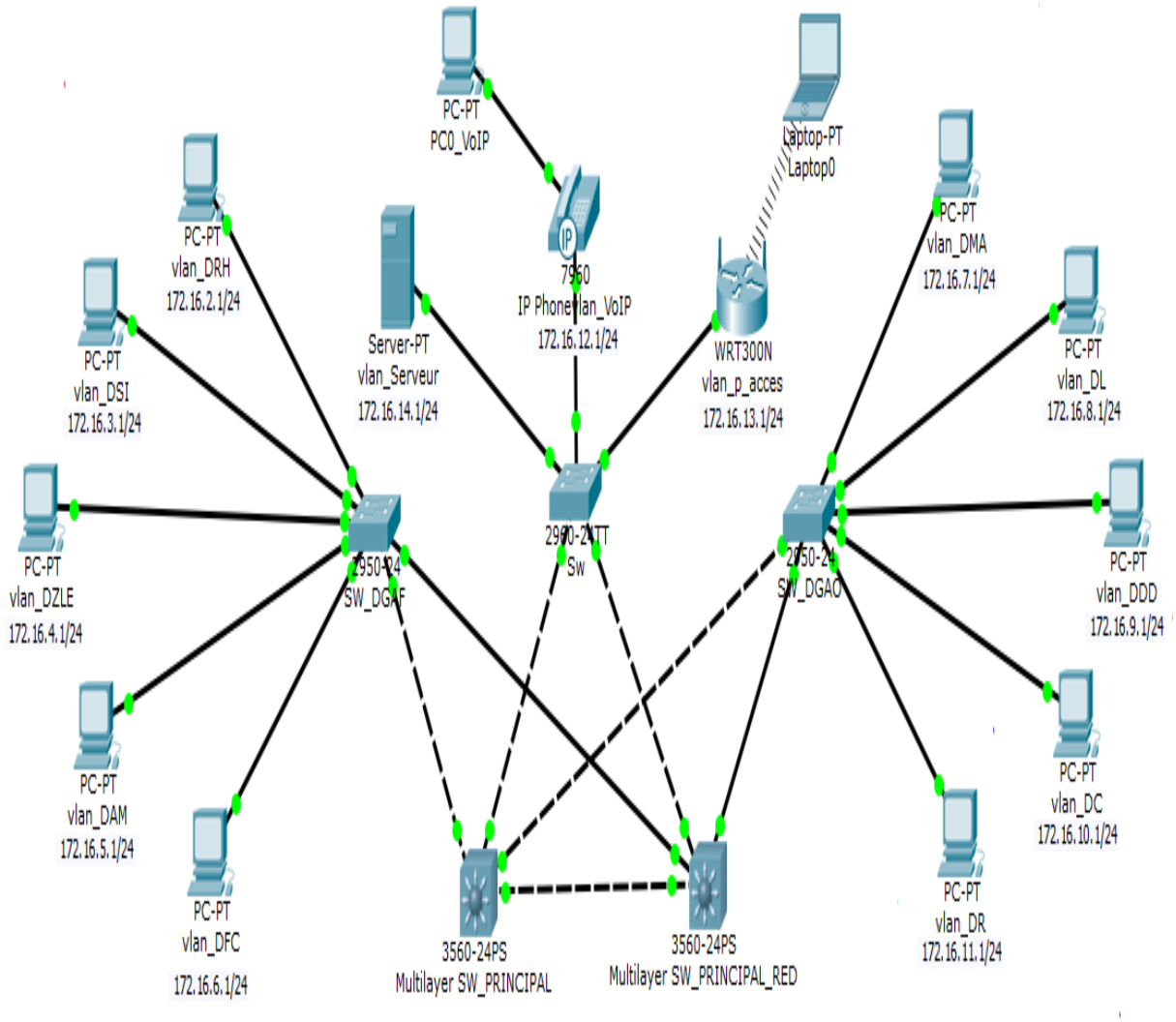

Figure 4. 11 : « Architecture réalisée pour le réseau de l'EPB »

4.2.2 Configuration des VLANs sous pfSense

Sur le pfSense, notre domain s'intitule pfsense.epbejaia, nous configurerons donc nos VLANs :

- VLAN "vlan SERVEURS" -VLAN "vlan DG" -VLAN "vlan DFC"
- VLAN "vlan WIRELESS" -VLAN "vlan DGAF" -VLAN "vlan DRI"
- VLAN "vlan VoIP" -VLAN "vlan DDD" -VLAN "vlan DL"
- VLAN "vlan DMA" - VLAN "vlan DAM"
- VLAN "vlan DRH"

NB : Les adresse des sous réseaux sont déjà déclarés dans la configuration des VLANs sous packet tracer

On

Pour commencer, dans le menu "Interface" on choisi "(assign)" :

Figure 4. 12 : le menu « interface »

Puis, dans l'onglet 'VLANs', on clique sur l'icône en forme de "+" qui se trouve en bas à droite de l'interface et on attribue les éléments de configurations suivants :

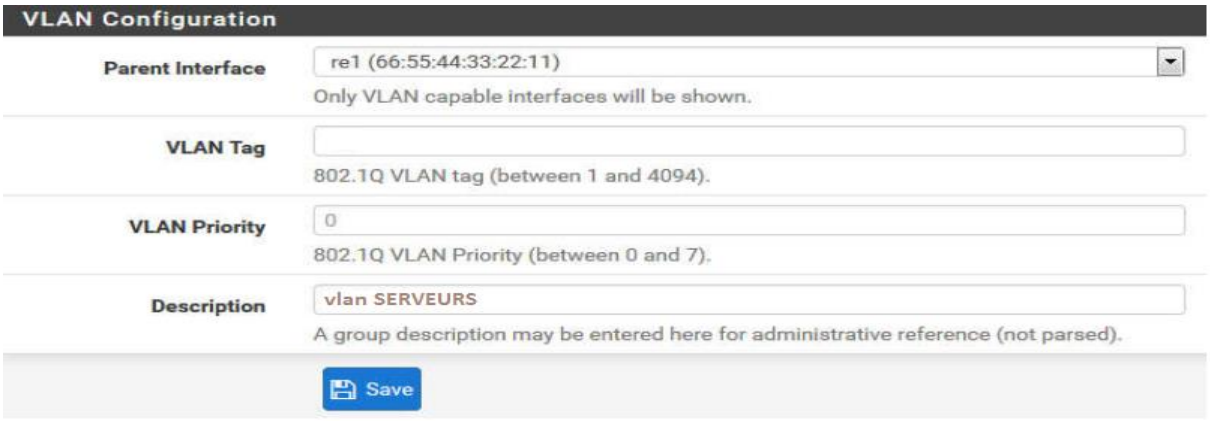

Figure 4. 13 : « configuration des VLANs »

Et une fois nos 13 VLANs créés, nous disposons de 13 interfaces virtuelles :

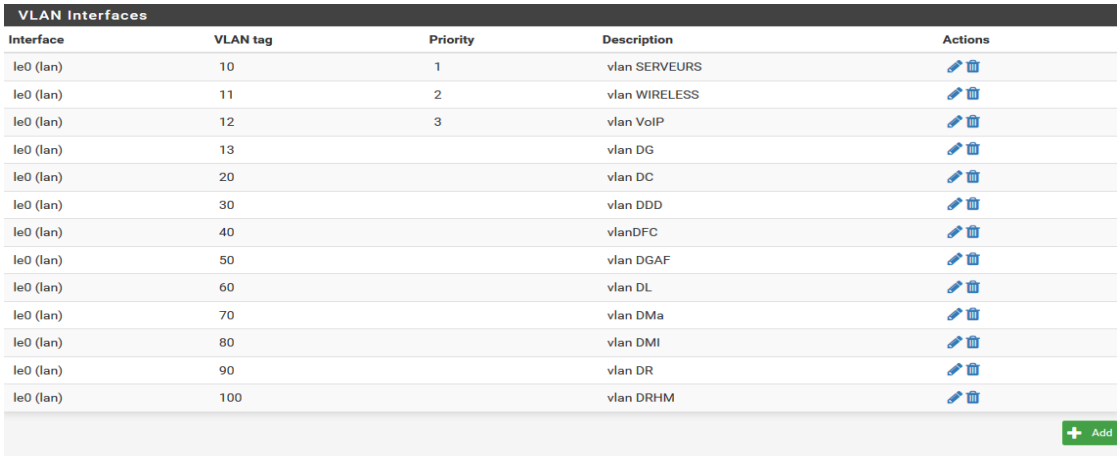

Figure 4. 14 – interface des VLANs

Afin de configurer nos VLANs, nous devons maintenant associer ces interfaces virtuelles à des interfaces logiques.

Pour cela dans l'onglet "Interface assignements", on clique sur l'icône en forme de "+" se situe en bas à droite de l'interface afin d'ajouter une nouvelle interface logique.

Par défaut, l'interface logique créée porte le nom "OPT1" (ou OPT2, OPT3, etc.).

Nous associons cette interface logique à l'interface virtuelle du VLAN que nous avons créé précédemment

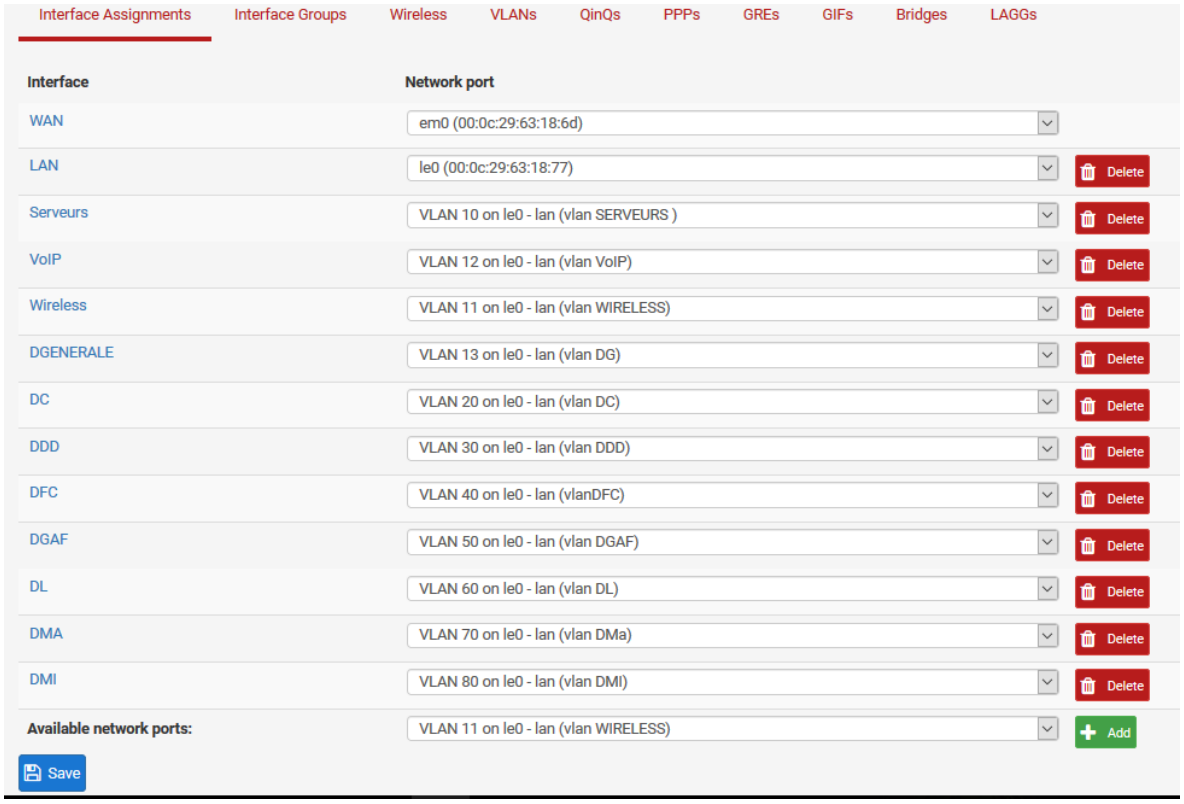

Figure 4. 15 : « associer les interfaces virtuelles à des interfaces logiques »

4.2.2.1 Activation de l'interface du VLAN

Pour modifier l'interface logique créée (et la renommer), nous cliquons sur son nom. Les éléments de configuration sont les suivants :

1. **Enable Interface** : on coche cette case pour activer l'interface
2. **Description** : nom de l'interface
3. **IPv4 Configuration Type** : la configuration IPv4 de cette interface. Dans notre cas, nous choisissons "Static IPv4"
4. **IPv6 Configuration Type** : la configuration IPv6 de cette interface. Dans notre cas, nous choisissons "None"
5. **MAC controls** : par défaut, c'est l'adresse MAC de l'interface physique qui est utilisée. Elle peut être personnalisée ici
6. **MTU** : la MTU pour cette interface. 1500 octets par défaut
7. **MSS** : "Maximum Segment Size", devrait être inférieur au MTU. Nous laissons vide
8. **Speed and duplex** : nous laissons le choix par défaut

Enfin, nous appliquons les paramètres de configuration IP (adresse IP de l'interface et masque réseau associé).

Exemple de résultat obtenu :

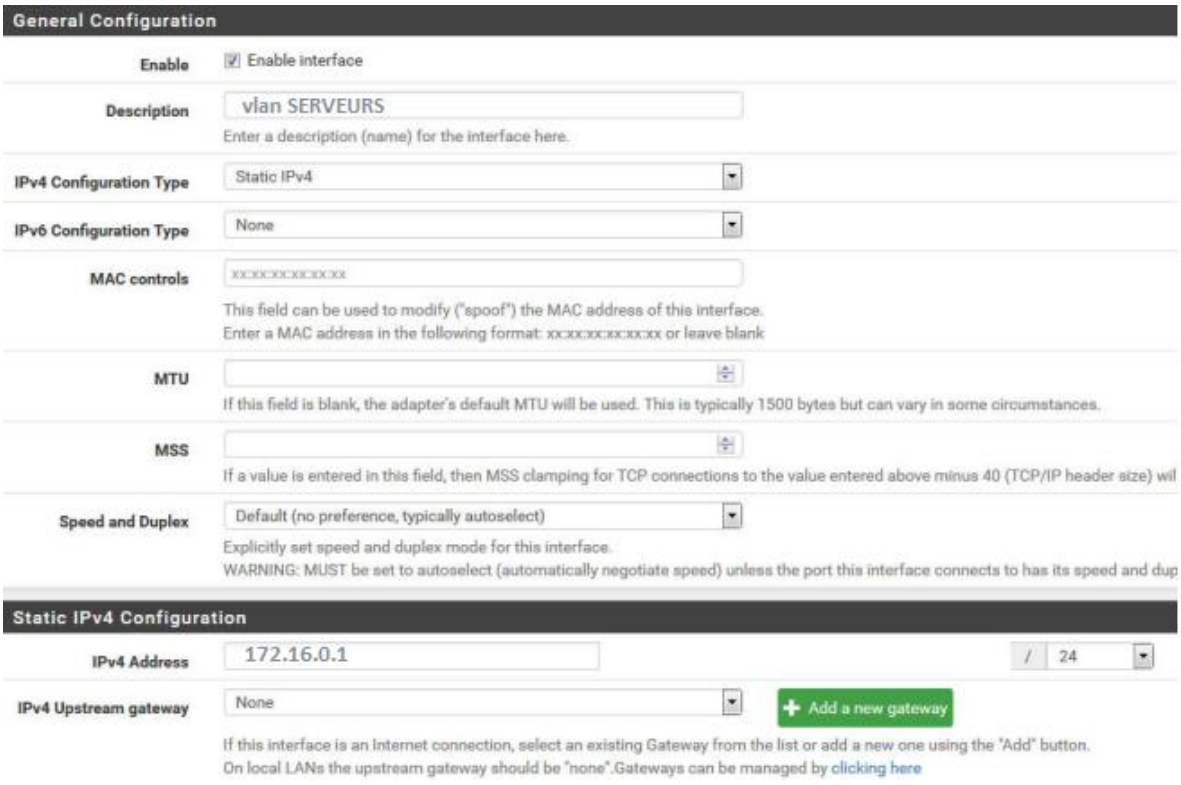

Figure 4. 16 : « Activation de l'interface du vlan dans configuration générale »

4.2.2.2 Activer le DHCP dans un VLAN donné :

Ici on va prendre comme exemple le VLAN VoIP parce que dans le vlan serveurs on attribue les adresse statiquement on active le DHCP sur l'interface la plage d'adresse qu'on a déclaré c'est de (172.16.5.1 jusqu'à 172.16.5.50) ce qui veut dire qu'on pourra avoir 50 appareils VoIP sur ce VLAN.

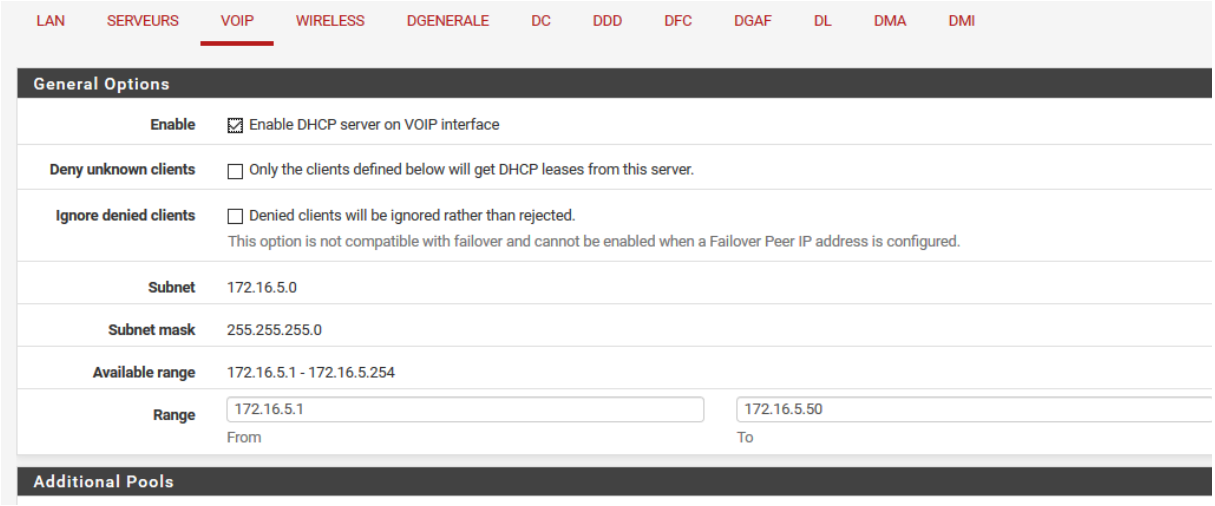

Figure 4. 17 : « Activer le DHCP dans un vlan donné »

4.2.2.3 Liste des VLANs et leurs interfaces et adresses associées :

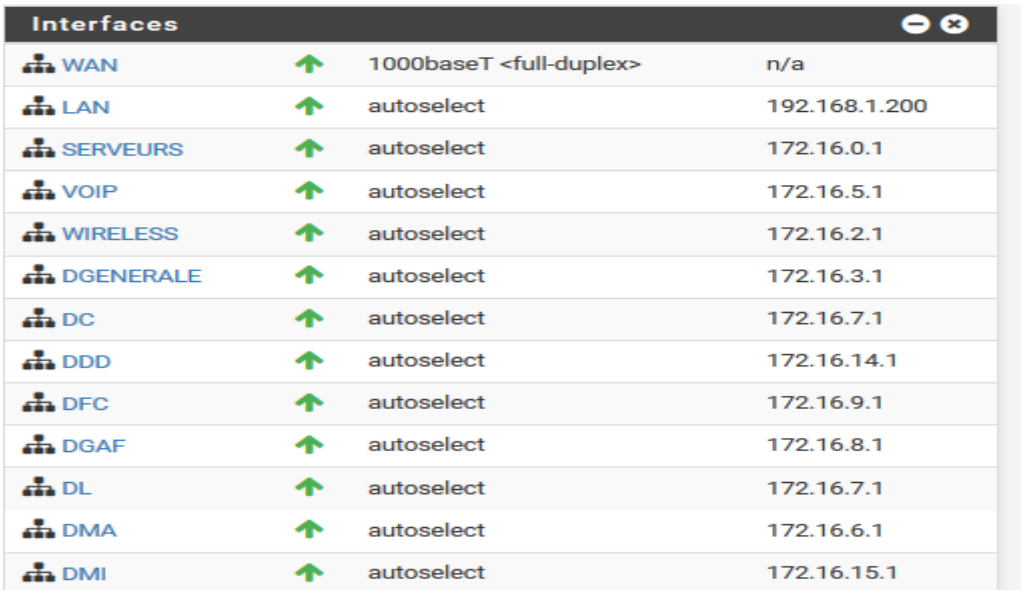

Figure 4. 18 : « Liste des VLANs et leurs interfaces et adresses associées »

4.2.2.4 Simulation d'une VM dans un VLAN :

Ici va connecter une VM (Windows 7) a une interface du VLAN VoIP (vmnet 3)

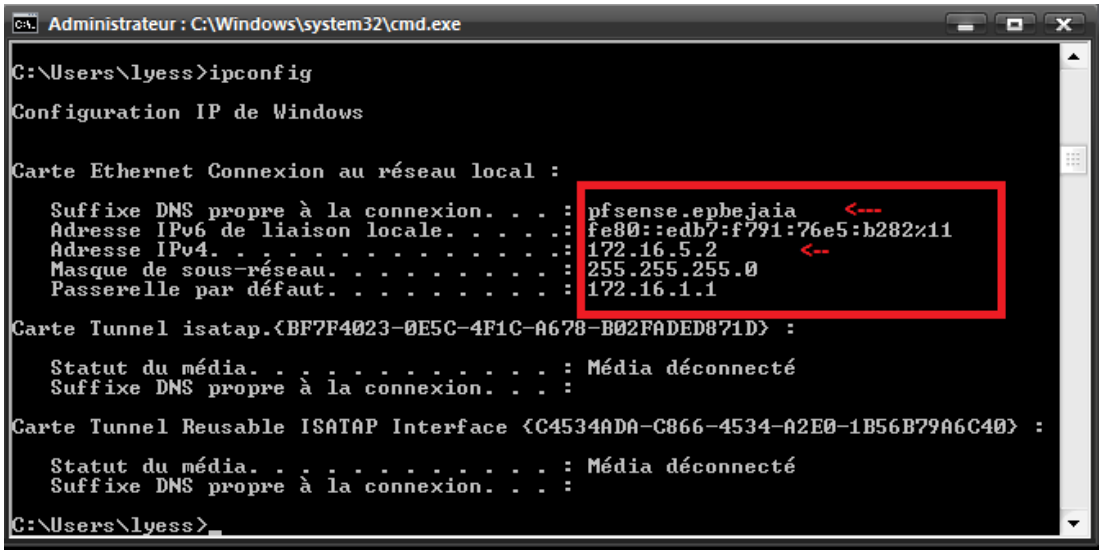

Figure 4. 19 : « Simulation d'une VM dans un VLAN »

4.3 Configuration de la messagerie

Installation et configuration des composants de notre serveur de messagerie ZIMBRA ainsi que les différentes étapes à suivre et les différents éléments a installés et a configurés afin de mettre en œuvre notre serveur de messagerie.

On configure le DNS (Serveur de Noms de Domaines) les caractéristiques d'adressage du réseau local du l'entreprise.

- Nom machine : lyes@centos01
- Domaine : linuxlab.local
- Adresse IP : 192.168.1.100
- Netmask : 255.255.255.0
- Passerelle : 192.168.1.1
- DNS1 : 192.168.1.100

L'installation et la configuration du serveur vont se dérouler en trois grandes phases qui sont :

_ Installation du système d'exploitation CentOS 6.9
_ Installation et Configuration du serveur DNS
_ Installation et configuration de Zimbra 8.7.7

4.3.1 Installation du système d'exploitation CentOS 6.9

Préparation de Notre Linux serveur (CentOS 6.9) :

Après avoir installé CentOS 6.9 qui est supporté par ZIMBRA, dans la configuration des interfaces réseau, on clique sur 'edit network ' puis 'network connexion' puis on change l'interface « eth0 » type de connexion IPV4 de automatic DHPC en manuel (configuration static) (voir la figure4.20)

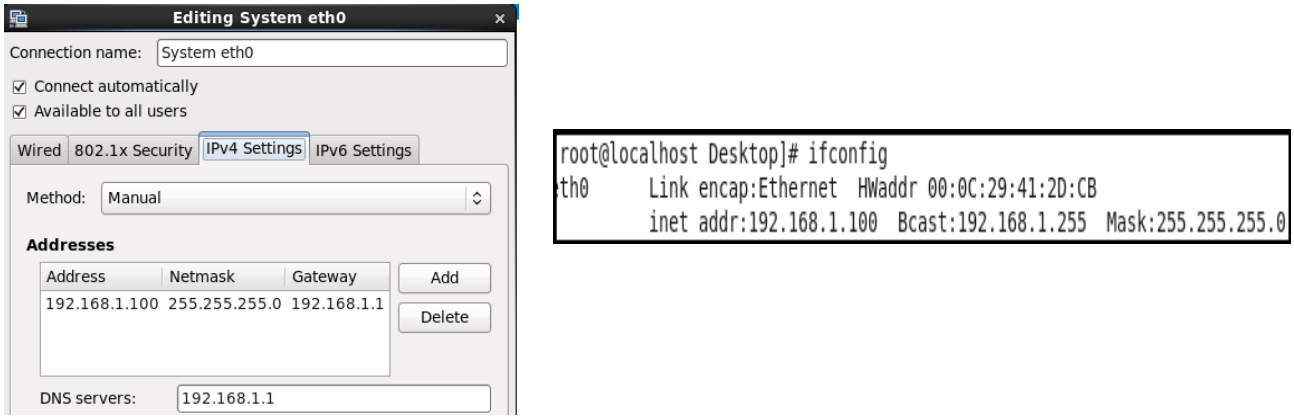

Figure 4. 20 : « Configuration de l'interface réseaux eth0 »

4.3.2 Installation et configuration du serveur DNS (BIND9) :

- téléchargement du BIND 9 avec la commande :

#Yum install bind

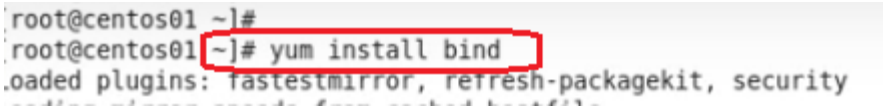

Figure 4. 21 : « commande pour télécharge le BIND 9 »

- Activation du service named avec la commande :

 # Chkconfig named on

- Modification du dossier named.conf

On accède avec la commande

#nano /etc/named.conf

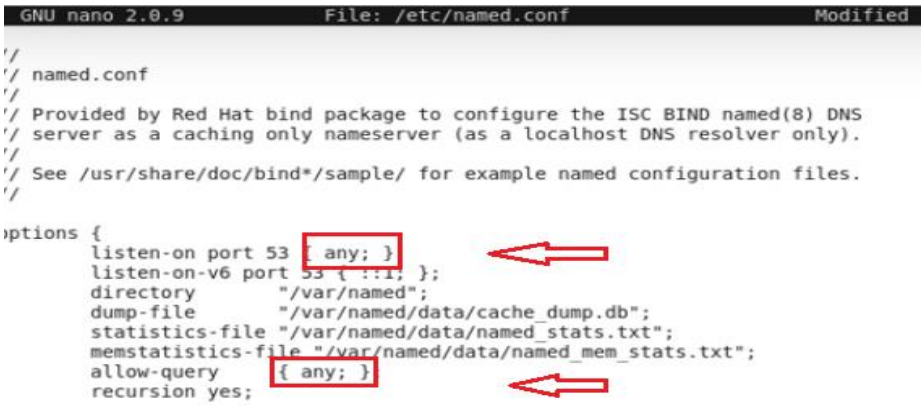

Figure 4. 22 : « Activation du service named »

Le fichier named.conf est une suite de déclarations utilisant des options insérées qui sont placées entre accolades. On doit être très prudent lorsqu'on modifie le fichier named.conf et particulièrement à ne pas faire de fautes de syntaxe car des erreurs mineures en apparence empêcheront le démarrage du service named.

- Lancement du répertoire named :
  On lance notre service avec la commande :
  #service named Start

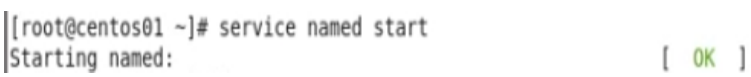

Figure 4. 23 : « Lancement du répertoire named »

- Création d'une zone dans le répertoire named.conf

Pour cela, on intègre le domaine qu'on souhaite crée dans ce répertoire

```
zone "linuxlab.local" IN {
type master;
file "linuxlab.local";
allow.update {none;};
```

Figure 4. 24 : « Création d'une zone dans le répertoire named.conf »

- Modification du répertoire qu'on vient de créer linuxlab.local dans le répertoire named
  Puis attribution de l'adresse du serveur DNS et de notre serveur de messagerie ainsi que le MX (Mail eXchanger)
  On accède avec la commande :

#nano /var/named/linuxlab.local

```
                    $TTL 1D@ IN SOA ns1.linuxlab.local.
                    hostmaster.linuxlab.local. (
                    0; serial
                    1D; refresh
                    1H; retry
                    1W; expire
                    3H); minimum

IN          NS                  ns1.linuxlab.local.
@           IN      MX    10    mail.linuxlab.local.
ns1         IN      A           192.168.1.100
mail        IN      A           192.168.1.100
```

Figure 4. 25 : « Modification du répertoire linuxlab.local. »

- Modification du fichier named ownership
  La modification se fait avec la commande :
  # chown root:named linuxlab.local

- Relancement du service named
  On relance avec la commande :
  #service named reload

- Tester si notre serveur DNS est opérationnel :
  Avec les commandes suites :

  dig @localhost ns1.linuxlab.local
  dig @localhost linuxlab.local MX
  dig @localhost linuxlab.local NS

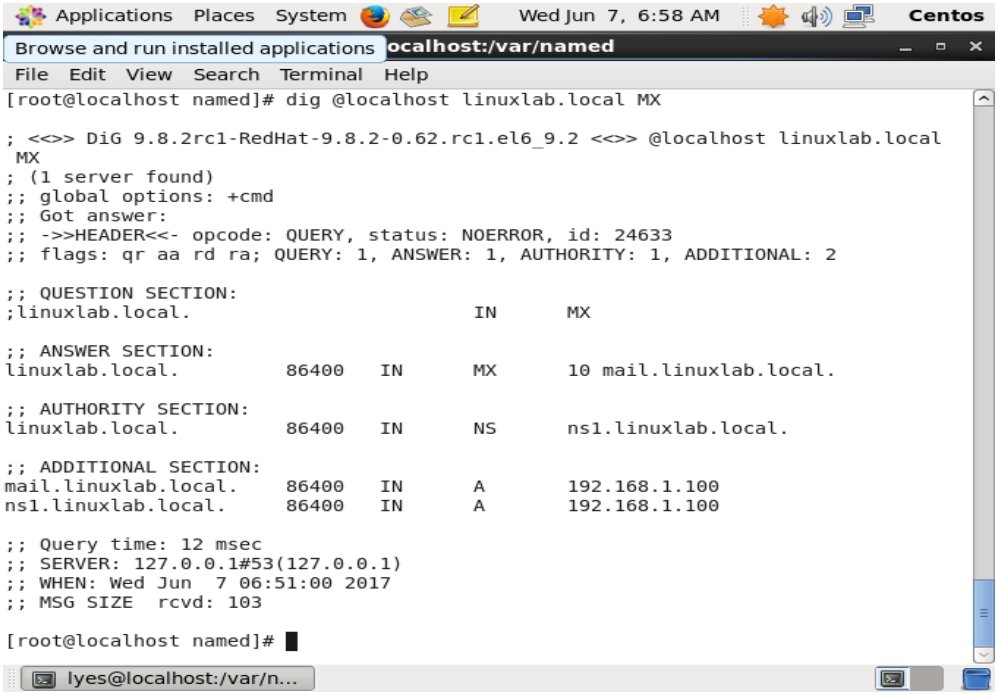

Figure 4. 26 : « serveur DNS opérationnel »

4.3.3 Installation et configuration de zimbra et ses modules

- Faire la mise à jour du système afin de procéder à l'installation du zimbra

On lance la commande :

#yum update

- Téléchargement des prérequis pour l'installation du zimbra

  On lance la suivant ligne de commande pour les télécharger

 # yum install sudo sysstat libidn gmp libtool-ltdl compat-glib vixie-cron nc perl libstdc++.i686

- **Téléchargement et décompression de l'archive et installation du zimbra**

Pour cela nous devons télécharger l'archive de zimbra la version compatible avec CentOS 6.9, puis décompresser l'archive de zimbra et pour finir lancer le script d'installation avec la commande **#./install.sh**

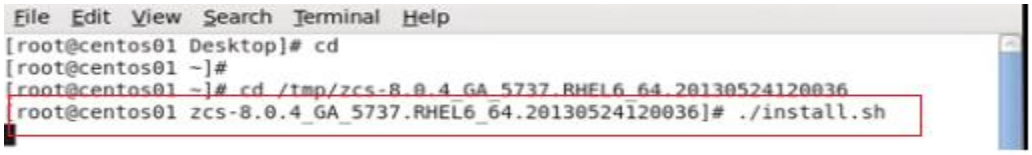

Figure 4. 27 : « lancement d'installation »

- configuration des modules du zimbra :

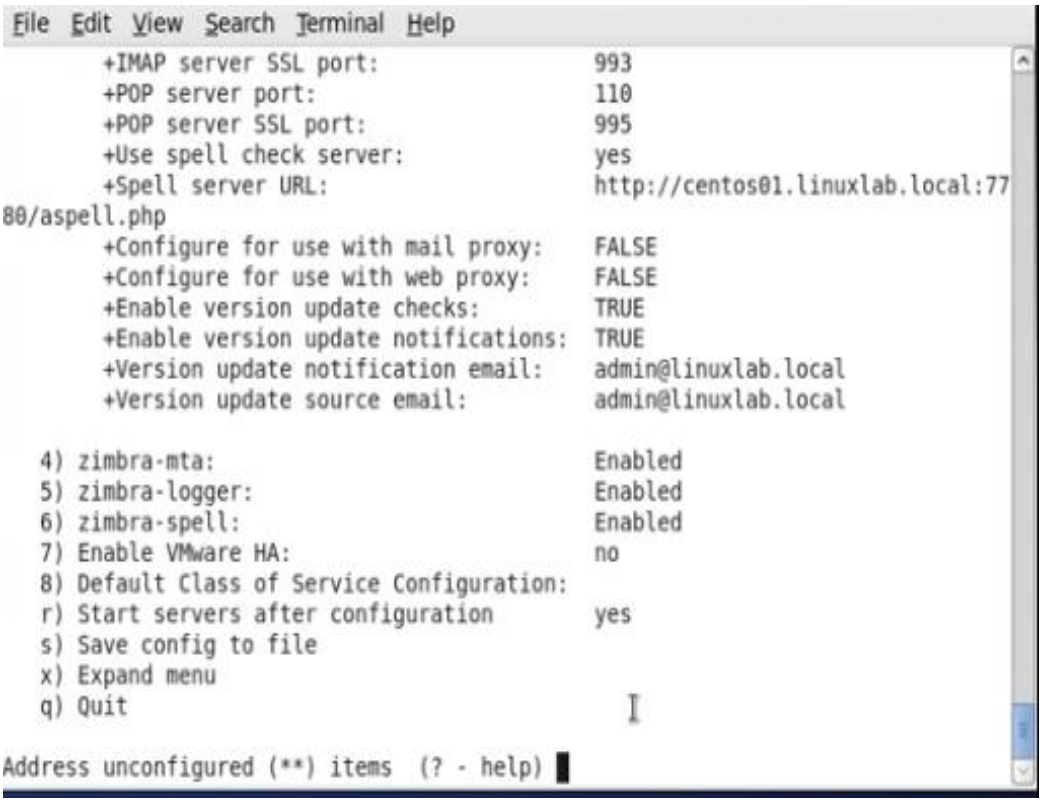

Figure 4. 28 : « configuration des modules du zimbra »

- Finaliser l'installation des modules du zimbra

Après avoir configuré et réglé tous les problèmes signalés, on aura le choix de si on compléter l'installation et cela en appuyant sur « a ».

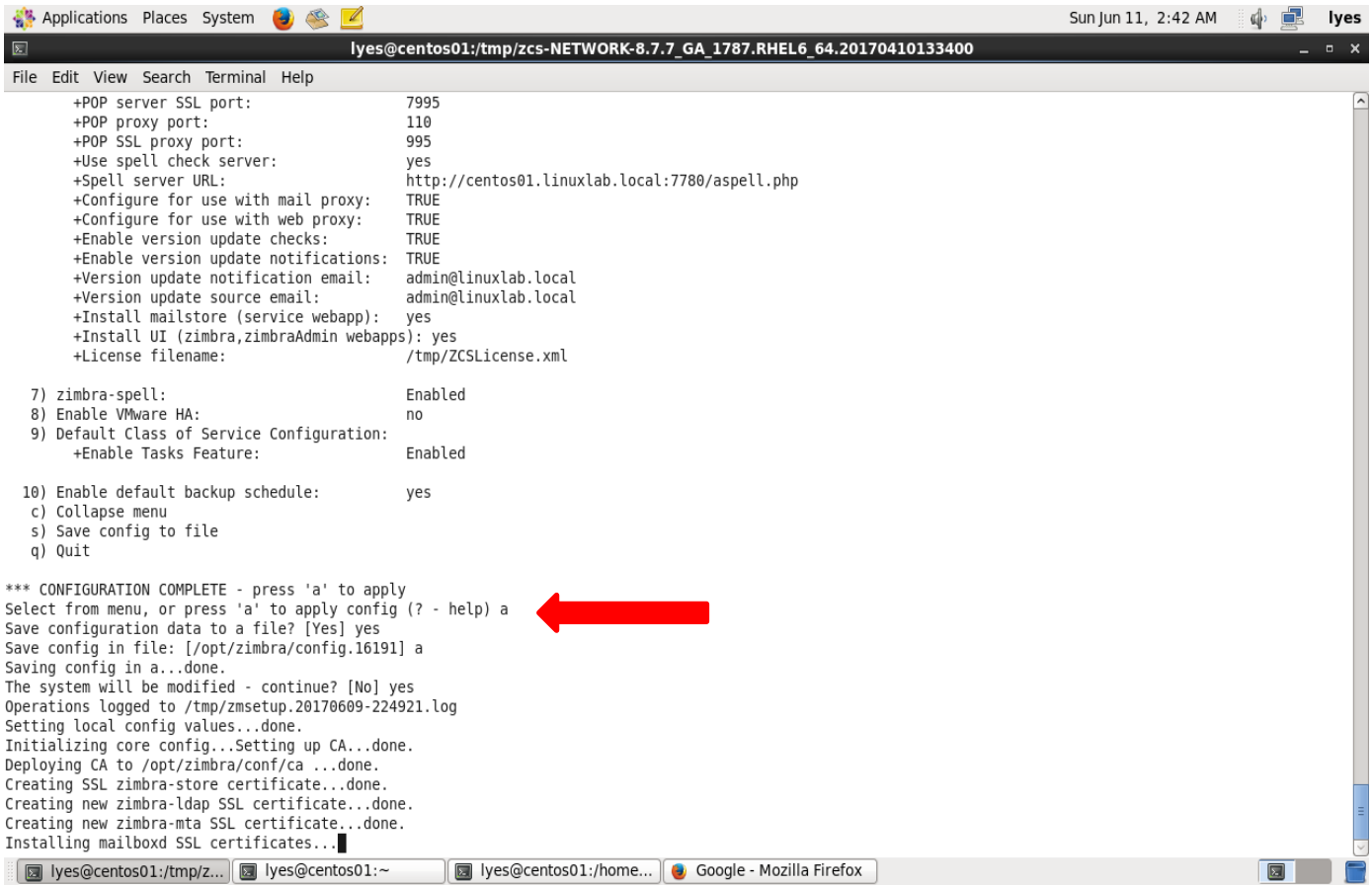

Figure 4. 29 : « achèvement de l'installation des modules du zimbra »

- Administration du serveur de messagerie :

apres que le serveur de messagerie zimbra est prêt, on pourra alors se rendre sur l'interface web administrateur avec le lien suivant en spécifiant les ports associé https://linuxlab.local:7071 Ou bien avec: https://192.168.1.100:7071
De même pour l'interface web d'utilisateur avec les liens suivants https://192.168.1.100:8443 ou bien avec https://linuxlab.local:8443

Et pour conclure l'interface web d'administrateur s'affichera (Figure 4.30).

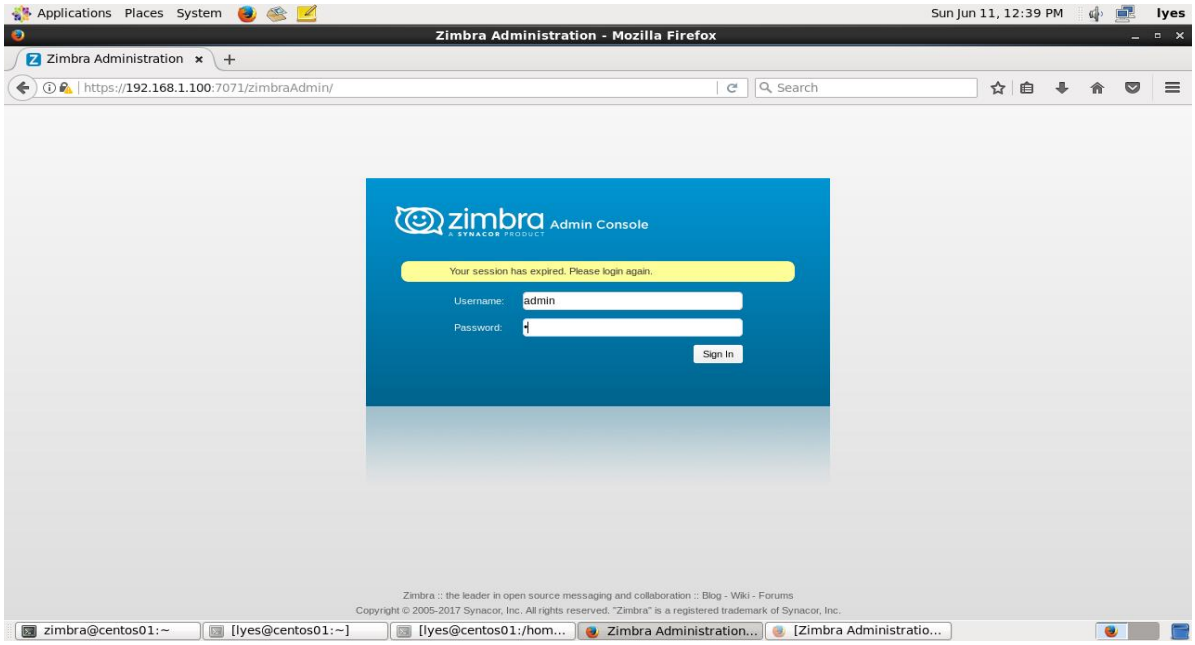

Figure 4. 30 : « Interface administrateur »

Après avoir saisi le nom d'utilisateur et le mot de passe l'interface administrateur se présente de cette façon (voir figure 4.31)

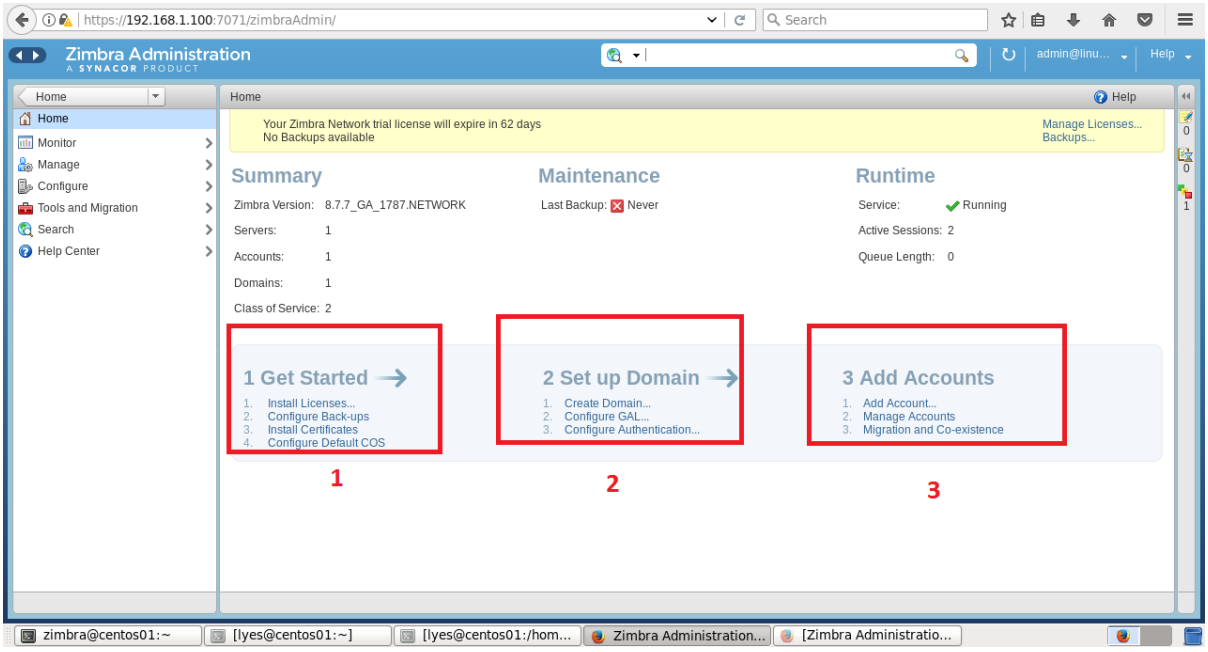

Figure 4. 31 : « l'Interface administrateur après la saisie du nom d'utilisateur et mot de passe »

L'administrateur peut faire quelques taches par exemple : pour ajouter un compte, il devra utiliser l'option 3 add accounts (ajouter un compte) puis remplir les différents champs et pour finir appuyer sur « terminer ».

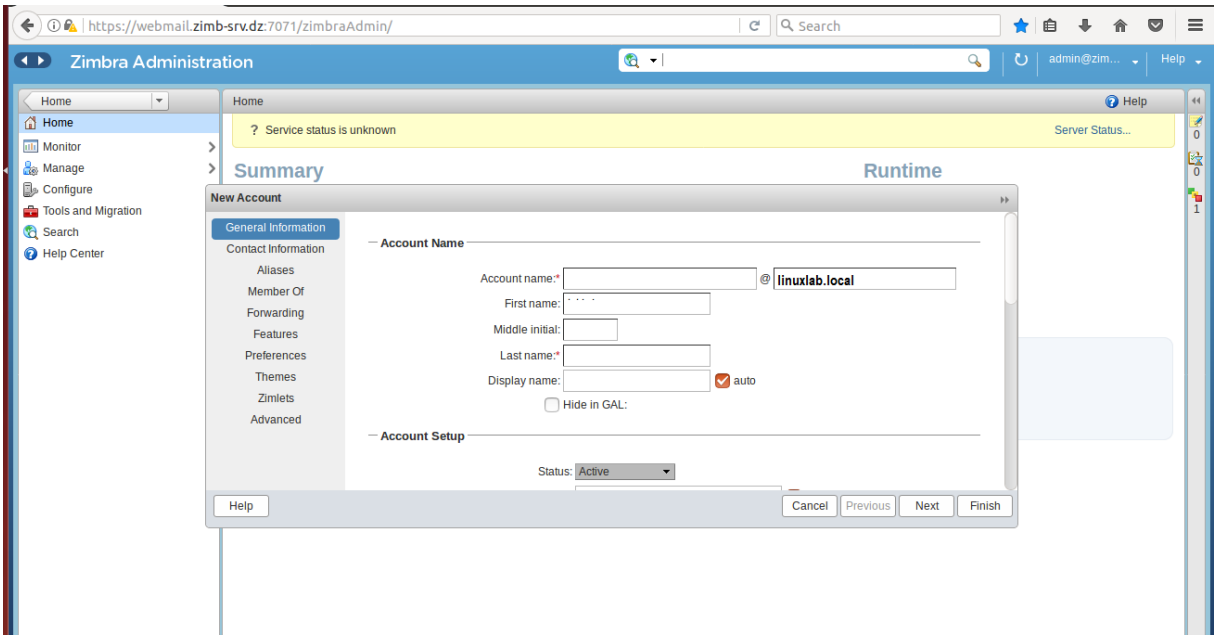

Figure 4. 32 : « ajouter un compte »

- visualiser la liste des comptes créer dans manage puis accounts

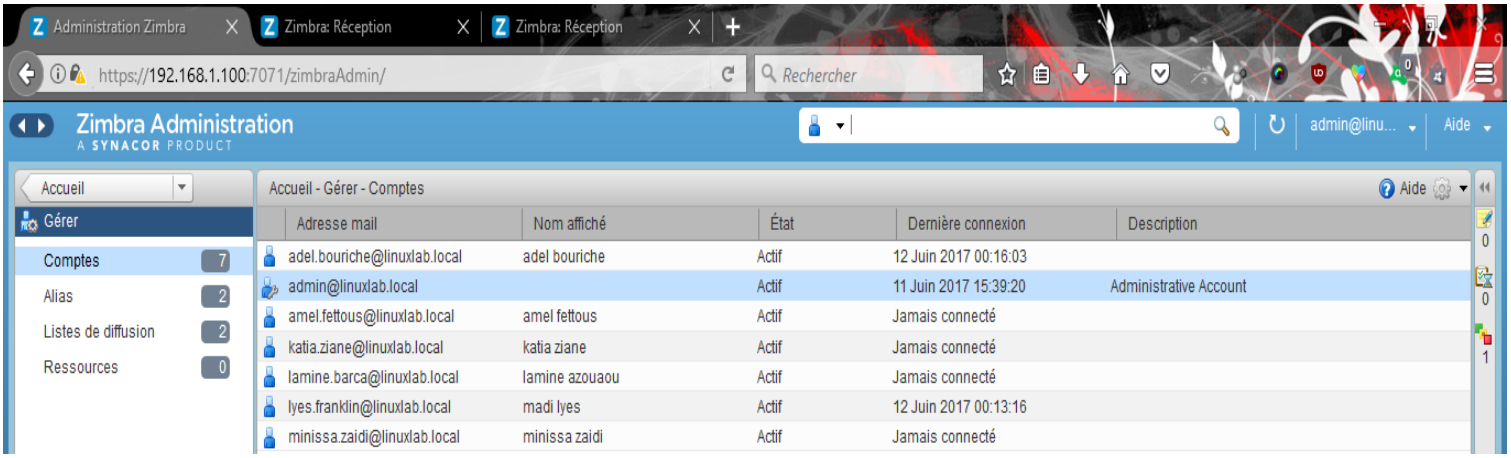

Figure 4. 33 - « la liste des comptes crée »

4.4 Conclusion

Pour finaliser notre projet, nous avons commencé par définir les différents outils utilisés pour la réalisation de nos solutions. Tels que le simulateur Cisco Packet tracer version 6, qui par la suite utilisé pour la configuration de notre architecture réseau, nous avons donc expliqué comment nous avons configuré les commutateurs (créations des VLANs, mots de passe, insertion des ACL, etc.) et, ensuite nous sommes passé à des tests de vérification. Autres point toujours pour la solution vlan et cela par la définition du PfSense qui est un logiciel open source possédant les fonctionnalités d'un pare-feu mais également d'un routeur comme définit auparavant dans le chapitre ainsi que la VMware qui tous deux contribuent à l'aboutissement de la création des VLANs .et pour finir après la définitions CentOS 6.9 qui est l'un **CentOS** l'une des distributions Linux les plus populaires pour les serveurs web Ainsi que Zimbra 8.7.7 notre choix comme serveur de messagerie avec des fonctionnalités de travail collaboratif dans le but de réaliser une messagerie électronique qui répond aux exigences souhaitée de l'entreprise EPB.

Conclusion générale

Nous avons essayé à travers ce mémoire d'apporter une solution pour organiser et sécuriser le réseau informatique de l'entreprise portuaire de Bejaia. Comme nous l'avons constaté, l'EPB est constituée de plusieurs directions à savoir la direction des ressources humaines DRH, ou bien direction du système d'information DSI,...etc.

C'est pour cela qu'on a opté pour des solutions basées en premier lieu sur les réseaux virtuels, en procédant à la segmentation logique du réseau local de l'entreprise. Puis, la messagerie électronique qui a son importance au niveau sécurité du partage de données entre les directions.

Dans notre projet, on retrouvera toutes les stratégies prévues pour compléter les lacunes qu'on a pu déceler au niveau de l'organisme des réseaux informatiques. Ainsi que les outils qui nous ont permis de mettre en œuvre nos solutions proposées.

Durant le présent projet de fin de cycle, il nous a été confié comme sujet principal d'étudier la hiérarchie de l'architecture réseaux de l'EPB afin d'optimiser ses ressources informatiques. Pour cela nous avons divisé notre travail en quatre chapitres :

Premièrement, on a commencé par mettre en avant les premiers concepts des réseaux informatiques, une diagnostique des besoins de sécurité et les importantes étapes qui précèdent la mise en place des stratégies de sécurité dans un réseau d'entreprise.

Ensuite, l'étude de l'existant nous a permis de bien comprendre la gestion des réseaux informatiques actuels de l'Entreprise Portuaire de Bejaïa, ce qui nous a aidés à retirer certaines lacunes des réseaux de cette entreprise.

Puis, nous l'avons poursuivi en proposant des stratégies qui pourraient éventuellement compléter l'organisme architectural des réseaux, et cela en apportant quelques améliorations telles que les VLANs et un serveur de messagerie.

Enfin, notre travail s'est achevé en réalisant et en mettant en œuvre nos solutions proposées qui visent l'organisation et la sécurité des informations véhiculées dans les réseaux au sein de l'EPB

Bibliographie

[1] P.Guy. Initiation-aux-réseaux, Eyrolles 8éme édition, 2014

[2] COUR CISCO CCNA1, chapitre 1 fourniture de ressources dans un réseau. Netacad,2017.

[3] F. Jacquenod. Cours Réseaux No5, les matériels d'interconnections. http://www.netalya.com/fr/reseaux5.asp. (Consulter le 08 mai 2017)

[4] COUR CISCO CCNA1, chapitre 3 Médias réseau. netacad, 2017.

[5] Mme Claire, "service AAA dans les réseaux ad hoc mobiles", Thèse de doctorat, université.Télécom.Paris,sud,2012 .

[6] J.F Pillou. Tout sur les réseaux et Internet, DUNOD 2006

[7] les types d'attaques informatique.Direction de recherche ingénierie de formation

[8] EVENGELISTA Thierry. les IDS (intrusion detection system). dunod, 2004

[9] https://blogs.business.microsoft.com/fr-fr/ (consulter 30 mars 2017)

[10] V. REMAZEILLES, COURS CISCO

[11] COLLEGE Lionel-Groulx. Publication, politique de sécurité informatique, Page 5

[12] G. Desgeorge.La sécurité des réseaux,Disponiblehttp//www.guill.net/.2000.

[13] J.F. carpentier ,Securite informatique, edition 2 anneé 2012

[14] Documents interne de l'EPB

[15] COUR CISCO CCNA2, chapitre 3. VLAN. netacad, 2017.

[16] http : //www-igm.univ-mlv.fr type de vlan Dernier accès juin 2017.

[17] http://cisco.goffinet.org Spanning-tree Dernier accès juin 2017.

[18] J.F. Pillou,jean-philippe RAY . Tout sur la sécurité informatique [TSI]

[19] https://www.osnet.eu/fr/content/tutoriels/d%C3%A9tail-des-fonctionnalit%C3%A9s-de-pfsense

[20] http: //hostedzimbra.itsintegra.com/presentation/pourquoi-choisir-zimbra(Consulter le 02 juin 2017)

[21] http: //www.linuxpedia.fr/doku.php/rpm/centos (Consulter le 15 juin 2017)

[22] Sébastien NEON, ZIMBRA messagerie collaborative d'entreprise, eni 2009

[25] http://www.i3s.unice.fr/~map/Cours/LPSILADMIN/UtilisationPacketTracer.pdf

[26] https://www.vmware.com/fr/products/workstation.html(Consulter le 08 avril 2017)

[29] http://deptinfo.cnam.fr/Enseignement/CycleProbatoire/RSX102/cours_messagerie.pdf

[30] notion de bases : lexiques détaillés est illustré, consulté en mai 2017

[31] http://www.acipia.fr/infrastructure/systeme/etude-comparative-de-messageries-collaboratives-open-source/ (Consulter le 01 juin 2017)

[33] N. Jean Comprendre et programmer les protocoles POP et IMAP Linux magazine France Janvier 2003, n°46

[32] N. Jean Comprendre et programmer le protocole SMTP Linux magazine France Decembre 2002, n°45

[33] http://hostedzimbra.itsintegra.com/presentation/pourquoi-choisir-zimbra

[34] R. SANCHEZ, Les reseaux locaux virtuels (VLAN), certa janvier 2006-v1.0.

Résumé

Ce mémoire fait l'objet de stage de fin d'étude au sein de l'entreprise portuaire de Bejaia (EPB)où nous avons pu réaliser notre projet qui a consisté à étudier l'infrastructure réseaux de cette dernière, et ce dans le but de proposer des améliorations et remédier aux éventuelles lacunes qu'on a pu constater. A cet effet , nous avons proposé des solutions qui vont changer les performances du réseau en matière de sécurité et de gestion , de fluidité et de souplesse tout en gardant la continuité du réseaux et en assurant la disponibilité des ressources matériels et logiciels. Dans un premier temps nous avons décrit les généralités sur les réseaux et la sécurité, puis on a présenté l'organisme d'accueil. Ensuite, nous avons proposé de nouvelles améliorations au réseau de l'entreprise tout en étudiant les solutions adéquates. Et enfin nous avons mis en œuvre ces dernières.

Mots clé : réseaux informatique d'entreprises, architecture réseaux, VLAN, Pfsense, serveurs de messagerie, ZIMBRA, CentOS.

Abstract

This following dissertation is realized to summarize our Final Year Internship done at Béjaïa Port Company i.e. EPB (**E**nterprise **P**ortuaire de **B**ejaïa). It consist of the study of network infrastructure of this company and some improvements proposed for the lacks seen that in order to improve the performances of the Network in terms of security, management, fluidity and flexibility maintaining the continuity of the Network and ensuring the disponibility of both hardware then software materials. We start, by some generalities on networks and security. In addition we represent the home organization. Next, we propose new improvements for company's network while studying the solutions. Finally, we go through implementation to realize our conception.

Keywords: Computer networks of companies, networks security, VLAN, PfSense, mail server, ZIMBRA, CentOS.