République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A.MIRA de Bejaia

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Faculté des Sciences Exactes

Département d'Informatique

MÉMOIRE DE FIN DE CYCLE

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

Spécialité : Administration et Sécurité des Réseaux Informatiques

---

Thème

Étude et simulation des VLANs et d'un pare-feu (Pfsense) cas Entreprise Portuaire Béjaia (EPB)

Travail réalisé par ATMANI Walid **et** AIT ATMANE Faouzi

Encadré par Dr. BRAHAMI Houda née ELBOUHISSI

Devant le jury composé de :

Président : DJEBARI N.

Examinateur : SABRI S.

Examinateur : KADJOUH N.

Promotion 2016 / 2017

Remerciements

Nous remercions Dieu, le tout puissant pour nous avoir donné la foi qui nous a guidé jusqu'à la réalisation et l'aboutissement de ce mémoire.

Nos vifs remerciements vont d'emblées à nos chers parents pour tous les sacrifices consentis à notre égard et leur énorme soutien.

Nous tenons à exprimer nos profondes gratitudes et nos sincères remerciements, aussi bien pour notre promotrice Mme Brahami Houda qui nous a encadrés et guidés tout au long de ce projet.

Nous tenons à remercier vivement les membres de jury, et à exprimer toute notre reconnaissance pour l'honneur qu'ils nous accordent en acceptant d'évaluer ce modeste travail.

Nous remercions aussi, toutes les personnes qui nous ont aidé ou encouragé, de près ou de loin, durant nos études (ma famille, et touts mes ami(es)).

Dédicaces

Nous dédions ce modeste
travail à nos parents pour
leur soutien et leur présence
a nos cotés et leurs encouragements,
A toutes nos familles et
A tous nos amis(es).

ATMANI Walid
AIT ATMANE Faouzi

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABRÉVIATIONS

DNS : Domain Name Service

SNMP : Simple Network Management Protocol

FTP : File Transfer Protocol

TELNET: TELetype NETwork

HTTP: HyperText Transfer Protocol

SMTP: Simple Mail Transfer Protocol

TCP: Transmission control Protocol

IP: Internet Protocol

UDP: User Data Protocol

ARP/RARP: Address Resolution Protocol /Reverse ARP

ICMP: Internet Control Message Protocol

HDLC: High Level Data Link Control

PPP : Point to Point Protocol

WIMAX: Worldwide Interoperability for Microwave Access

VLAN: Virtual Local Area Network

VTP: Virtual Trunking Protocol

WAN : Wide Area Network

EPB : Enterprise Portuaire Béjaia

DC : Direction Capitainerie.

DDD : Direction Domaine et du Développement.

DFC : Direction des Finance et comptabilité.

DL : Direction de la Logistique.

DMA : Direction Manutention et Acconage.

ISO : International Organization for Standardization

Introduction générale

Durant ces dernières années, l'évolution technologique a permis d'améliorer la capacité et les fonctionnalités des ressources des réseaux.

Bien que la croissance d'une entreprise soit généralement souhaitée, elle génère un certain nombre de contraintes supplémentaires pouvant réduire les performances d'un réseau : augmentation rapide du nombre des utilisateurs et des clients, volume accru du trafic généré par chaque client, applications toujours plus complexes et fichiers plus volumineux. Tous ces facteurs peuvent contribuer à l'augmentation du trafic d'un réseau et, par conséquent, à en altérer les performances.

La performance d'un système d'information d'une entreprise est d'une importance capitale pour son efficacité et son bon fonctionnement. La recherche de cette performance entraine de plus en plus l'utilisation d'un système informatique pour la gestion quotidienne des informations. C'est dans cette optique que nous avons été accueillis à l'entreprise portuaire de Béjaia (EPB) pour étudier et mettre en place un réseau informatique sécurisé.

La sécurité se place actuellement au premier plan de la mise en œuvre et de l'administration réseau. La difficulté que représente la sécurité dans son ensemble, est de pouvoir trouver un compromis entre deux besoins essentiels : le besoin d'ouverture de réseaux afin de profiter des différentes fonctionnalités offertes et le besoin de protection des informations.

L'application d'une stratégie de sécurité efficace est l'étape la plus importante qu'une entreprise doit franchir pour protéger son réseau. Les outils classiques offrent des solutions de sécurité minimales (authentification par login et mot de passe, installation d'un anti-virus, etc.) se révèlent utiles mais dans la plupart des cas, insuffisantes.

Aucune personne n'ignore l'importance de l'information dans une institution qui nécessite l'organisation, la fiabilité et le bon fonctionnement du système d'information.

Les technologies de l'information et de la communication (TIC) nous introduisent dans un siècle de vitesse en nous offrant de nouvelles perspectives en ce qui concerne la communication de l'information au sein de nos organisations.

Voilà quelques questions que nous avons retenu et qui traduisent et reflètent nos préoccupations:

1. Comment segmenter un réseau en domaines de diffusion restreints pour en simplifier la gestion et ainsi augmenter considérablement la performance tout en renforçant la sécurité ?

2. Commet mettre en place une solution de filtrage afin de limiter l'accès aux utilisateurs et contrôler les accès entrant et sortant

Nous essayons dans la mesure du possible d'envisager une politique optimale de partage des informations afin que l'échange des ressources ne pose plus de problème au sein de l'entreprise.

Dans le cadre de notre travail, nous avons jugé bon de joindre au système d'information existant au sein de l'entreprise des dispositifs VLANs et pare-feu(pfsense).

En vue de remédier toujours aux inquiétudes soulevées au travers des questions posées dessus, nous pensons : Qu'il existe un moyen d'échange de l'information qui serait adapté à la gestion efficace, simplifiée et sécurisée :

- Le VLAN permettra de segmenter et de séparer le réseau en domaines de diffusions.
- PfSense offre une solution complète de routage, filtrage et de contrôle les accès entrant et sortant et protéger l'environnement (vis à vis de l'extérieur et de l'intérieur).

Qu'une configuration appropriée existe et les logiciels Pack Tracer et GNS3 serait les mieux adapté pour cela.

Après l'introduction générale, le premier chapitre nous allons présenter l'organisme d'accueil et l'étude effectuée durant notre stage au sein de ce dernier

Dans le second chapitre, nous allons présenter les généralités sur les réseaux informatiques

Dans le troisième chapitre, nous allons présenter la sécurité des réseaux informatiques

Le quatrième chapitre décrit la partie pratique de notre travail, dans lequel nous allons présenter l'environnement de travail ainsi que le cas d'étude qui consiste à faire une simulation d'une segmentation, filtrage et de contrôle les accès entrant et sortant et protéger l'environnement**,** et définir les différentes configurations réalisées.

Enfin, nous terminerons ce mémoire par une conclusion et nous allons présenter les perspectives de ce travail.

CHAPITRE 1

Présentation générale de l'organisme d'accueil

1.1 Introduction

Ce chapitre sera réservé à l'étude du réseau existant dans l'EPB et aux améliorations proposées, d'abord nous allons évoquer un bref aperçu de l'entreprise pour mieux connaitre sa structure et ses objectifs. Ensuite, nous allons étudier le réseau et ses composants pour pouvoir proposer d'éventuelles améliorations.

1.2 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 1er port d'Algérie en marchandises générales et 3ème port pétrolier. Il est également le 1er port du bassin méditerranéen certifié ISO 9001 :2000 pour l'ensemble de ses prestations, et avoir ainsi installé un système de management de la qualité.

Cela constitue une étape dans le processus d'amélioration continue de ses prestations au grand bénéfice de ses clients. L'Entreprise Portuaire a connu d'autres succès depuis, elle est notamment certifiée à la Norme ISO 14001 :2004 et au référentiel OHSAS 18001 :2007, respectivement pour l'environnement et l'hygiène et sécurité au travail [1].

1.2.1 Historique

Au cœur de l'espace méditerranéen, la ville de Bejaia possède de nombreux sites naturels et vestiges historiques datant de plus de 10 000 ans, ainsi que de nombreux sites archéologiques recelant des objets d'origine remontant à l'époque néolithique.
Bejaia joua un grand rôle dans la transmission du savoir dans le bassin méditerranéen, grâce au dynamisme de son port, la sécurité de la région, la bonne politique et les avantages douaniers. Bougie a su attirer beaucoup de puissants marchands.

La Saldae romaine devient un port d'embarquement de blé du grenier de Rome, ce n'est qu'aux XIéme siècle, que Bgaieth, devenue Ennaceria, pris une place très importante dans le monde de l'époque, le port de Bejaia devient l'un des plus importants de la méditerranée.

La réalisation des ouvrages actuels débuta en 1834, elle fut achevée en 1987. C'est en 1960 qu'a été chargé le premier pétrolier d'Algérie.

1.2.2 Création de l'EPB

Le décret n°82-285 du 14 Août 1982 publié dans le journal officiel n° 33 porta création de l'Entreprise Portuaire de Bejaia **;** entreprise socialiste à caractère économique **;** conformément aux principes de la charte de l'organisation des entreprises, aux dispositions de l'ordonnance n° 71-74 du 16 Novembre 1971 relative à la gestion socialiste des entreprises et les textes pris pour son application à l'endroit des ports maritimes**.**

L'entreprise, réputée commerçante dans ses relations avec les tiers, fut régie par la législation en vigueur et soumise aux règles édictées par le susmentionné décret.

Pour accomplir ses missions, l'entreprise est substituée à l'Office National des Ports (ONP), à la Société Nationale de Manutention (SO.NA.MA) et pour partie à la Compagnie Nationale Algérienne de Navigation (CNAN).

Elle fut dotée par l'Etat, du patrimoine, des activités, des structures et des moyens détenus par l'ONP, la SO.NA.MA et de l'activité Remorquage, précédemment dévolue à la CNAN, ainsi que des personnels liés à la gestion et au fonctionnement de celles-ci.

En exécution des lois n° 88.01, 88.03 et 88.04 du 02 Janvier 1988 s'inscrivant dans le cadre des réformes économiques et portant sur l'autonomie des entreprises, et suivant les prescriptions des décrets n°88.101 du 16 Mai 1988, n°88.199 du 21 Juin 1988 et n°88.177 du 28 Septembre 1988.

L'Entreprise Portuaire de Bejaia ; entreprise socialiste ; est transformée en Entreprise Publique Economique, Société par Actions (EPE-SPA) depuis le 15 Février 1989, son capital social fut fixé à Dix millions (10.000.000) de dinars algériens par décision du conseil de la planification n°191/SP/DP du 09 Novembre 1988. Actuellement, le capital social de l'entreprise a été ramené à 1.700.000.000 Da, détenues à 100% par la Société de Gestion des Participations de l'Etat « Ports », par abréviation « SOGEPORTS ».

1.2.3 Missions et Activités de l'EPB

1.2.3.1 Ses Missions

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

1.2.3.2 Ses Activités

Les principales activités de l'entreprise sont :

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

1.2.4 Présentation des différentes structures de l'entreprise

Organigramme :

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 à la gestion et au développement de l'entreprise (voir figure 1.1).

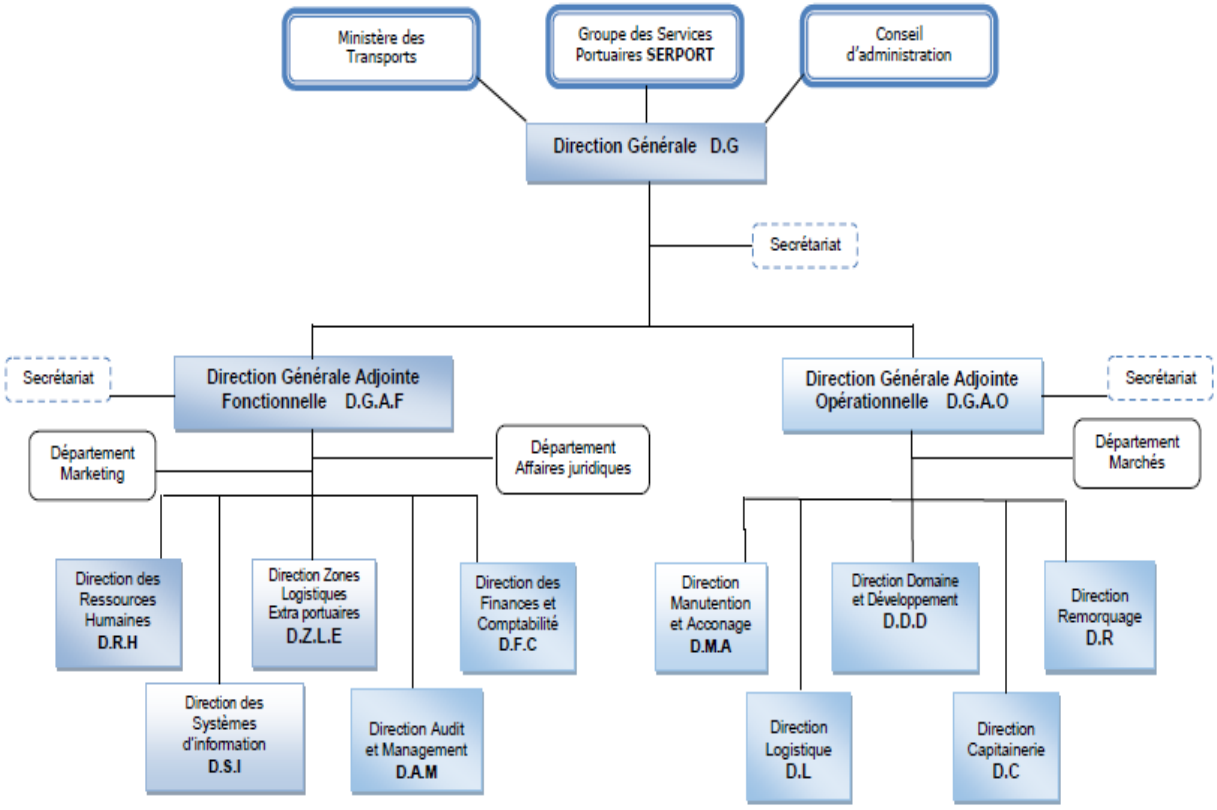


Figure 1.1 : Organigramme général de l'EPB

1.3 Présentation de la direction des systèmes d'information

Elle a pour mission :

La réalisation du schéma directeur par la conduite des projets d'informatisation en veillant à la cohérence fonctionnelle et technique ainsi qu'à la qualité et la sécurité des systèmes d'information [2].

- La mise en œuvre des systèmes d'information à la fois flexibles et fiables ;
- Le management des évolutions des systèmes d'information et des projets informatiques ;

- L'excellence opérationnelle et l'optimisation des fonctions de soutien de la DSI.

1.3.1 Organisation humaine de la direction des systèmes d'information

La figure 1.2 représente l'organisation humaine du la direction des systèmes d'information

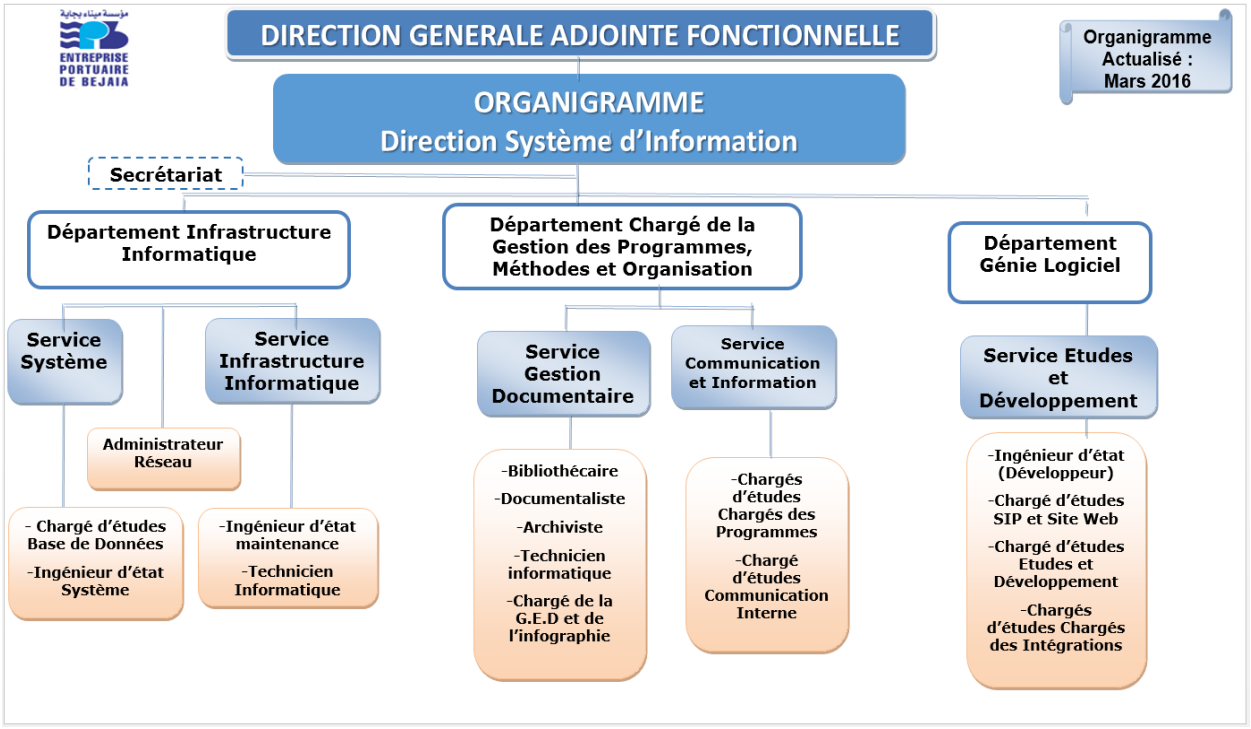


Figure 1.2: l'organigramme de la structure informatique

1.4 L'infrastructure informatique

1.4.1 Le réseau informatique de l'EPB

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 1.3). 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.

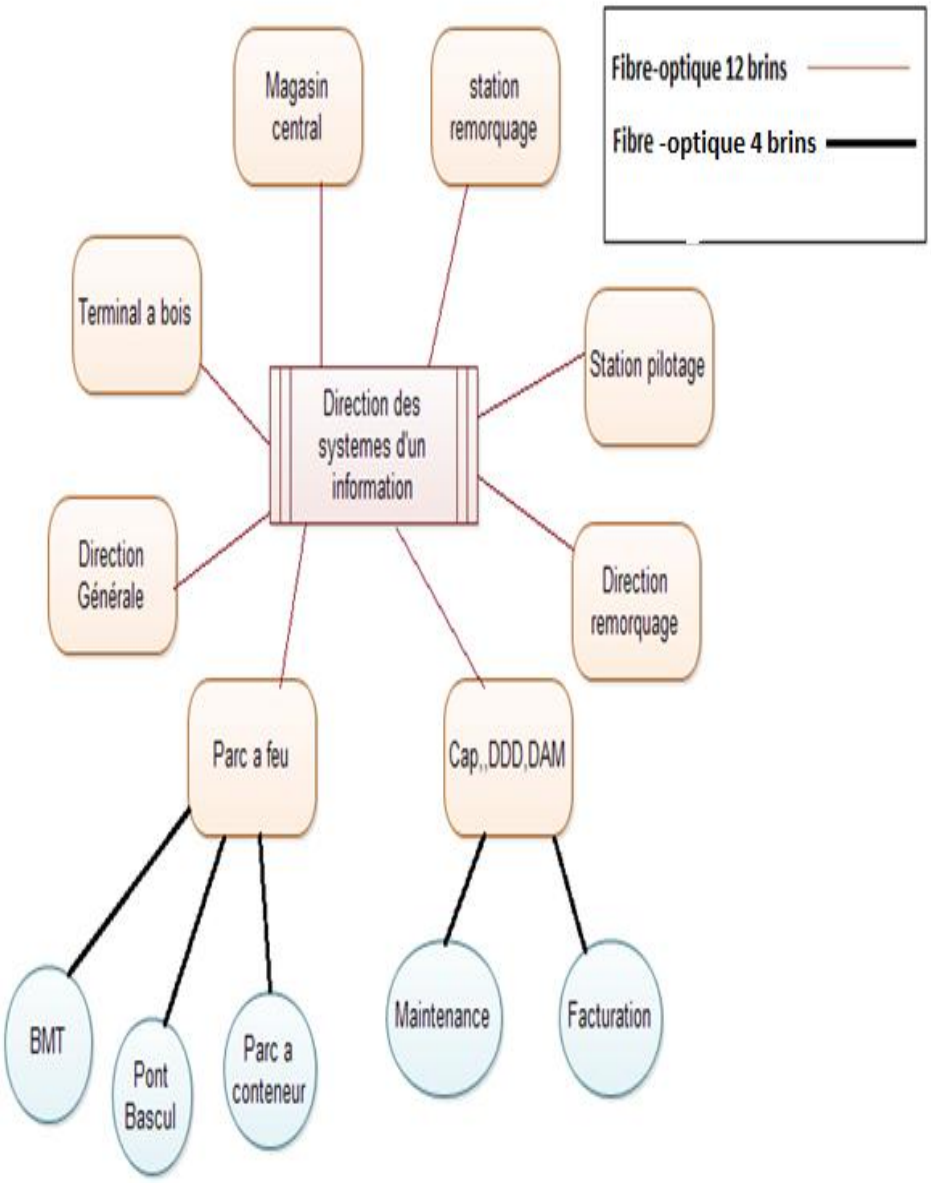


Figure 1.3: réseau fibre optique de l'EPB

1.4.2 Présentation de l'architecture de l'EPB

Dans cette partie nous allons décrire les différents composants de l'architecture de l'EPB (figure 1.4).

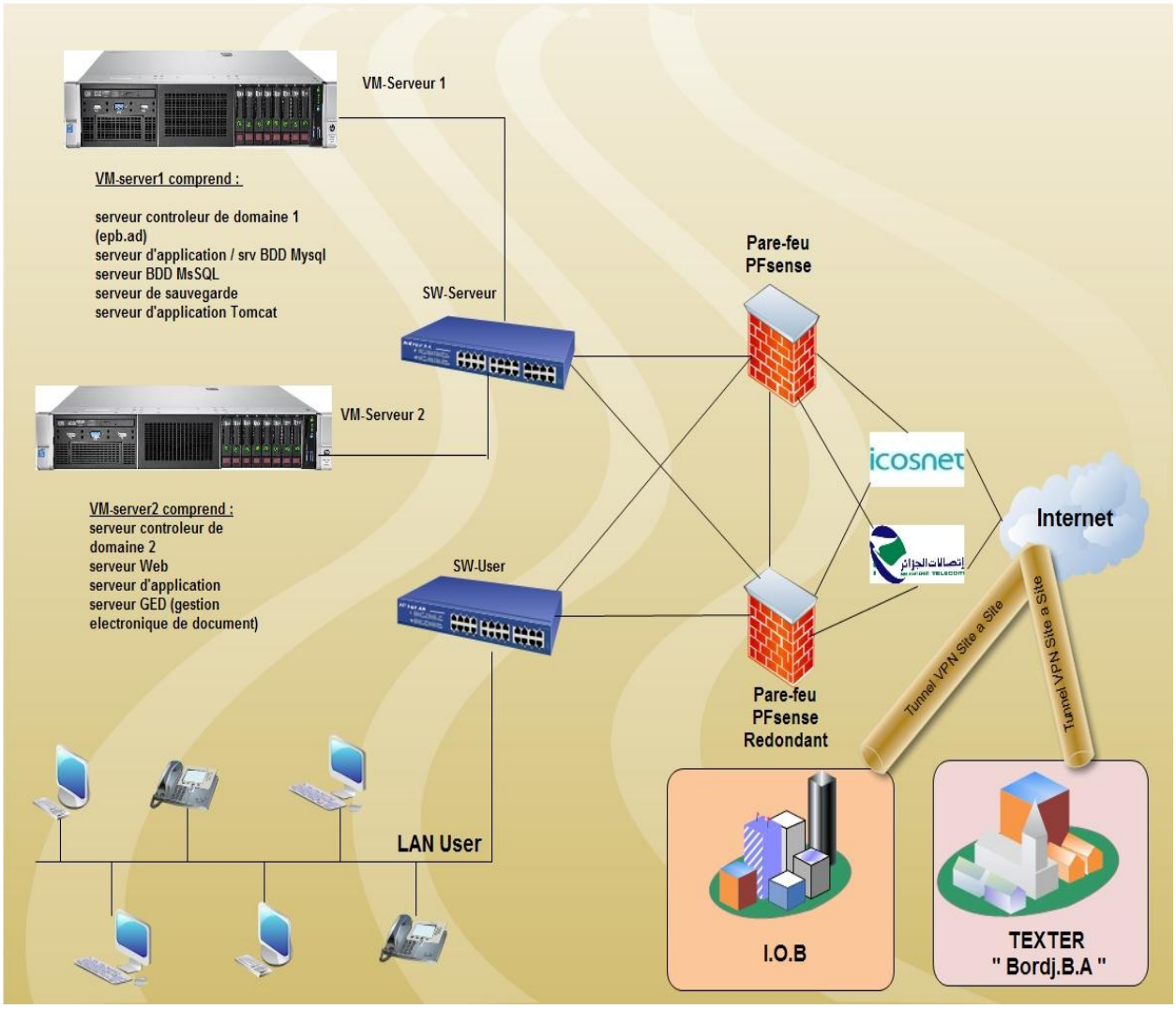


Figure 1.4: Architecture réseau de l'EPB (ancienne version)

1.4.2.1 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 hertziennes 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 :**

  La sécurité est assurée par un pare-feu pour appliquer les stratégies d'accès et les règles de routages déterminant la manière dont les clients accèdent à Internet.

- **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 Switches elle comporte les différentes machines serveurs :

- ✓ **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 bases 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 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 application/fichier :**

C'est un serveur sur lequel sont installées les applications utilisées par les usagers, 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.

1.4.2.2 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.

- **Absence de serveurs en redondances pour assurer la tolérance aux pannes :**

- ✓ Pour assurer la disponibilité et la continuité des données et des ressources dans une entreprise un serveur en redondance est important.
- ✓ Le serveur en redondance prend en charge tous les services défectueux du premier serveur.

- **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 lourd, 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 VLAN.
✓ Changements et configuration des switch au niveau des armoires pour mettre à niveau le réseau VLAN de l'entreprise.

1.4.2.3 Les objectifs de la direction des systèmes d'information

Afin d'assurer les besoins de l'entreprise il est nécessaire d'améliorer les performances du réseau, et pour cela il faudra passer en revue tous les aspects intervenant dans ce système, notamment :

1. Amélioration de la sécurité, de la disponibilité et des performances réseau.
2. Amélioration du câblage interne.
3. Amélioration du plan d'adressage IP.
4. Mise à niveau des systèmes d'exploitation.
5. Amélioration de la qualité du matériel (serveurs, commutateurs et hôtes).
6. Maitrise de l'impact des trafics générés par les serveurs d'authentification - des médias d'interconnexion.

Notre travail consiste à mettre en œuvre d'autres améliorations à cette architecture pour un meilleur fonctionnement et pour assurer la continuité de quelques services.

1.5 Cahier des charges

La DSI de l'EPB lance le projet de réorganisation de son réseau afin de répondre aux exigences d'une meilleure performance et répondre aux objectifs fixés par la direction générale.

Au fur et à mesure du développement de la structure, les applications gagnent en complexité, les débits ne sont pas détaillés par importance de groupe de travail, les utilisateurs et les ressources entre lesquels les communications sont fréquentes ne sont pas regroupés tous ces phénomènes entrainent la dégradation du réseau. La segmentation devient alors nécessaire afin d'améliorer la réactivité, le débit et la souplesse du réseau.

Description :

a. Objectifs :
- Mettre en place une solution d'optimisation de la bande passante du réseau par la segmentation des domaines de broadcast d'EPB.
- Mettre en place une solution de filtrage afin de limiter l'accès aux utilisateurs et contrôler les accès entrant et sortant.

b. Solution :
- La solution VLAN est la première étape du processus d'amélioration des performances du réseau contre les surcharges rencontrées par les utilisateurs d'EPB.
- pfSense offre une solution complète de routage , filtrage et de contrôle les accès entrant et sortant et protéger l'environnement (vis à vis de l'extérieur et de l'intérieur).

c. Procédure :

- Illustrer le support des Vlan 802.1Q par pfSense et mettre en relief les principales étapes de configuration :
  - Mise en place des Vlans sur l'interface LAN de pfSense
  - Configuration des VLANs au niveau des switchs
  - Configuration d'un serveur DHCP pour chaque Vlan avec une plage d'adresse différente.

1.5.1 Architecture proposée pour le réseau de l'EPB

Nous pouvons regrouper les améliorations proposées dans l'architecture suivante (voir figure 1.5).

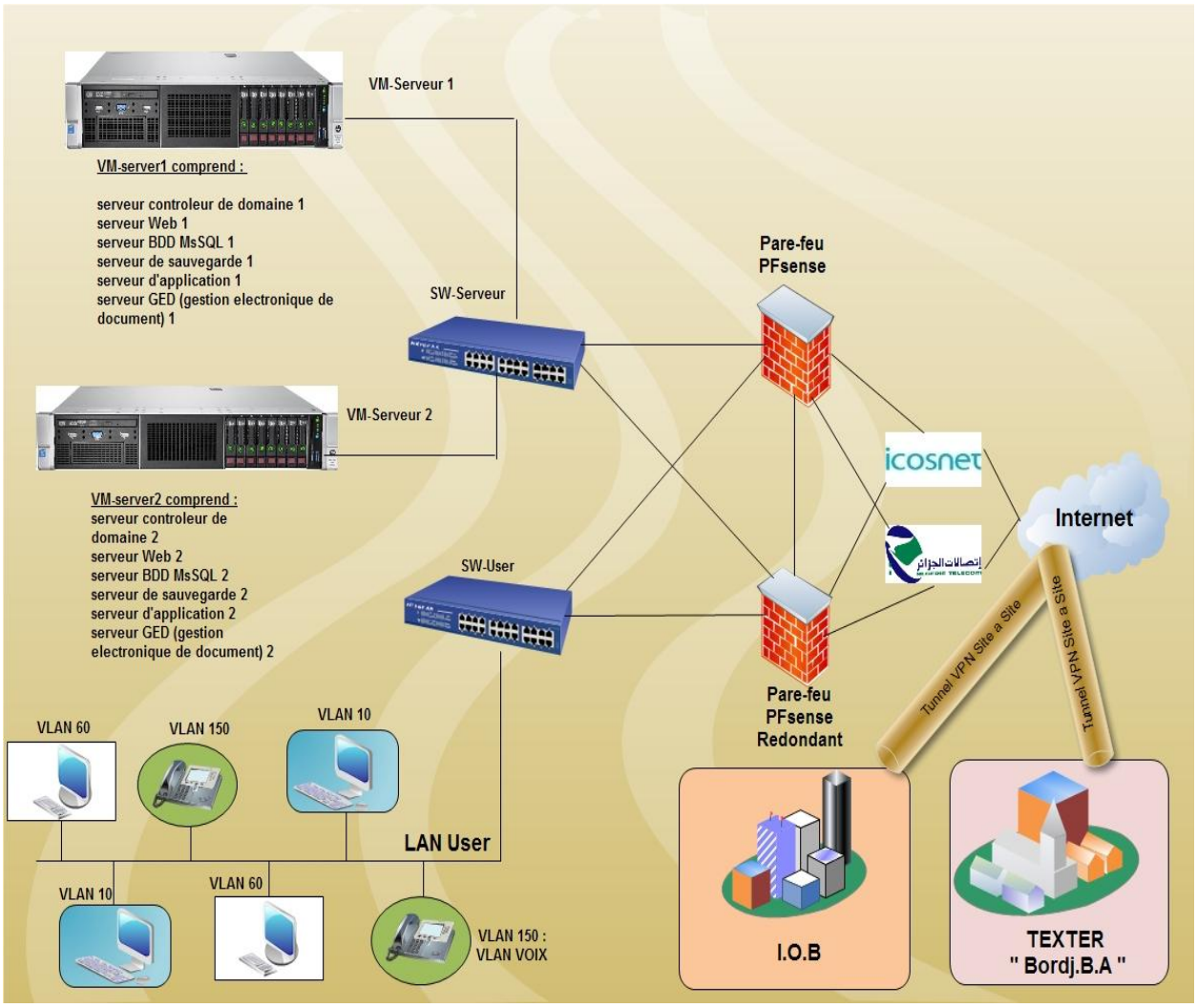


Figure 1.5: architecture proposée pour le réseau de l'EPB

1.6 Conclusion

Ce chapitre a donné un bref aperçu de l'entreprise, nos missions et le projet en question, l'étude de l'existant nous a permis de se familiariser avec le réseau actuel de l'EPB, et de comprendre l'utilité de chaque détail profondément, et c'est ce qui nous a permis de voir les lacunes et les faiblesses du réseau. l'étude de ces lacunes nous a conduits à proposer une solution pour palier à ses dernières.

Après avoir choisi la solution à adopter nous avons tracé nos objectifs ensuite nous avons défini un plan de travail pour mettre en œuvre cette solution.

Le chapitre suivant présente un background sur les réseaux informatiques car ils représentent le noyau de notre application.

CHAPITRE 2

Généralités sur les réseaux informatiques

2.1 Introduction

Ce chapitre a pour objectif de présenter des notions de base sur les réseaux informatiques, on entend par réseau, un ensemble interconnecté, se constituer d'un nombre d'entités et de leurs interrelations. Il permet la circulation d'un flux d'éléments matériels ou immatériels, entre-les différentes entités selon des règles bien définies.

2.2 Les réseaux informatiques des entreprises

2.2.1 Définition d'un Réseau

Le Réseau informatique est un ensemble d'ordinateurs et de périphériques reliés entre eux par des canaux électroniques de communications (filaire ou sans fil), qui leur permettent d'échanger des informations [3].

2.2.2 Les principaux composants matériels d'un réseau informatique :

2.2.2.1 Equipements d'interconnexion

- **La carte réseau :**

  Elle constitue l'interface entre l'ordinateur et le câble du réseau. Elle est employée pour faire communiquer un ordinateur avec d'autres éléments [4].

Figure 2.1 : carte réseau

- **Le concentrateur :**

  Le concentrateur (appelé Hub en anglais) est un élément matériel qui permet de relier plusieurs ordinateurs entre eux. Son rôle c'est de prendre les données parvenant d'un port est les diffuser sur l'ensemble des ports [4].

Figure 2.2 : Concentrateur (hub)

- **Le répéteur :**

Le répéteur (en anglais repeater) c'est un équipement utilisé pour régénérer le signal entre deux nœuds du réseau, afin d'étendre la distance du réseau. On peut l'utiliser pour relier deux câbles de types différents [4].

Figure 2.3 : Un répéteur

- **Le pont :**

Le pont (en anglais bridge) c'est un dispositif matériel permettant de relier des réseaux travaillant avec le même protocole. Il reçoit la trame et analyse l'adresse de l'émetteur et du destinataire et la dirige vers la machine destinataire [4].

Figure 2.4 : Un pont

- **Le commutateur :**

Comme le concentrateur, le commutateur (en anglais switch) est un élément matériel qui permet de relier plusieurs ordinateurs entre eux. Sa seule différence avec le Hub, il est capable de connaître l'adresse physique des machines qui lui sont connectés et d'analyser les trames reçues pour les diriger vers la machine de destination [4].

Figure 2.5 : Commutateur (switch)

- **La passerelle :**

La passerelle est un système matériel et logiciel permettant de relier deux réseaux, servant d'interfaces entre deux protocoles différents. Lorsqu'un utilisateur distant contact un tel dispositif, celui-ci examine sa requête, et si celle-ci correspond aux règles que l'administrateur réseaux a défini, la passerelle crée un pont entre les deux réseaux. Les informations ne sont pas directement transmises plutôt traduite pour assurer la transmission de deux protocoles [4].

Figure 2.6 : Passerelle

- **Le routeur :**

C'est un matériel de communication de réseau informatique qui permet de choisir le chemin qu'un message va empruntés. Il est utilisé pour relier des réseaux locaux de technologie différente (par exemple Ethernet et token ring). Il intervient sur la couche réseau [4].

Figure 2.7 : Routeur

- **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 [4].

Figure 2.8 : le modem

2.2.2.2 Supports de transmissions

Les Câbles à paires torsadées :

- **Les câbles à paires torsadées (Twisted Pair Câbles)**

  Sont des câbles constitués au moins de deux brins de cuivres entrelacés en torsade (le cas d'une paire torsadée) et recouverts des isolants. En réseau informatique, on distingue deux types de câbles à paires torsadées [4] :

✓ **Les câbles STP (Shielded Twisted pair)**:

Sont des câbles blindés. Chaque paire est protégée par une gaine blindée comme celle du câble coaxial. Théoriquement les câbles STP peuvent transporter le signal jusqu'à environ 150m à 200m.

- **Vitesse et débit** : 0 à 100Mbit/s.

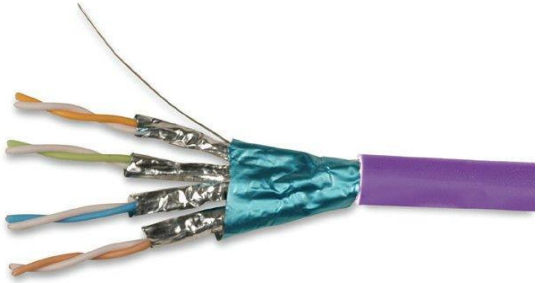


Figure 2.9 : Câble STP

✓ **Les câbles UTP (Unshielded Twisted Pair):**

Sont des câbles non blindés, c'est-à-dire aucune gaine de protection n'existe entre les paires des câbles. Théoriquement les câbles UTP peuvent transporter le signal jusqu'à environ 100m.

- **Vitesse et débit :** 10-100-1000 Mbit/s.

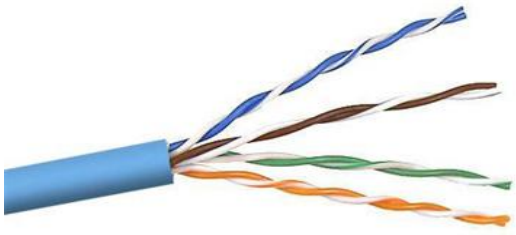


Figure 2.10 : Câble UT

Les câbles à paires torsadées possèdent 4 paires torsadées. Pour les utiliser, on utilise les connecteurs RJ 45 (des connecteurs proches aux RJ 11)

- **Le câble coaxial**

Le câble coaxial, parfois appelé le câble BNC (*British Naval Connector*), a été utilisé pendant longtemps pour le multiplexage des voies téléphoniques. On en distingue habituellement deux types :

✓ **Le câble coaxial fin :**

- Il est en mesure de transporter le signal à une distance de 185m avant que le signal soit atténué

✓ **Le câble coaxial épais :**

- Il est en mesure de transporter le signal à une distance de 500m avant que le signal soit atténué.

Il est constitué de quatre parties : la partie centrale est le conducteur interne, une couche d'isolant appelée diélectrique entoure le conducteur interne, un treillis métallique appelé blindage recouvre la diélectrique, la couche finale est un isolant appelé gaine de protection [5].

- **Vitesse et débit** : 10 à 100Mbit/s.

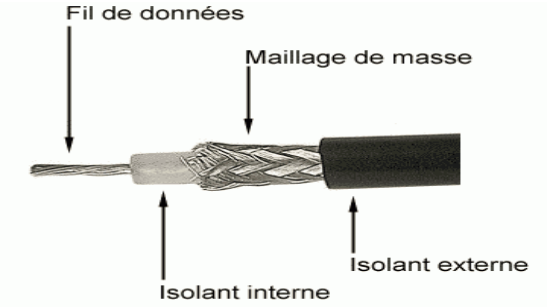


Figure 2.11 : Câble coaxial

- **Fibre optique**

Contrairement aux câbles coaxiaux et paire torsadées, qui conduisent les signaux électriques, la fibre optique conduit un signal fait de photons.

Cette lumière est conduite par une fibre en verre entourée d'une gaine également en verre et le tout est protégé par un enrobage en plastique [6].

Elle est constituée de : Un cœur, une gaine optique et un revêtement primaire qui assure la tenue mécanique.

Les fibres optiques peuvent être classées en deux catégories, selon le diamètre de leur cœur et la longueur d'ondes utilisée :

- ✓ **La fibre multimode :** est généralement utilisée pour des courtes distances. Elle est la plus employée pour les réseaux privés.
- ✓ **La fibre monomode :** cette fibre est utilisée essentiellement pour les sites à distance.

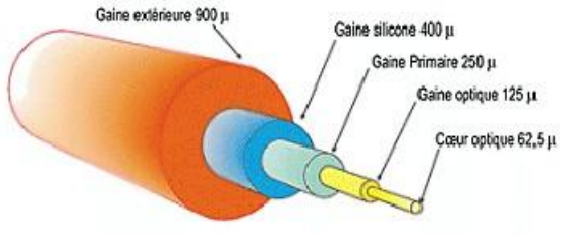


Figure 2.12 : Fibre optique

Le tableau ci-dessous présente une comparaison entre les différents supports de transmission cité précédemment :

	Paires torsadée (Catégorie 6)	Câble coaxial	Fibre optique
Vitesse de transmission	1 Gbits / s	500 Mbps	2 Gbps (très rapide)
Facilité d'installation	Facile	Modérée	Difficile
Difficulté de maintenance	Faible	Modérée	Faible
Sécurité	Bonne	Bonne	Excellente
Avantages	Peu couteux	Possède une plus grande capacité que la paire torsadée	- le plus difficile à espionner. - possède la plus grande capacité
Inconvénients	Interférences Electromagnétique (EMI)	Difficile de travailler avec	Epissure difficile
Cout	Le moins couteux	Modérée	Le plus couteux

Tableau 2.1 : Comparaison des supports de transmission

2.2.2.3 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 [7] :

- Ordinateurs.
- Imprimantes réseau.
- Téléphones VoIP.
- Terminal TelePresence.
- 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).

Une fois les équipements d'interconnexion connecter aux réseaux, ainsi que les supports de transmission, on passe aux types d'architecture d'un réseau ;

2.2.3 Architecture réseau

Différentes architectures existent pour la conception d'un réseau poste à poste et Client/serveur [8] :

- **L'Architecture Poste à Poste :**

  Dans cette architecture, les postes de travail sont simplement reliés entre eux par le réseau ; aucune machine ne joue un rôle particulier car chaque poste peut partager ses ressources avec les autres postes, chaque utilisateur est son propre administrateur et planifie lui-même sa sécurité.

- **L'architecture client /serveur :**

  L'architecture client /serveur désigne un mode de communication dans un réseau qui définit une machine généralement très puissante en terme de capacité d'entrée/sortie et qui correspondent au serveur qui fournit des services à une ou plusieurs machines (clients) qui lui envoient des requêtes.

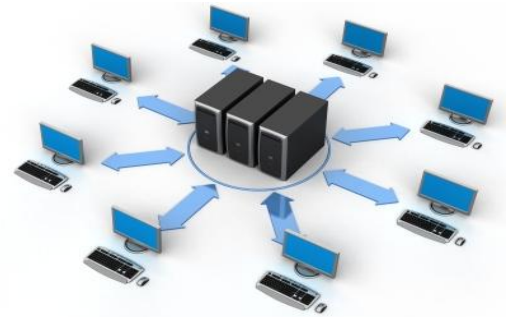


Figure 2.13 : Architecture client/serveur

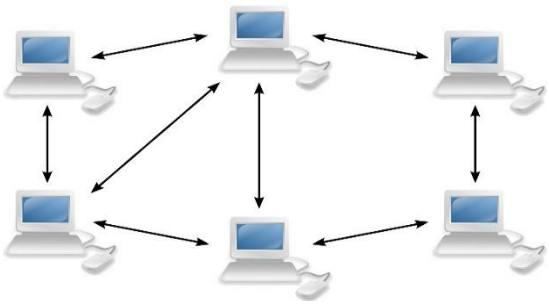


Figure 2.14 : Architecture poste à poste

	Poste à poste	Client/serveur
Avantages	• Facile de mettre en réseau des nouveaux postes. • Pratique pour un réseau domestique. • Peu coûteuse.	• Les ressources réseaux sont centralisées. • Une meilleure sécurité. • L'administrateur est le serveur. • Dans ce modèle le réseau est évolutif. • Plus performant et plus fiable.
Inconvénients	• Les outils de sécurité sont très limités. • Une ressource partagée est accessible par tous les postes du même réseau. • Le système devient ingérable lorsque le nombre de postes augmente.	• Plus coûteux • Si le serveur tombe en panne, ses ressources ne sont plus disponibles.

Tableau 2.2 : Comparaison de deux architectures poste à poste et client/serveur

2.2.4 Les différents modes de liaisons

Il existe trois modes de liaisons sur un réseau : **Simplex, Half-duplex** et **Full-duplex**. On parle de mode **Simplex** lorsque la liaison est à sens unique de transmission, d'un émetteur vers un récepteur.

Dans une transmission de type **Half-duplex**, la liaison est bidirectionnelle mais ne peut être utilisée que dans un sens à la fois. Dans ce cas, les différentes stations d'un réseau peuvent échanger des données en étant tour à tour, émettrices et réceptrices sur une liaison donnée. Il faut alors établir une méthode d'accès au support afin d'éviter les collisions de données *[5]*.

Enfin, le mode **Full-duplex** permet une transmission simultanée de données entre deux stations. Les câbles Ethernet actuels permettent, par exemple, une liaison Full-duplex, permettant la

transmission et la réception simultanées de données par un même câble (mais dans 2 fils différents) *[5]*.

2.2.5 Topologies des réseaux

2.2.5.1 Topologie logique

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

2.2.5.2 Topologie physique :

Désigne la manière dont les équipements sont interconnectés en réseau. En distingue principalement trois types : en bus, en étoile, en anneau *[4]*.

- **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 la même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau *[9]*.

  Elle a pour avantages d'être facile à mettre en œuvre, par contre elle est extrêmement vulnérable étant donné que si un des coupleurs est défectueux, c'est l'ensemble du réseau qui est affecté.

Figure 2.15 : Topologie en bus

- **Topologie en anneau :**

  Une topologie en anneau ressemble assez à une topologie en bus, sauf qu'elle n'a pas de début ni de fin, elle forme une boucle. Quand un paquet est envoyé, il parcourt la boucle jusqu'à ce qu'il trouve le destinataire. Il existe soit la topologie en anneau simple soit la topologie en double boucle FDDI (Fiber Distributed Data Interface), qui permet une redondance et qui comme son nom l'indique est formé de deux anneaux *[4]*.

Figure 2.16 : Topologie en anneau

- **Topologie en étoile :**

  Dans cette topologie chaque périphérique (ordinateur ou imprimante) est relié au nœud central. Les performances d'un réseau Ethernet dépendent principalement du nœud central. C'est un type de réseau relativement efficace et économique. La plupart des petits réseaux locaux fonctionnent sur un même nœud *[4]*.

Figure 2.17 : Topologie en étoile

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 *[10]*.

Relier des ordinateurs avec des topologies différentes dépend lui aussi de certains critères comme la distance et le nombre de machine à connecter donc selon ces critères on comprend que les réseaux sont classifiés comme ci-dessus.

2.2.6 Classification des réseaux

En se basant sur le critère de l'étendue géographique (taille), on arrive à distinguer 4 types de réseaux comme l'illustre la *figure 2.18.* [11]

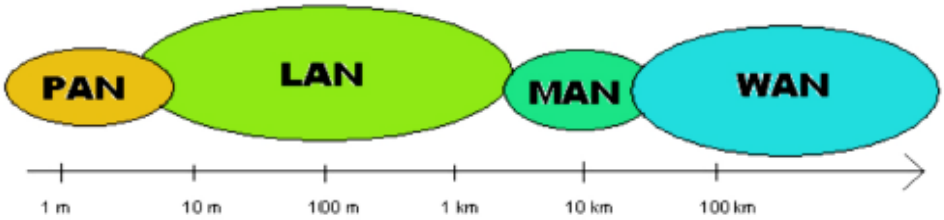


Figure 2.18: Classification des réseaux informatiques

- **Réseau PAN (Personal Area Network) :**

Un réseau PAN (appelé aussi réseau domestique ou réseau individuel) désigne un type de réseau informatique restreint en terme d'équipements, généralement mis en œuvre dans un espace d'une dizaine de mètres [11].

- **Réseau LAN (Local Area Network) :**

Egalement appelés réseaux locaux, dont l'étendue ne dépasse pas quelques kilomètres et limité donc à une circonscription géographique réduite (bâtiment, entreprise, etc.). Les LANs sont généralement réalisés via des liaisons Ethernet, mais peuvent aussi se présenter sous forme de fibres optiques, ou encore, via les technologies sans fil telles que le Wifi. Un réseau LAN sans fil est alors appelé WLAN [11].

- **Réseau MAN (Metropolitan Area Network) :**

Ces réseaux sont généralement utilisés pour interconnecter un ensemble de réseaux locaux géographiquement dispersés, et peuvent couvrir une circonscription géographique importante (un grand campus ou une ville) [12].

- **Réseau WAN (Wide Area Network):**

C'est un réseau à échelle étendue, comme une région, un pays, voir le monde entier. Le plus grand réseau **WAN** et également le plus connu est Internet. Les liaisons peuvent être filaires, mais également en partie sans fil, comme pour les liaisons GSM ou Satellites [12].

2.2.7 Les modèles de références

2.2.7.1 Le modèle OSI :

L'ISO **(*International Standardization Organization*)** a normalisé sa propre architecture sous le nom d'OSI (Open System Interconnexion). Ce modèle théorique (en 7 couches) permettant l'interconnexion des réseaux hétérogènes, a pour rôle de standardiser les transferts entre les machines et permettre aux constructeurs de mettre au point des produits (logiciels ou matériels) compatibles.

Chaque couche du modèle communique avec une couche adjacente (celle du dessus ou celle du dessous), Elle utilise ainsi les services des couches inférieures et en fournit à celle du niveau supérieur [13].

Le tableau ci-dessous offre une description des 7 couches du modèle OSI :

Position dans le modèle OSI	Nom de la couche	Description
7	Couche application	Interface de communication entre le réseau et les applications, elle offre le service réseau à l'application qui le demande.
6	Couche présentation	Gère tous les aspects liés à la présentation des données : format , cryptage , encodage ,etc.
5	Couche session	Responsable de l'initialisation de la session, de sa gestion et de fermeture .
4	Couche transport	Optimise l'utilisation de la couche réseau ,assure la fiabilité et la régulation du transfert de données.
3	Couche réseau	Connexion logique entre les hôtes. Elle traite de tout ce qui concerne l'identification et le routage dans le réseau.
2	Couche liaison de données	Permet d'assurer une liaison fiable par une bonne synchronisation et une détection d'erreurs.
1	Couche physique	Emet des signaux assurant la bonne transmission.

Tableau 2.3: modèle OSI

2.2.7.2 Modèle TCP /IP (Transport Control Protocol /Internet Protocol) :

On parle de **TCP/IP,** en dénommant ainsi les deux protocoles sur lesquels repose le réseau. Le modèle **TCP/IP** représente l'ensemble des règles de communication sur Internet et se base sur la notion « Adressage IP ». Il s'inspire du modèle OSI, auquel il reprend l'approche modulaire mais réduit le nombre à quatre. [4]

Position dans le modèle TCP/IP	Nom de la couche	Description
4	*Couche application*	Elle englobe les applications standards du réseau et s'assure que les données soient correctement « empaquetées » pour qu'elles soient lisibles par la couche suivante.
3	*Couche Transport*	Elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaitre l'état de la transmission.
2	*Couche Internet*	chargée de fournir le paquet des données et de gérer la décomposition / recomposition des segments.
1	*Couche Accès réseau*	spécifie la forme sous laquelle les données doivent être transmises, quel que soit le type de réseau utilisé.

Tableau 2.4: modèle TCP/IP

Le modèle OSI a été développé à vocation normative, pour servir de référence dans le déroulement de la communication entre deux hôtes. Alors que le modèle TCP/IP a une vocation descriptive, il décrit le déroulement de la communication entre deux hôtes. Voici un tableau comparatif des deux modèles [14] :

Les couches OSI	Les couches TCP/IP	Les protocoles
Application	*Application*	DNS , SNMP,FTP, TFTP, TELNET, HTTP,SMTP
Présentation		
Session		
Transport	*Transport*	TCP, UDP
Réseau	*Internet*	IP, ARP, RARP, ICMP
Liaison de données	*Accès réseau*	PPP, HDLC, Ethernet
Physique		

Tableau 2.5: Comparaison des deux modèles

2.2.8 L'Adressage IP :

2.2.8.1 Présentation de l'adresse IP :

Chacun des éléments d'un réseau travaillant avec le protocole IP doit posséder une adresse unique sur le réseau : **adresse IP**. Ce label numérique est employé d'une part pour identifier chaque équipement et d'autre part pour réaliser le routage des datagrammes IP dans le réseau [15].

IPv4 et IPv6 représentent les deux versions d'adresses IP qui existent aujourd'hui. Presque tous les réseaux utilisent la première tandis qu'un nombre croissant d'entreprises ont adopté la seconde qui est l'avenir des adresses IP.

2.2.8.2 Les classes d'adresses IP :

Le but de la division des adresses IP en trois classes A, B et C, est de faciliter la recherche d'un ordinateur sur le réseau. En effet, avec cette notation il est possible de rechercher dans un premier temps le réseau à atteindre, puis de chercher un ordinateur sur celui-ci. Ainsi l'attribution des adresses IP se fait selon la taille du réseau [15].

- L'Adresse de **classe A** autorisé 2^7-2 = 126 réseaux (0 et 127 étant réservés) et 2^{24}=16777216 machines. Elle est utilisée pour les très grands réseaux.

- L'Adresse de **classe B** : le 1er octet doit être compris entre 128 et 191. Les 2 premiers octets (16 bits) représentent l'adresse du réseau et les deux derniers l'adresse de la machine (partie hôte à 16 bits).
- L'Adresse de **classe C** : le premier octet doit être compris entre 192 et 223. Les trois premiers octets (24 bits) représentent l'adresse du réseau et le dernier l'adresse de la machine (8 bits). Elle est la plus utilisée en ce moment, dû à la disparition des classes B devenues indisponibles par suite de manque d'adresses.

2.2.8.3 Les adresses IP publiques et privées

Les adresses publiques sont celles qui sont utilisées sur Internet. Un réseau local ne doit pas utiliser d'adresses publiques. Il utilise des adresses privées.

Les adresses privées peuvent être utilisées par des hôtes au sein d'une organisation, en interne, tant que ces hôtes ne se connectent pas directement à Internet.

L'Autorité d'Affectation de Numéros sur Internet a réservé les 3 blocs suivant dans l'espace d'adressage pour des réseaux internes [8] :

- **Les adresses IP privées :**

Préfixe	Bloc	Plage IP	Nombre d'adresses
10.0.0.0/8	Bloc 24 bit	10.0.0.0 – 10.255.255.255	16777216
172.16.0.0/12	Bloc 20 bit	172.16.0.0 – 172.31.255.255	1048576
192.168.0.0/16	Bloc 16 bit	192.168.0.0 – 192.168.255.255	65536

Tableau 2.6 : Les adresses IP privées

2.3 Conclusion

Au cours de ce chapitre, nous avons parcouru des généralités sur les réseaux informatiques en soulignant leur importance, leurs différents composants et leurs topologies les plus répandues.

Par la suite, nous avons présenté la manière dont les données sont transmises à travers les couches des deux modèles OSI et TCP/IP, en passant par les Protocoles, les services offerts par ces derniers ainsi que l'adressage et ses classes.

Le chapitre suivant présente les différentes attaques réseau ainsi que les moyens et technologies qui permettent de faire face à ces attaques.

CHAPITRE 3

La sécurité des réseaux informatiques

3.1 Introduction :

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

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système, contre les menaces accidentelles ou intentionnelles. D'une manière générale, elle consiste à assurer que les ressources matérielles ou logicielles d'une organisation soient uniquement utilisées dans le cadre prévu [16].

Il est nécessaire de définir dans un premier temps une politique de sécurité dont la mise en œuvre se fait selon les quatre étapes suivantes :

- Identifier les besoins en termes de sécurité, les risques informatiques pesant sur l'organisation et leurs éventuelles conséquences.
- Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés.
- Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés.
- Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace.

3.2 Les enjeux de la sécurité des réseaux informatiques

La sécurité d'un réseau informatique, d'une manière générale, vise les objectifs suivants [16] :

- **La confidentialité :** La protection de données émises sur le réseau, de façon à ce qu'elles ne soient compréhensibles que par des entités autorisées.
- **L'authentification :** La garantie que les données reçues proviennent bien de l'entité émettrice.
- **L'intégrité :** La garantie que les données reçues n'ont subi aucune modification lors du transport dans le réseau.
- **La non-répudiation :** Constitue un moyen efficace pour identifier l'auteur d'une transaction et d'assurer la preuve de l'authenticité de cette dernière.

3.3 Les attaques intentionnelles

C'est l'ensemble des actions malveillantes qui constituent la plus grosse partie du risque, elles font principalement l'objet de mesures de protection. Parmi elles, on compte les menaces passives et les menaces actives [16].

3.3.1 Les attaques passives

Méthode se basant sur l'écoute du réseau à l'aide de sniffeurs : (analyseurs du trafic réseau), elle consiste au détournement des données et des logiciels sans modifier le fonctionnement du réseau. On cite : Espionnage industriel et commercial, copies illicites de logiciels.

3.3.2 Les attaques actives

Ces attaques consistent à modifier des données, à se glisser dans des équipements réseaux ou à perturber le bon fonctionnement de ce réseau.
On cite : Modification et sabotage des informations (ex : fraude financière informatique), modifications des logiciels (ex : virus, ver).

3.4 Quelques solutions de sécurité

3.4.1 Solutions de sécurité minimum

C'est l'ensemble des mesures offrant le minimum en matière de sécurité :

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

3.4.2 La cryptographie

La cryptographie est l'étude de méthodes de chiffrement et de déchiffrement. Elle permet d'assurer l'authenticité, l'intégrité et la confidentialité des données [16].

3.4.2.1 La cryptographie symétrique :

Elle est basée sur une clé unique partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypter les messages.

3.4.2.2 La cryptographie asymétrique (à clé publique) :

Contrairement à la cryptographie symétrique, la cryptographie asymétrique utilise deux clés : un est privée et n'est connue que par l'utilisateur, l'autre est publique et donc accessible par tout le monde.

3.4.2 VLAN (Virtual Local Area Network)

Les réseaux virtuels (Virtual LAN) sont apparus comme une nouvelle fonctionnalité dans l'administration réseau avec le développement des commutateurs [17].

Le VLAN est un concept qui permet de réaliser des réseaux de façon indépendante du système de câblage. Ces réseaux permettent de définir des domaines de diffusion restreints, cela signifie qu'un message émis par une station du VLAN ne pourra être reçu que par les stations de ce même VLAN. Un VLAN est donc, un regroupement logique et non physique de plusieurs stations [17].

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

3.4.2.1 Types de VLAN

Nous pouvons distinguer trois types de VLANs :

- **VLAN de niveau 1 (par port)** :

Le réseau local virtuel est défini en fonction des ports du commutateur (voir *Figure 3.1*) Un inconvénient majeur est qu'une station se déplaçant, implique une modification de la configuration du port auquel elle était associée et du port auquel elle s'associe [18].

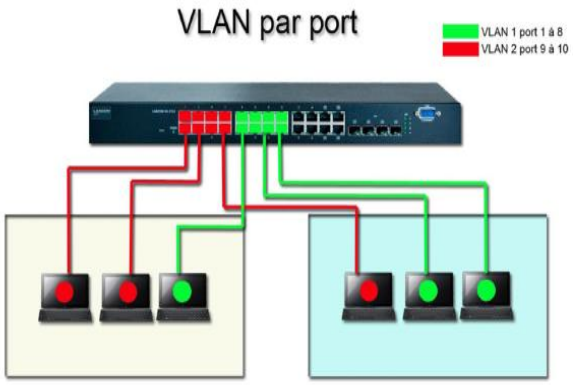


Figure 3.1 : VLAN par port

- **VLAN de niveau 2 (par adresse MAC) :**

Dans ce cas**,** ce sont les adresses MAC des machines qui permettent de déterminer leur appartenance au VLAN (voir *Tableau 3.2*). L'identification des machines par leurs adresses MAC uniques, permet de rendre leur appartenance au VLAN indépendante de leur emplacement [18].

Host MAC Address	VLAN
00 00 80 45 FE 21	VLAN 2
00 00 80 45 DA 47	VLAN 2
00 40 00 80 45 FE	VLAN 3
00 40 80 10 AA 21	VLAN 3
00 00 80 00 FF AB	VLAN 4

Tableau 3.1 : Table de correspondance adresse MAC/VLAN d'un Switch

- **VLAN de niveau 3 :**

Nous en distinguons :

✓ **Par sous-réseau :**

Le VLAN par sous-réseau permet de regrouper plusieurs machines suivant le sous-réseau au quel elles appartiennent. Pour créer un tel VLAN, il faut associer une adresse de sous-réseau à un VLAN (voir *Figure 3.3)* [18].

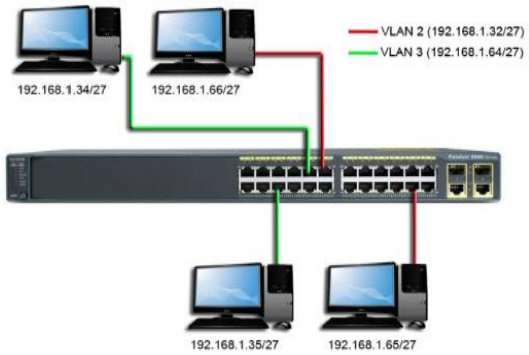


Figure 3.2 : VLAN par sous-réseau (adresse IP).

✓ **Par protocole :**

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

3.4.2.2 les Intérêt des Vlans :

Les Vlans présentent les intérêts suivants [19] :

- ✓ Peut couvrir tout un bâtiment, relier plusieurs bâtiments ou encore s'étendre au niveau d'un réseau plus large (WAN).
- ✓ Optimise la bande passante.
- ✓ Améliorer la gestion du réseau.
- ✓ Séparer les flux.
- ✓ Segmentation réduire la taille d'un Broadcast.
- ✓ Sécurité **:** permet de crée un ensemble logique isolé pour améliorer la sécurité,
  Le seul moyen pour communiquer entre des machines appartenant à des Vlans différents est alors de passer par un routeur ou plusieurs.

3.4.2.3 Les avantages du VLAN :

Parmi les avantages liés à la mise en œuvre d'un VLAN, on retiendra notamment [20] :

- ✓ La flexibilité de segmentation du réseau.
- ✓ La simplification de la gestion.
- ✓ L'augmentation considérable des performances du réseau.

3.4.2.4 Les protocoles de transport des VLANs :

3.4.2.4.1 VTP (Virtual Trunking Protocol) :

C'est un protocole de niveau 2, utilisé pour configurer et administrer les VLANs sur les périphériques CISCO. VTP permet d'ajouter, renommer ou supprimer, un ou plusieurs réseaux locaux virtuels sur un seul commutateur qui propagera cette nouvelle configuration à l'ensemble des autres commutateurs du réseau. VTP permet ainsi d'éviter toute incohérence de configuration de VLANs sur l'ensemble d'un réseau local. [21]

- **Fonctionnement :**

Les messages, VTP diffusent des annonces de création, de suppression ou de modification de VLAN. Lors de chaque création/suppression/modification, une variable appelée RN (Révision Number) s'incrémente (initialement 0 puis 1 puis 2 puis 3, etc.).

Le switch Server envoie un message VTP avec la nouvelle valeur du RN. Les autres switches comparent le RN reçu du switch Server avec le RN qu'ils stockent en local. Si ce dernier est plus petit (logiquement), alors les switches se synchronisent avec le Server et récupèrent la nouvelle base de données des VLANs.

Le switch possède 3 modes VTP :

- Server
- Client
- Transparent

VTP Server :

Le switch en mode Server (mode par défaut), permet à l'administrateur de faire des modifications sur les VLANs et de les propager automatiquement vers tous les switches du réseau.

Figure 3.3 : VTP Server

VTP Client :

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

Figure 3.4 : *VTP Client*

VTP Transparent :

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

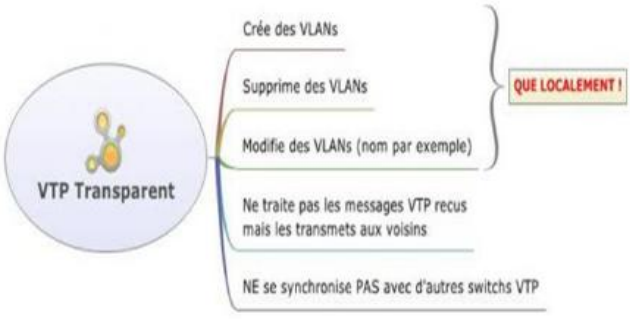


Figure 3.5 : VTP transparent

3.4.2.4.2 Le Trunk

Le trunk est le mécanisme qui permet d'insérer l'identifiant du VLAN sur une trame utilisateur. Toute trame se propageant sur plusieurs switchs conservera toujours l'information de son

appartenance à son VLAN. Et le switch de destination saura avec quels ports la trame peut être commutée (ports appartenant au même VLAN) [22].

Cette configuration de lien Trunk peut être placée entre deux commutateurs, entre un commutateur et un hôte supportant le trunking ou encore entre un commutateur et un routeur.

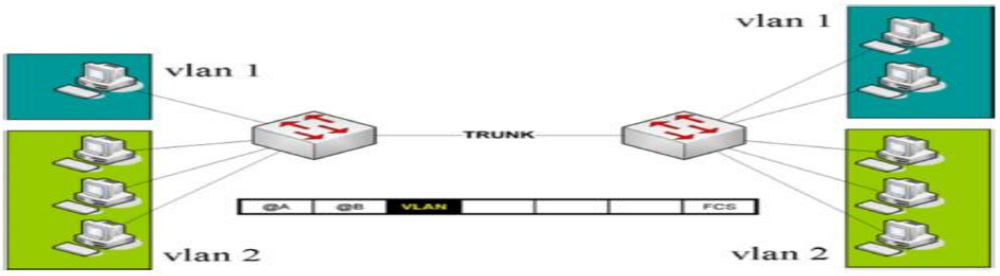


Figure 3.6 : Configuration de liens inter-switch en trunk

Dans le schéma ci-dessous, on configure le lien inter-switch en Trunk. Toutes les trames qui sortiront sur ce lien (switch de droite ou de gauche), se verront appliquer une étiquette supplémentaire qui contiendra l'identifiant du VLAN (en noir sur la trame).

Historiquement, Cisco avait créé son propre protocole de Trunk entre ses switchs, nommé ISL (Inter Switch Link). Mais très rapidement, cette fonctionnalité plus qu'essentielle, demanda une inter-opérabilité avec d'autres constructeurs.

La norme Trunk 802.1Q fut sortie et Cisco l'implémenta aussi dans ses switchs. D'où la possibilité sur certains switchs Cisco de décider quel trunk on souhaite faire, ISL ou 802.1Q.

- **Trunk ISL :**

Le trunk propriétaire Cisco ISL a la particularité d'encapsuler toute la trame de l'utilisateur dans une nouvelle trame, nommée trame ISL. Voici à quoi ressemble une trame ISL :

Entête ISL	Trame Ethernet Utilisateur	FCS
26 octets	0 – 1500 octets	4 octets

Figure 3.7 : Trame trunk ISL

- **Trunk 802.1Q :**

Le trunk normalisé 802.1Q, n'encapsule pas toute la trame de l'utilisateur comme ISL mais casse la trame et y insère une étiquette ou tag, nommée TAG 802.1Q. Voici à quoi ressemble une trame utilisateur avec le rajout du TAG 802.1Q :

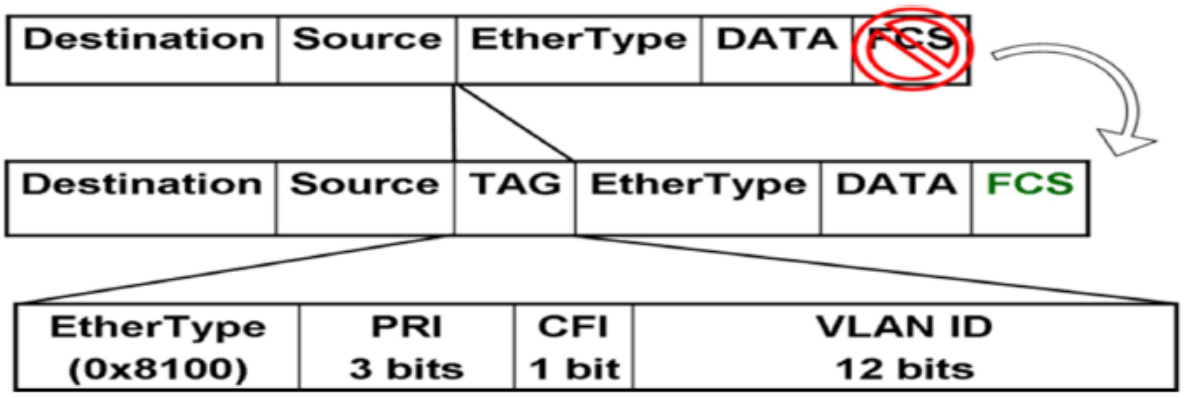


Figure 3.8 : Trame trunk 802.1q

La première trame est celle de l'utilisateur qui arrive sur le switch. Dès que cette trame sort vers un port configuré en Trunk 802.1Q, le switch insère l'étiquette TAG (trame n°2 dans le schéma). En inspectant le contenu de ce TAG, on remarque les champs suivants (trame n°3 dans le schéma) :

- ✓ **Ethertype** : Permet de préciser ce qu'est une trame 802.1Q, la valeur en hexa est
- ✓ 0×8100.
- ✓ **PRI** : Champs de priorité sur 3 bits qui permet de classifier le trafic utilisateur pour lui appliquer de la qualité de service (voix, vidéo…).
- ✓ **CFI** (Canonical Format Identifier) : Permet la compatibilité d'un réseau Ethernet avec un réseau TokenRing.
- ✓ **VLAN ID** (VLAN Identifier) : Codé sur 12bits : valeur numérique du VLAN auquel la trame utilisateur appartient.

3.4.3 Les pare-feu

Un pare-feu (firewall) est un dispositif utilisé pour empêcher les accès non autorisés à un réseau. Sa fonction est double : renforcer une politique de sécurité et journalier un trafic réseau. Le renforcement d'une politique de sécurité consiste à décider s'il faut accepter ou rejeter une connexion selon des règles spécifiques de filtrage permettant de forcer un réseau à se conformer à une politique donnée. La journalisation quant à elle, consiste à enregistrer tous les aspects du trafic afin de pouvoir mieux l'analyser.

Un pare-feu est donc un composant clé pour la conception d'un réseau sécurisé. Cependant, étant un point de passage pour tout le trafic réseau, un pare-feu peut aussi être un unique point de défaillance. Par conséquent, son choix ainsi que son emplacement sont d'importantes tâches pour la sécurité des infrastructures réseau [23].

3.4.3.1 Types des pares-feux

- **Filtrage de paquets** (packet-filtering firewall):

Un pare-feu de filtrage de paquets opère au niveau de la couche réseau. Il examine le contenu des paquets IP et filtre le trafic en fonction des adresses, ports et autres options des paquets.

Le fait d'opérer au niveau réseau lui procure une performance assez élevée car le trafic réseau passe sans délai notable.

Ce type de pare-feu est alors une excellente solution lorsque la performance est une exigence importante. Par exemple, la conception d'un réseau qui doit accueillir une application web telle qu'un site de e-commerce [24].

- **Circuit de passerelles** (circuit Gateway firewall) :

Un pare-feu à circuit de passerelle opère au niveau de la couche transport. Il filtre également le trafic en fonction des adresses. Son principal objectif est de créer un circuit virtuel entre les hôtes source et destination afin d'avoir une connexion plus transparente. Cependant, sa mise en œuvre requiert des "sockets" pour garder une trace des connexions séparées [24].

- **Application proxy** (application-proxy firewall) :

Un pare-feu d'application de proxy œuvre au niveau application et contrôle toutes les connexions entrantes et sortantes du réseau. Si une connexion est autorisée, l'application-proxy l'initie vers l'hôte destination au nom de l'hôte source. Ce type de pare-feu est capable de s'assurer que le trafic qui le traverse est conforme à la politique de sécurité et que les fonctions au sein d'un protocole ou d'une application sont conformes aux politiques spécifiées [24].

3.4.3.2 Emplacement d'un pare-feu

Après le choix du pare-feu approprié, son emplacement nécessite également une attention particulière. Un pare-feu n'est pas une solution magique qui résoudra tous les problèmes de sécurité. Son emplacement doit être choisi selon les fonctions et objectifs envisagés.

- **Emplacement périphérique :**

Étant un dispositif qui doit empêcher tout accès non autorisé, un pare-feu est le plus souvent placé comme intermédiaire entre le réseau qu'il protège et l'extérieur. Cette disposition simple lui permet d'inspecter tout le trafic en provenance ou vers le réseau protégé [25].

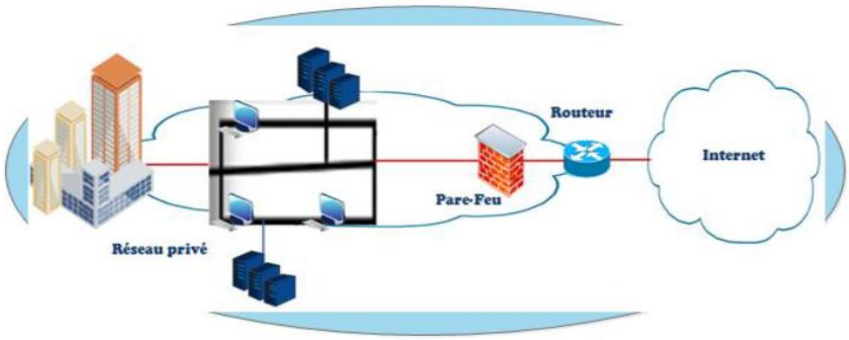


Figure 3.9 : Emplacement périphérique d'un pare-feu

- **Emplacement interne :**

Un pare- feu peut aussi être placé à l'intérieur d'un réseau pour le diviser en plusieurs sous-réseaux et contrôler les différents accès entre eux, le Pare-feu fournit une protection interne entre les différents segments du réseau. Il peut être configuré pour octroyer des accès privilégiés ou restreintes.

Une telle disposition nécessite une puissance de traitement élevée ainsi qu'un dispositif avec plusieurs interfaces. Ce qui est plus coûteux qu'un commutateur normal [25].

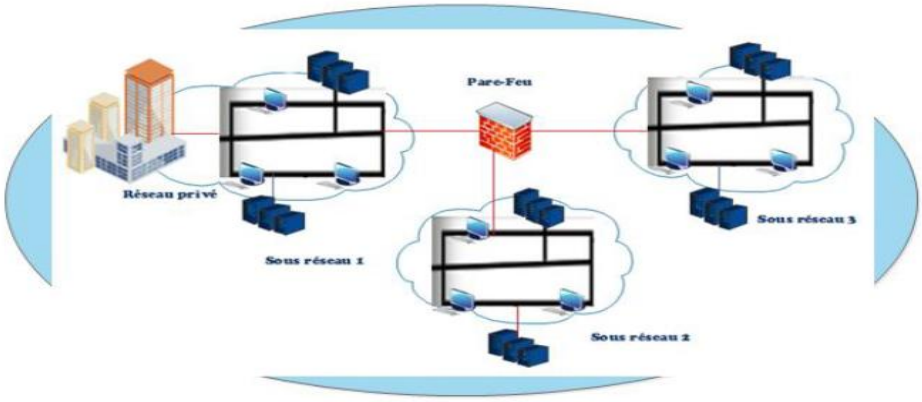


Figure 3.10 : Un pare-feu au centre d'un réseau

3.5 Conclusion

Dans ce chapitre, nous avons très rapidement évoqué les enjeux de la sécurité des réseaux afin de mettre en évidence la nécessité d'élaborer des politiques de sécurité complètes et cohérentes. La mise en place de telles politiques nécessite de penser à prévoir une architecture sécurisée dès la conception avec des redondances aux points stratégiques.

Nous avons ainsi exploré plusieurs techniques de conception sécuritaire d'un réseau telles que les pares-feux, les systèmes de détection et la segmentation. Le pare-feu est l'outil le plus utilisé pour sécuriser un réseau grâce à ses capacités de renforcer une politique de sécurité et d'enregistrer tous les aspects du trafic réseau. Il existe plusieurs types de pare-feu qui pouvant être placés à l'intérieur comme à la périphérique d'un réseau.

Bien qu'étant un puissant outil pour sécuriser un réseau, un pare-feu tout seul ne peut fournir la protection complète souhaitée. La sécurité d'un réseau ne doit pas se reposer sur un seul mécanisme. Une imbrication de mécanismes offre une garantie de sécurité bien supérieur, d'où la nécessité d'inclure des systèmes de détection.

Enfin, pour éviter de concentrer la sécurité en un seul point et optimiser les performances du réseau en réduisant la taille des zones de diffusion (*broadcast*) et augmenter son efficacité, un réseau peut être segmenté en plusieurs sections en effectuant une séparation physique ou logique de ses composantes. Ainsi, on obtient un équilibre entre la sécurité, la vivacité, le coût et la commodité du réseau.

Le chapitre suivant présente la solution proposée pour la réalisation de notre projet, avec l'ensemble des configurations nécessaires à implémenter sur les LANs de l'EPB.

CHAPITRE 4

Cas pratique :
Configuration de l’architecture améliorée

4.1 INTRODUCTION

Chaque projet ou travail, commence généralement par une étude théorique, et se termine par une étude pratique qui est la mise en œuvre de la solution ou bien la réalisation du projet.

Ce présent chapitre, consistera à mettre en œuvre la solution proposée pour la réalisation de notre projet, avec l'ensemble des configurations nécessaires à implémenter sur le réseau local de l'EPB. Ces configurations entourent entre la configuration de routage et des différents protocoles de sécurité pour les VLANs et le Pare-feu(PFsense).

Pour visualiser l'efficacité de notre travail et mettre en évidence l'efficacité de notre solution, nous avons partagé notre travaille en deux parties la première partie segmentation du réseau LAN de l'EPB en VLANs et la deuxième partie installation et configuration du pare-feu (PFsense), nous avons utilisé le simulateur Cisco Packet Tracer version 7.0 et GNS3 qu'est des logiciels très pratique open source pour maquetter un réseau. Il pourra nous servir à reproduire une architecture physique ou logique complète avant la mise en production.

4.2 Partie 1 : Segmentation du réseau de l'EPB en VLANs

4.2.1 Présentation du simulateur (Cisco Packet Tracer 7.0)

Packet tracer : est un logiciel puissant permettant de construire un réseau physique virtuel et de simuler le comportement des Protocoles réseaux sur un réseau.

L'utilisateur construit son réseau à l'aide d'équipements tel que les routeurs, les commutateurs ou des ordinateurs, le tout relier grâce à des connexions tel que (câbles diverses, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP [26].

Le fonctionnement du simulateur PACET TRACER est détaillé en annexe A

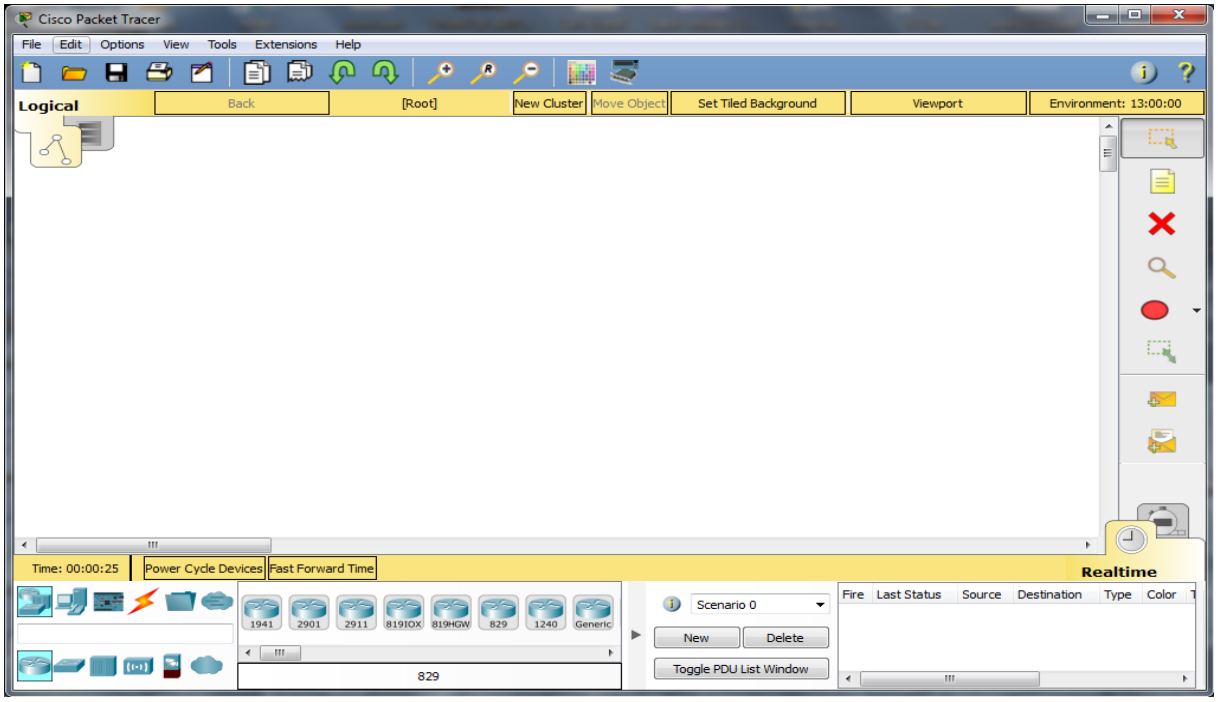


Figure 4.1: Interface Cisco Packet Tracer

4.2.1.1 Méthode de configuration des équipements

Pour configurer les caractéristiques du modèle, nous utilisons le CLI (Command LanguageInterface).

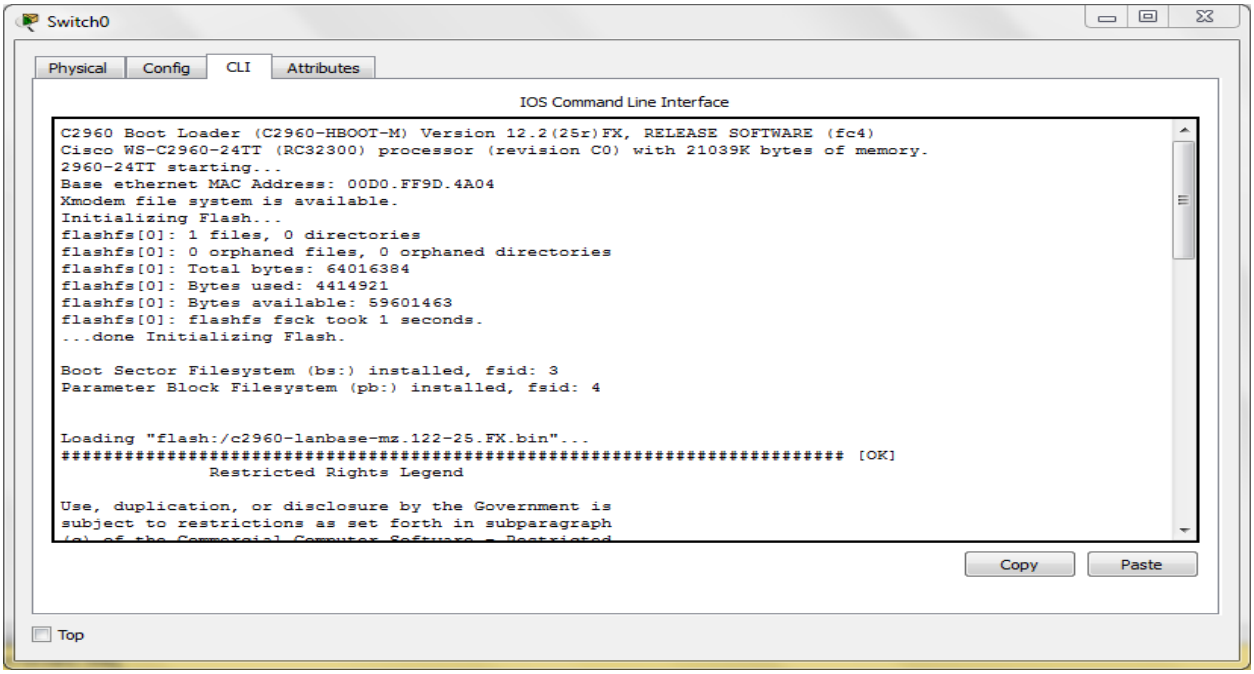


Figure 4.2 : Interface CLI (Command Language Interface).

4.3.1 Segmentation en VLAN

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

- ✓ D'améliorer la gestion du réseau.
- ✓ D'optimiser la bande passante.
- ✓ De Séparer les flux.

4.3.1.1 Matériels et équipements utilisés

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

- ✓ 14 Switch Cisco 2960.
- ✓ 1 switch fédérateur cisco WS-C3560-24PS.
- ✓ Câble RJ45 droit.
- ✓ Câble RJ45 croisé.
- ✓ Des ordinateurs.

4.3.1.2 Schéma du réseau à mettre en œuvre

Le réseau conformément au schéma suivant **:**

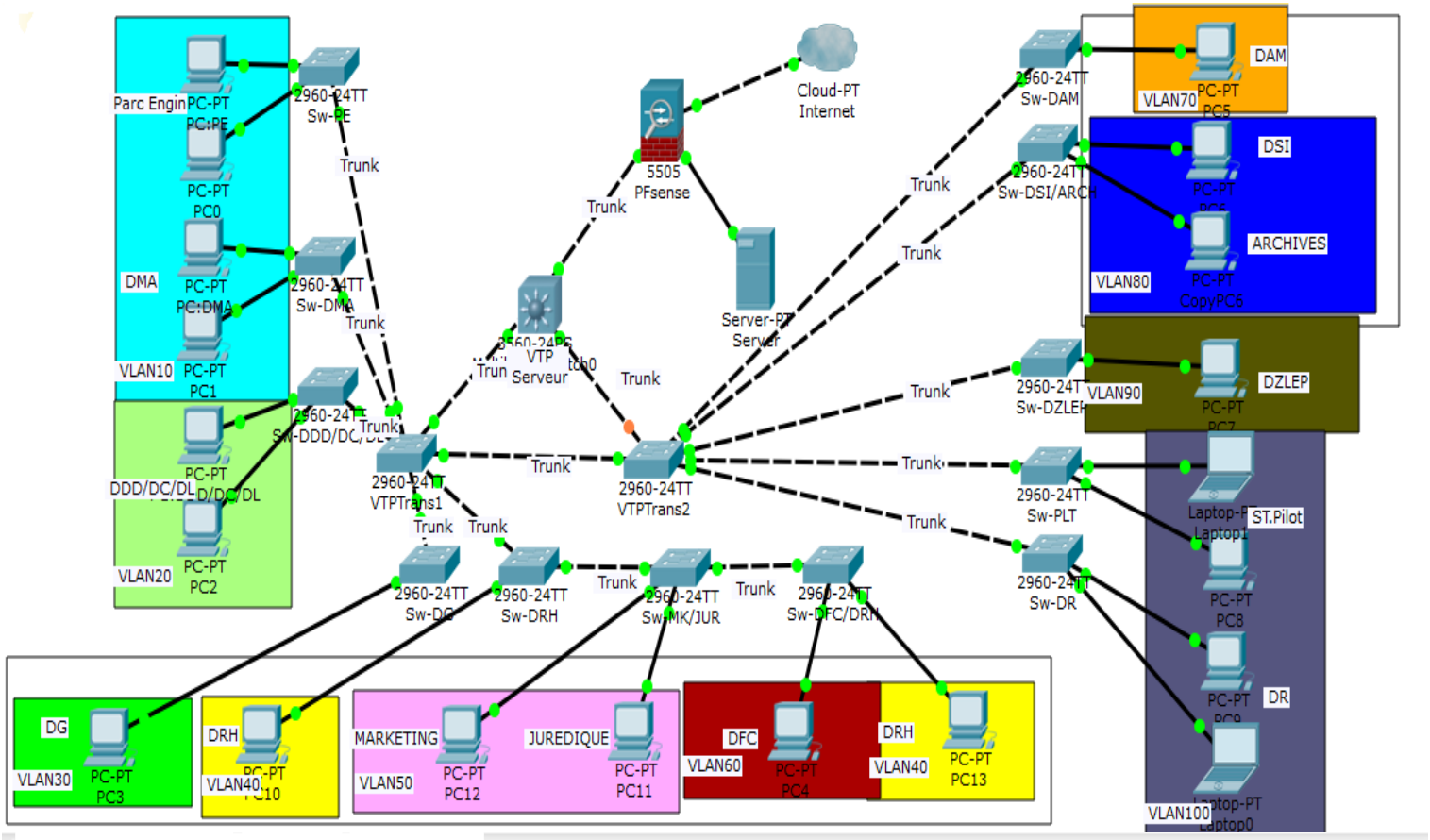


Figure 4.3 : Schéma du réseau à mettre en œuvre

4.3.1.3 Réseau Hiérarchique

- **La couche cœur** contient un switch fédérateur cisco WS-C3560-24PS.
- **La couche de distribution** contient deux Switch VTP TRANSPARENT. (trans1 et trans 2).
- **La couche d'accès** contient douze (12) Switch VTP CLIENT, les ordinateurs, serveurs et imprimantes.

4.3.1.4 Les différents VLANs à implémenter

Après analyse, nous avons défini 13 VLANs répartis comme suit :

- **VLAN DMA/PE (D. Manutention et Acconage / Parc Engin) : Vlan 10**
  - ✓ Ce Vlan contient des ordinateurs et des imprimantes.
- **VLAN DC/DL/DDD (D. Capitainerie/D. Logistique /D. Domaine et Développements) : Vlan 20**
  - ✓ Ce Vlan contient des ordinateurs et des imprimantes.
- **VLAN DG (Direction générale) : Vlan 30**
  - ✓ Ce Vlan contient des ordinateurs et des imprimantes.
- **VLAN DRH (D. Ressources humain) : Vlan 40**
  - ✓ Ce Vlan contient des ordinateurs et des imprimantes.
- **VLAN MK/JUR (Marketing/juridique) : Vlan 50**
  - ✓ Ce Vlan contient des ordinateurs et des imprimantes.
- **VLAN DFC (D. Finance et Comptabilité) : Vlan 60**
  - ✓ Ce Vlan contient des ordinateurs et des imprimantes.
- **VLAN DAM (D. AM): Vlan 70**
  - ✓ Ce Vlan contient des ordinateurs et des imprimantes.
- **VLAN DSI/ARCH (D. Système d'information / Archive) : Vlan 80**
  - ✓ Ce Vlan contient des ordinateurs et des imprimantes relier au réseau.
- **VLAN DZLEP (D. ZLEP): Vlan 90**
  - ✓ Ce Vlan contient des ordinateurs et des imprimantes.
- **VLAN Gestion (Native) : Vlan 99**
  - ✓ Ce Vlan contient des ordinateurs
- **VLAN DR/PLT (D. Remorquages /Pilotage) : Vlan 100**
  - ✓ Ce Vlan contient des ordinateurs et des imprimantes.
- **VLAN Voix IP (Voix IP) : Vlan 150**
  - ✓ Ce Vlan contient des téléphones.
- **VLAN serveur : Vlan 200**
  - ✓ Ce Vlan contient des serveurs relier au réseau.

4.3.1.5 Attribution des ports de Switch aux différents VLANs

Après identification des utilisateurs destinés à échanger des données entre eux, nous avons procéder à l'attribution des ports du Switch aux différents VLANs.
Ainsi, chaque ordinateur connecté à un port du Switch sera assigné à son propre VLAN.

Switch	Ports	Mode	Poste de travail	VLANs
VTPServeur	Fa0/1-3	Trunk	-	-
VTPTrans1	Fa0/1-7	Trunk	-	-
VTPTrans2	Fa0/1-7	Trunk	-	-
Sw-PE	Fa0/1	Trunk	-	-
	Fa0/2-22	Access	PE	VLAN 10
	Fa0/23	Access	PE	VLAN 150
	Fa0/24	Access	PE	VLAN 99
Sw-DMA	Fa0/1	Trunk	-	-
	Fa0/2-22	Access	DMA	VLAN 10
	Fa0/23	Access	DMA	VLAN 150
	Fa0/24	Access	DMA	VLAN 99
Sw-DDD/DC/DL	Fa0/1	Trunk	-	-
	Fa0/2-22	Access	DDD/DC/DL	VLAN 20
	Fa0/23	Access	DDD/DC/DL	VLAN 150
	Fa0/24	Access	DDD/DC/DL	VLAN 99
Sw-DG	Fa0/1	Trunk	-	-
	Fa0/2-22	Access	DG	VLAN 30
	Fa0/23	Access	DG	VLAN 150
	Fa0/24	Access	DG	VLAN 99
Sw-DRH	Fa0/1-2	Trunk	-	-
	Fa0/3-22	Access	DRH	VLAN 40
	Fa0/23	Access	DRH	VLAN 150
	Fa0/24	Access	DRH	VLAN 99

Sw-MK/JUR	Fa0/1-2	Trunk	-	-
	Fa0/3-22	Access	MK/JUR	VLAN 50
	Fa0/23	Access	MK/JUR	VLAN 150
	Fa0/24	Access	MK/JUR	VLAN 99
Sw-DFC/DRH	Fa0/1	Trunk	-	-
	Fa0/2-13	Access	DFC	VLAN 60
	Fa0/14-21	Access	DRH	VLAN 40
	Fa0/23	Access	DFC/DRH	VLAN 150
	Fa0/24	Access	DFC/DRH	VLAN 99
Sw-DR	Fa0/1	Trunk	-	-
	Fa0/2-22	Access	DR	VLAN 100
	Fa0/23	Access	DR	VLAN 150
	Fa0/24	Access	DR	VLAN 99
Sw-PLT	Fa0/1	Trunk	-	-
	Fa0/2-22	Access	PLT	VLAN 100
	Fa0/23	Access	PLT	VLAN 150
	Fa0/24	Access	PLT	VLAN 99
Sw-DZLEP	Fa0/1	Trunk	-	-
	Fa0/2-22	Access	DZLEP	VLAN 90
	Fa0/23	Access	DZLEP	VLAN 150
	Fa0/24	Access	DZLEP	VLAN 99
Sw-DSI/ARCH	Fa0/1	Trunk	-	-
	Fa0/2-22	Access	DSI/ARCH	VLAN 80
	Fa0/23	Access	DSI/ARCH	VLAN 150
	Fa0/24	Access	DSI/ARCH	VLAN 99
Sw-DAM	Fa0/1	Trunk	-	-
	Fa0/2-22	Access	DAM	VLAN 70
	Fa0/23	Access	DAM	VLAN 150

	Fa0/24	Access	DAM	VLAN 99

Tableau 4.1 : attributions des ports des switchs au différents VLANs

4.3.1.5 L'adressage

Après l'attribution des ports du switchs aux différents VLANs, nous avons données des adresses de Sous-réseaux aux différents VLANs, des adresses IP aux différents machines, des adresses IP de passerelles aux interfaces et des adresses IP de l'interface de gestion de switchs comme indiqué dans le tableau ci-dessous :

Nom de Vlan	ID	**Adresse Réseau**	**Plan d'adressage**	**Adresse de diffusion**	**Passerelle**	**Masque sous-réseau**	
Vlan DMA/PE	10	10.0.0.0	10.0.0.1 - 10.0.0.126	10.0.0.127	10.0.0.126	255.255.255.128	/25
Vlan DDD/DC/DL	20	10.0.0.128	10.0.0.129 - 10.0.0.254	10.0.0.255	10.0.0.254	255.255.255.128	/25
Vlan DG	30	10.0.1.0	10.0.1.1 - 10.0.1.126	10.0.1.127	10.0.1.126	255.255.255.128	/25
Vlan DRH	40	10.0.1.128	10.0.1.129 - 10.0.1.254	10.0.1.255	10.0.1.254	255.255.255.128	/25
Vlan MK/JUR	50	10.0.2.0	10.0.2.1 - 10.0.2.126	10.0.2.127	10.0.2.126	255.255.255.128	/25
Vlan DFC	60	10.0.2.128	10.0.2.129 - 10.0.2.254	10.0.2.255	10.0.2.254	255.255.255.128	/25
Vlan DAM	70	10.0.3.0	10.0.3.1 - 10.0.3.126	10.0.3.127	10.0.3.126	255.255.255.128	/25
Vlan DSI/ARCH	80	10.0.3.128	10.0.3.129 - 10.0.3.254	10.0.3.255	10.0.3.254	255.255.255.128	/25
Vlan DZLEP	90	10.0.4.0	10.0.4.1 - 10.0.4.126	10.0.4.127	10.0.4.126	255.255.255.128	/25
Vlan gestion	99	10.0.4.128	10.0.4.129 - 10.0.4.254	10.0.4.255	10.0.4.254	255.255.255.128	/25
Vlan DR/PLT	100	10.0.5.0	10.0.5.1 - 10.0.5.126	10.0.5.127	10.0.5.126	255.255.255.128	/25
Vlan Voix Ip	150	10.0.5.128	10.0.5.129 - 10.0.5.254	10.0.5.255	10.0.5.254	255.255.255.128	/25
Vlan Serveurs	200	10.0.6.0	10.0.6.1 – 10.0.6.126	10.0.6.127	10.0.6.126	255.255.255.128	/25

Tableau 4.2 : Adressage des différents VLANs

4.3.1.6 Création des VLANs

4.3.1.6.1 Configuration de base

Nous présentons si dessous la configuration de base du switch (Direction des systèmes D'information), switch mode VTPTransparent et le Switch central (création du nom et des mots passe) .

Multilayer Switch: VTPserveur

Switch>enable
Switch#configure terminal
Switch(config)#hostname VTPServeur

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

VTPserveur(config)#enable secret **class**

• **Configurer la ligne console** :

VTPServeur(config)#line console 0
VTPServeur(config-line)#password**cisco**
VTPServeur(config-line)**#**login
VTPServeur(config-line)#exit

• **Configurer le terminal virtuel (VTY) :**

VTPServeur(config)#line vty 0 15
VTPServeur(config-line)#password **cisco**
VTPServeur(config-line)#login
VTPServeur(config-line)#exit

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

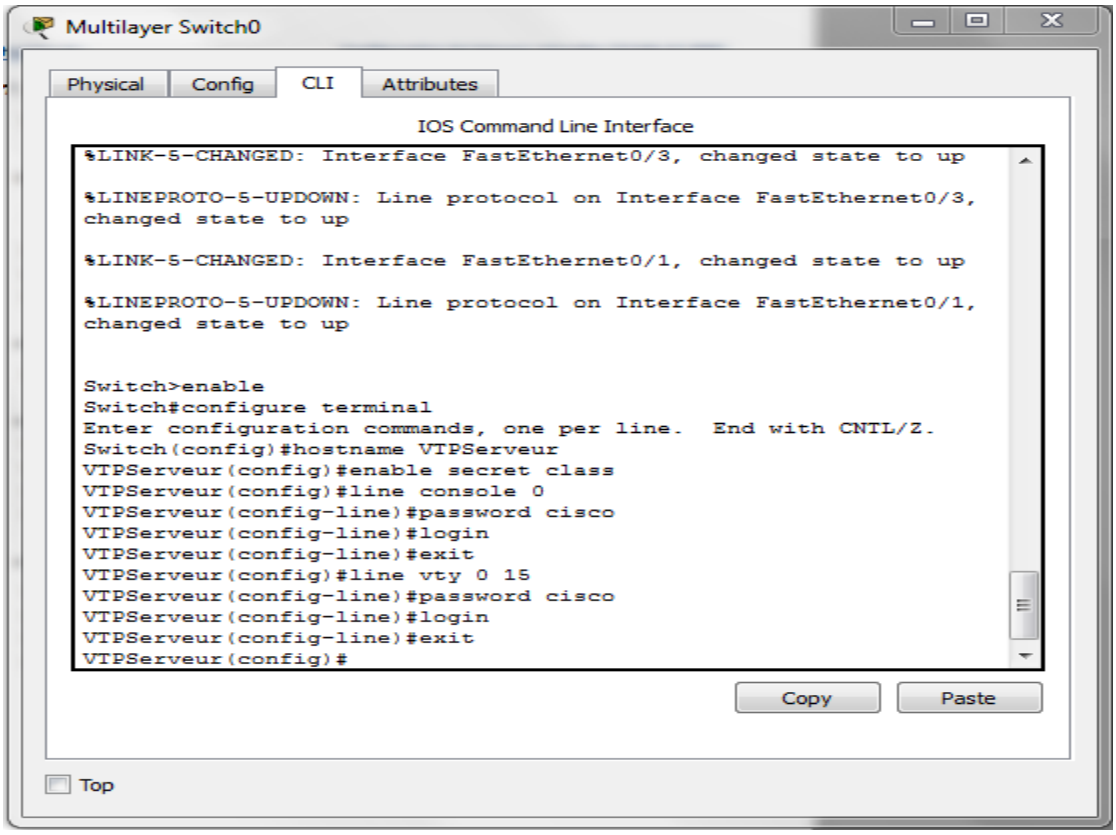


Figure 4.4 : Configuration de base

4.3.1.6.2 Configuration du VTP :

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

- **Mode VTP serveur :**

• Activation du mode trunking des ports fa 0/1-3 :

VTPServeur(config)#interface range fa 0/1-3
VTPServeur(config-if-range)#switchport Trunk encapsulation ?
dot1q Interface uses only 802.1q trunking encapsulation when trunking
VTPServeur(config-if-range)#switchport trunk encapsulation dot1q
VTPServeur(config-if-range)#switchport mode trunk
VTPServeur(config-if-range)#exit

• Activation du serveurVTP :

VTPServeur(config)#vtp version 2
VTPServeur(config)#vtpdomain EPB
Changing VTP domain name from NULL to EPB
VTPServeur(config)#no ip domain lookup

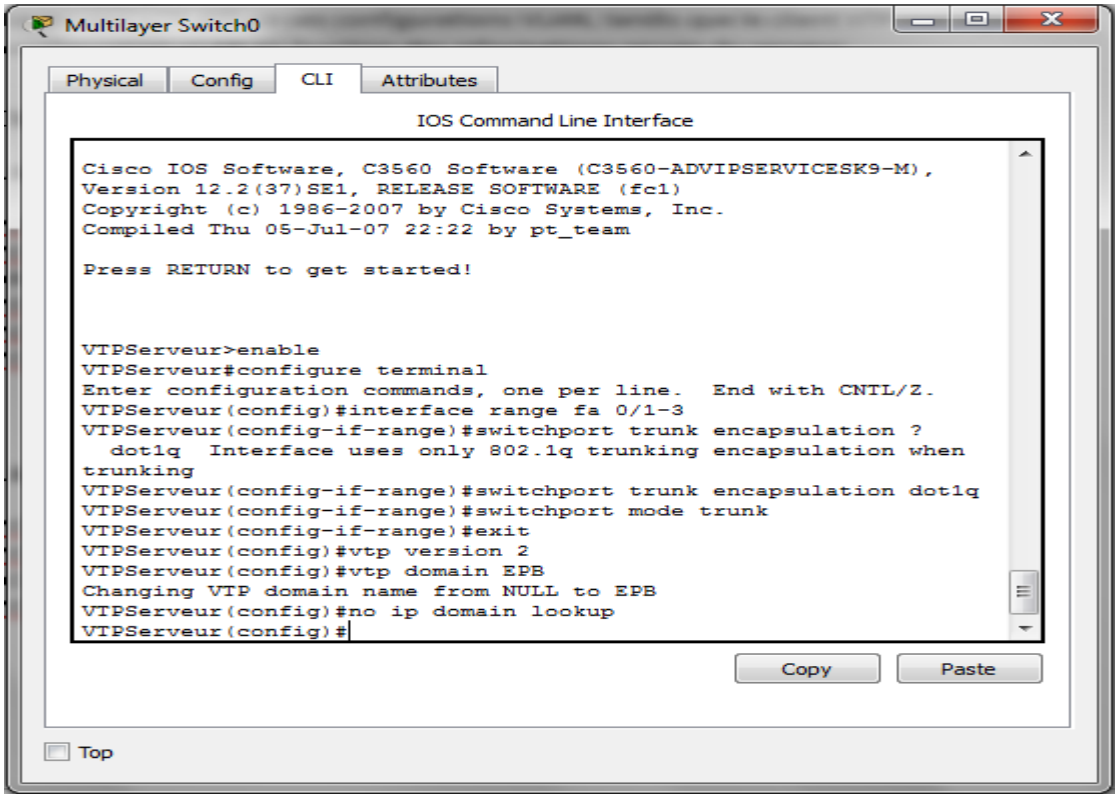


Figure 4.5 :Activation du mode VTPServeret mode trunking

Cette configuration de base s'applique aux niveaux de switch fédérateur cisco WS-C3560-24PS pour activer le mode VTP serveur et le mode Trunk.

Il faut désactiver les ports Non-utiles

- **Mode VTP transparent :**

• **Activation du mode trunking des ports fa 0/1-7 :**

VTPTrans1(config)#interface range fa 0/1-7
VTPTrans1(config-if-range)#switchport mode trunk
VTPTrans1(config-if-range)#exit

• **Activation du transparent VTP :**

VTPTrans1(config)#VTP domain EPB

VTPTrans1(config)#VTP mode transparent
VTPTrans1(config)#exit

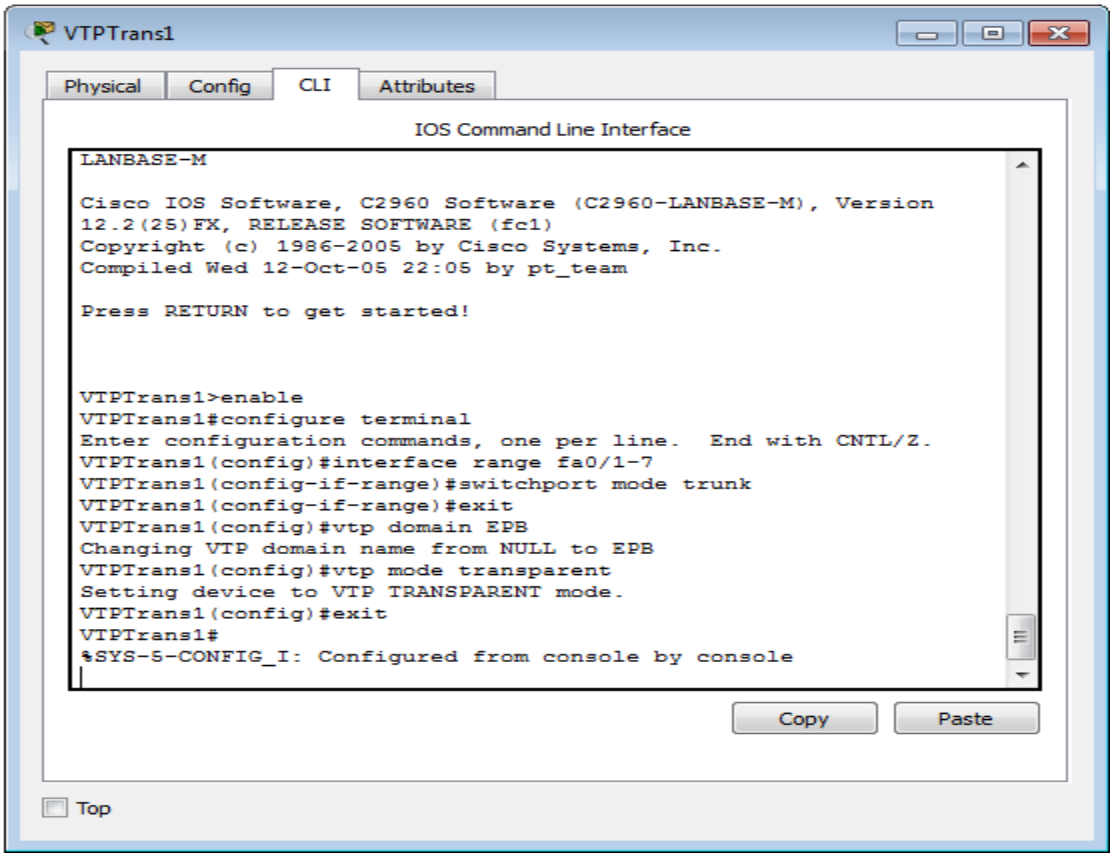


Figure 4.6 : Activation du mode VTPTransparent et mode truking

Cette configuration de base s'applique aux niveaux de deux switchsde la couche de distribution pour activer le mode VTP transparent et le mode Trunk.

- **Mode VTP client :**

Switch DSI/ARCH :

• **Activation du mode trunking des ports fa 0/1 :**

DSI/ARCH (config)#interface fa 0/1
DSI/ARCH (config-if)#switchport mode trunk
DSI/ARCH (config-if)#exit

• **Activation du client VTP :**

DSI/ARCH (config)#VTP domain EPB
DSI/ARCH (config)#VTP mode client

DSI/ARCH (config)#exit

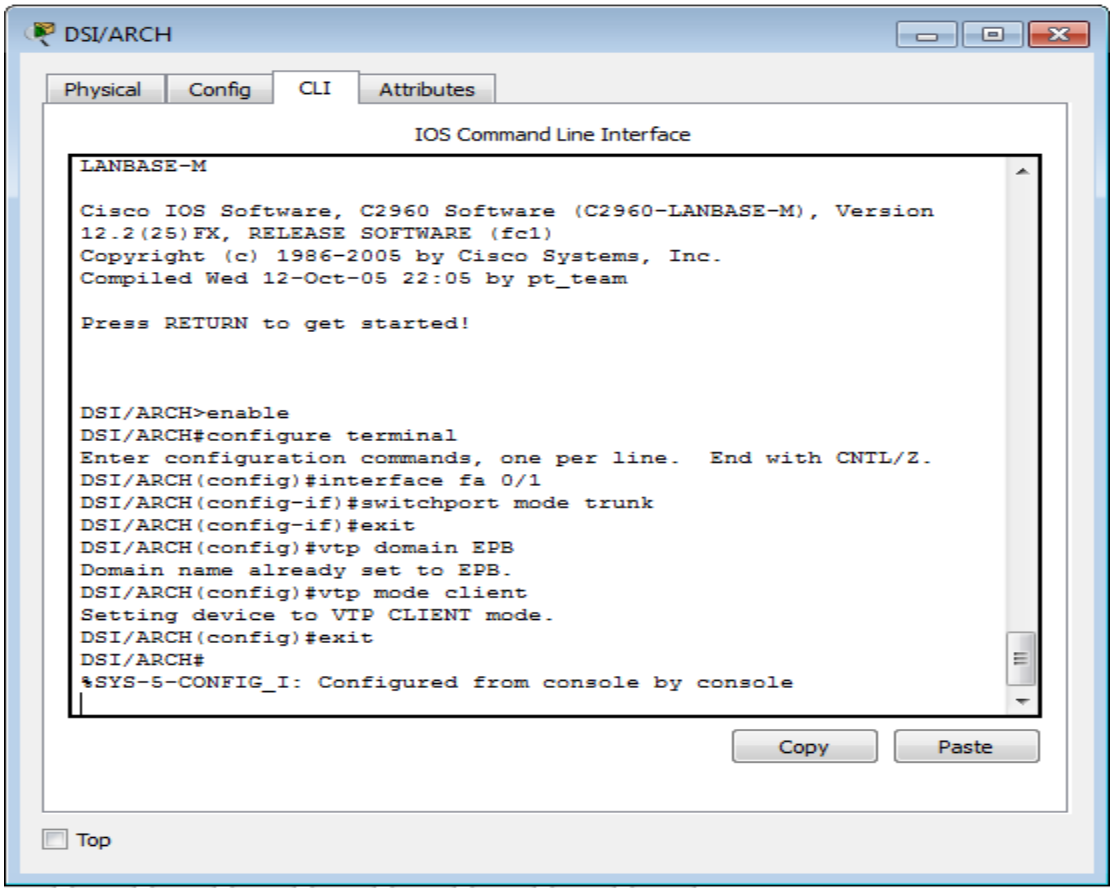


Figure 4.7 : Activation du mode VTPClient et mode truking

Cette configuration de base s'applique aux niveaux de tous les switchs de la couche d'accès, pour activer le mode VTP client et le mode Trunk.

4.3.1.6.3 Configuration et créations des VLANs sur le serveur VTP :

- **Création des VLANs :**

Maintenant on va créer et nommer les VLANs au niveau de Switch VTPServeur

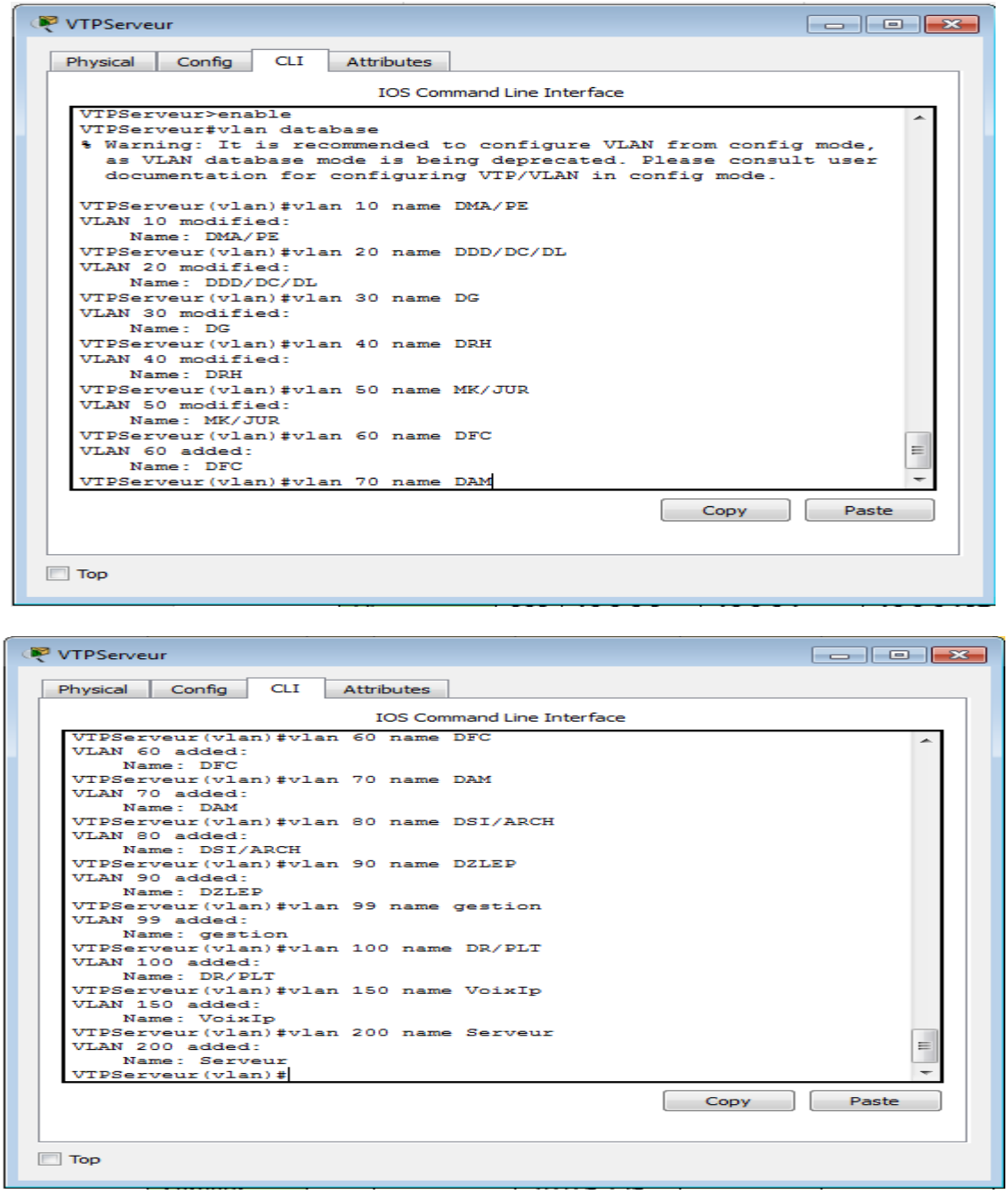


Figure 4.8 : Création Des VLANs au niveau de switch Fédérateur

Vérification :

On vérifier si les réseaux locaux virtuels criés sur SW fédérateur (VTPServeur) ont été distribués aux différents switchs en mode client.

Pour **DSI/ARCH** :

On va taper la commande **show vlan brief**

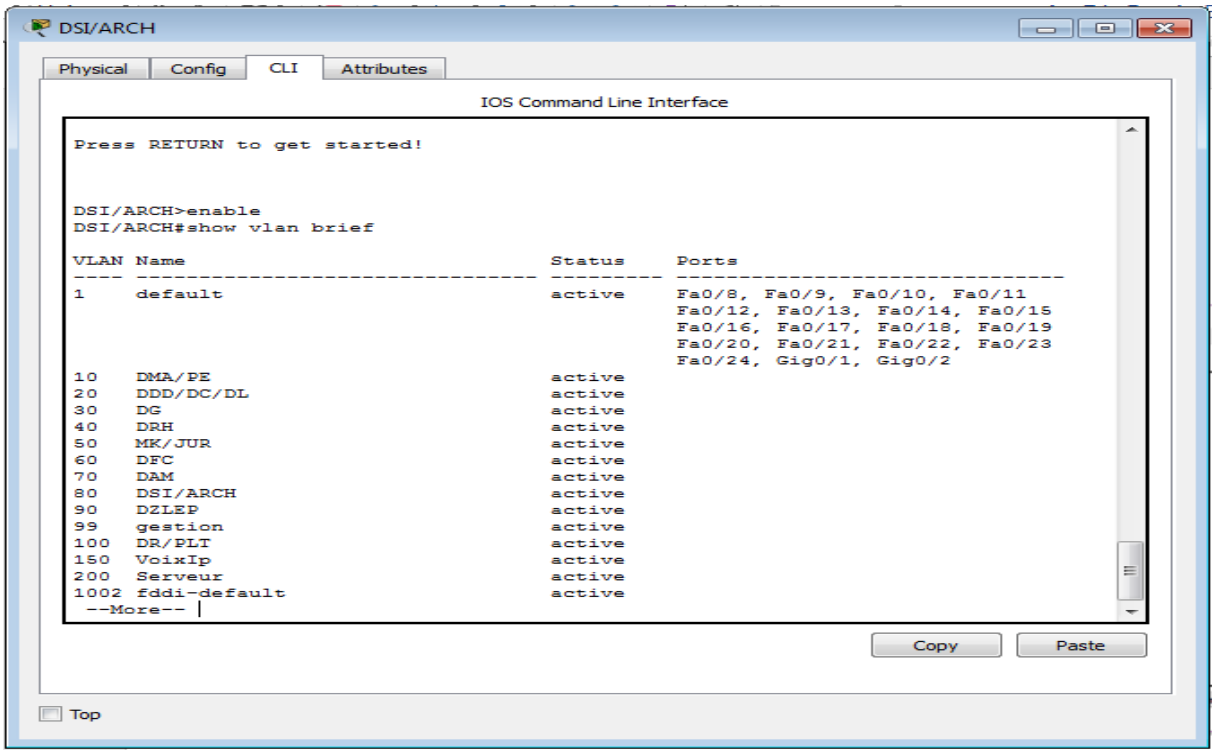


Figure 4.9 : Vérification de la création des vlans au niveau des switchs mode client.

La même chose pour tous les switchs et on voie que le serveur VTP a distribuer tous les nomsqu'on a crié.

4.3.1.6.4 Configuration des VLANs sur le serveur VTP

Maintenant que tous les VLANs sont créés on va distribuer les adresses des sous-réseaux automatiquement sa veux dire dynamiquement en activant le protocole DHCP pour chaque VLANsauf VLAN Serveur (statiquement) en utilisant la commande :

#IP DHCP pool suivi du « nom du vlan »
#Network « address IP de sous-réseau » et le masque de « sous-réseau »
Et la passerelle en utilisant la commande
#default-router « passerelle »
Même configuration pour tous les VLANs qu'on a créés

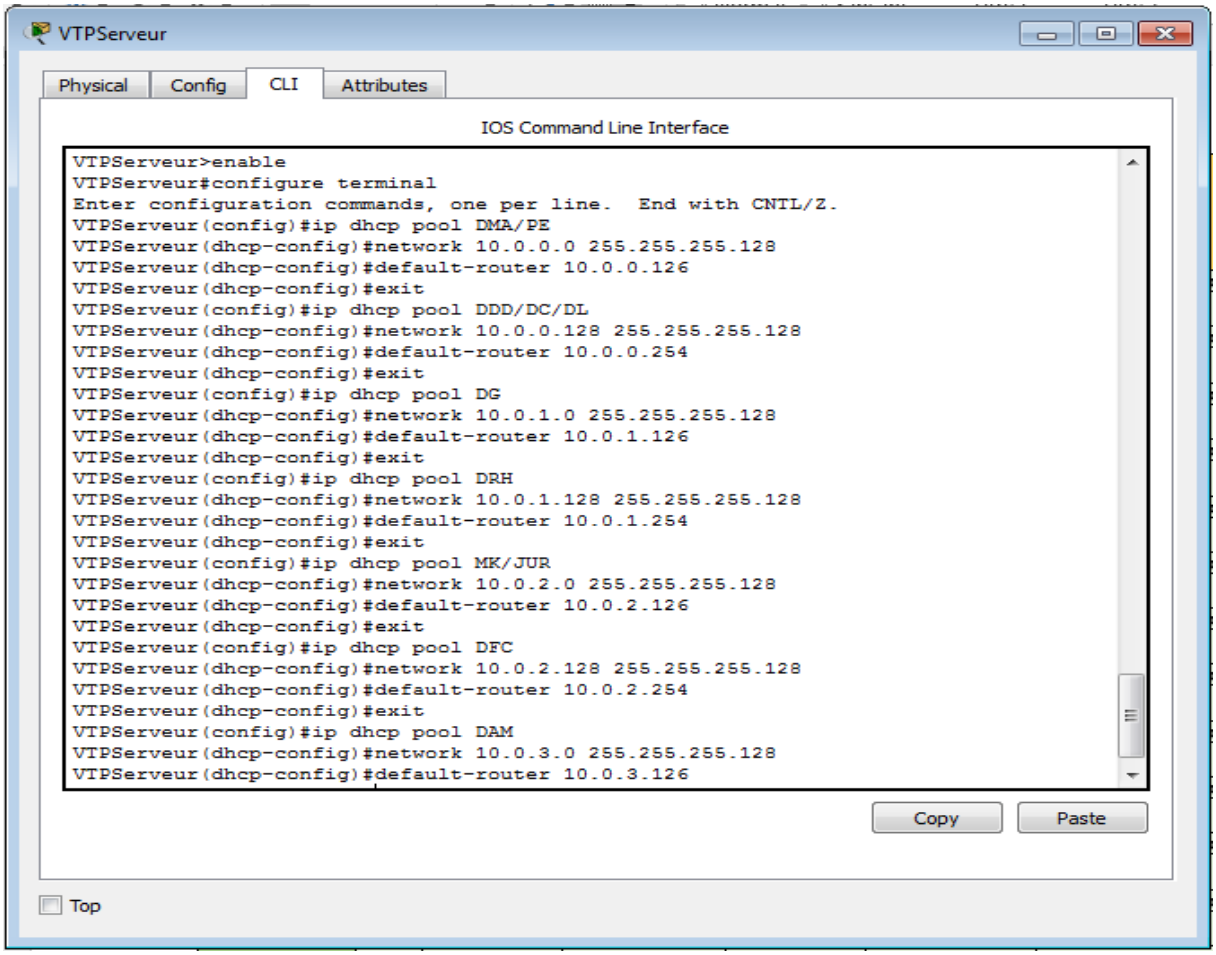


Figure 4.10 :distribution des adresses IP dynamiquement(DHCP)

- **Configuration des ports VLANs sur les switchs (Mode Access) :**

•SwitchDFC/DRH

- **DFC VLAN 60 port 2-13**

DFC/DRH (config)# interface range FastEthernet 0/2-13
DFC/DRH (config-if-range)#switch access VLAN 60
DFC/DRH (config-if-range)#exit

- **DRH VLAN 40 port 14-21**

DFC/DRH (config)# interface range FastEthernet 0/14-21
DFC/DRH (config-if-range)#switch access VLAN 40
DFC/DRH (config-if-range)#exit

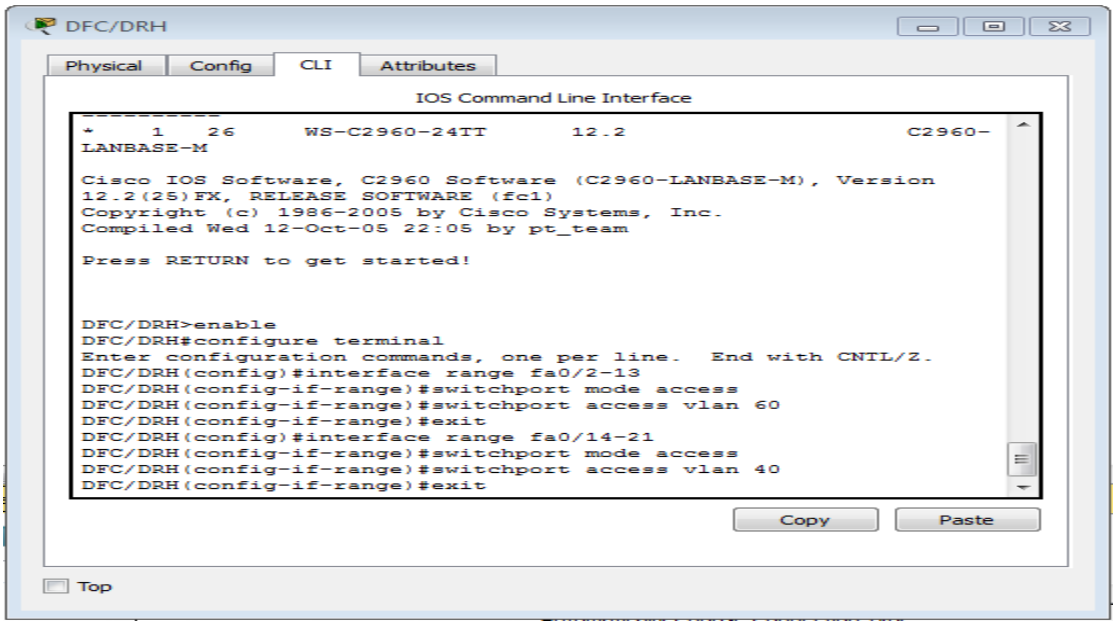


Figure 4.11 : affectation de port au vlan

Cette configuration de base s'applique aux niveaux de tous les switchs, pour activer le mode Access à s'avoir les VLAN et chaque vlan associer à son port.

Vérification :

Maintenant c la dernière étape on passe à la vérification :

•On vérifier les vlan qu'on a créé :

On utilisant la commande **show vlan brief ou show vlan** :

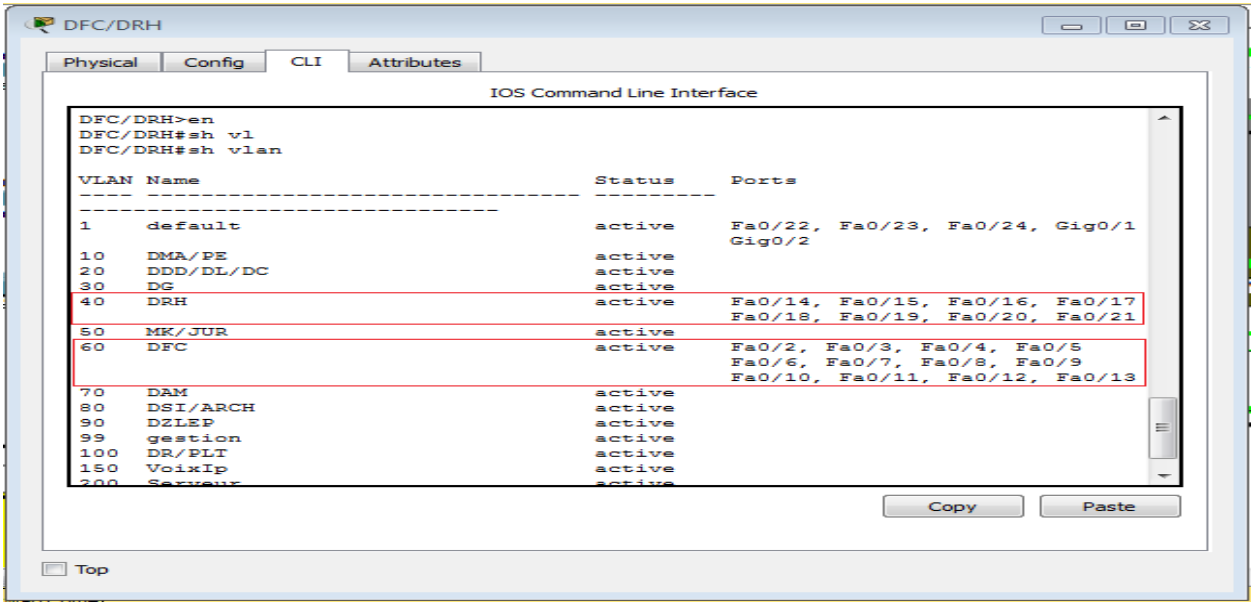


Figure 4.12 : vérificationd'affectation de port au vlan

La même procédure pour tous les switchs, on voie que les vlan sont criée.

•Les tests (les pings) :

Testez la communication entre les différents PC du réseau local de l'EPB :

Résultats du test effectué au niveau du vlan 10 :
Ping réussi entre PC :PE et PC : DMA du VLAN PE/DMA

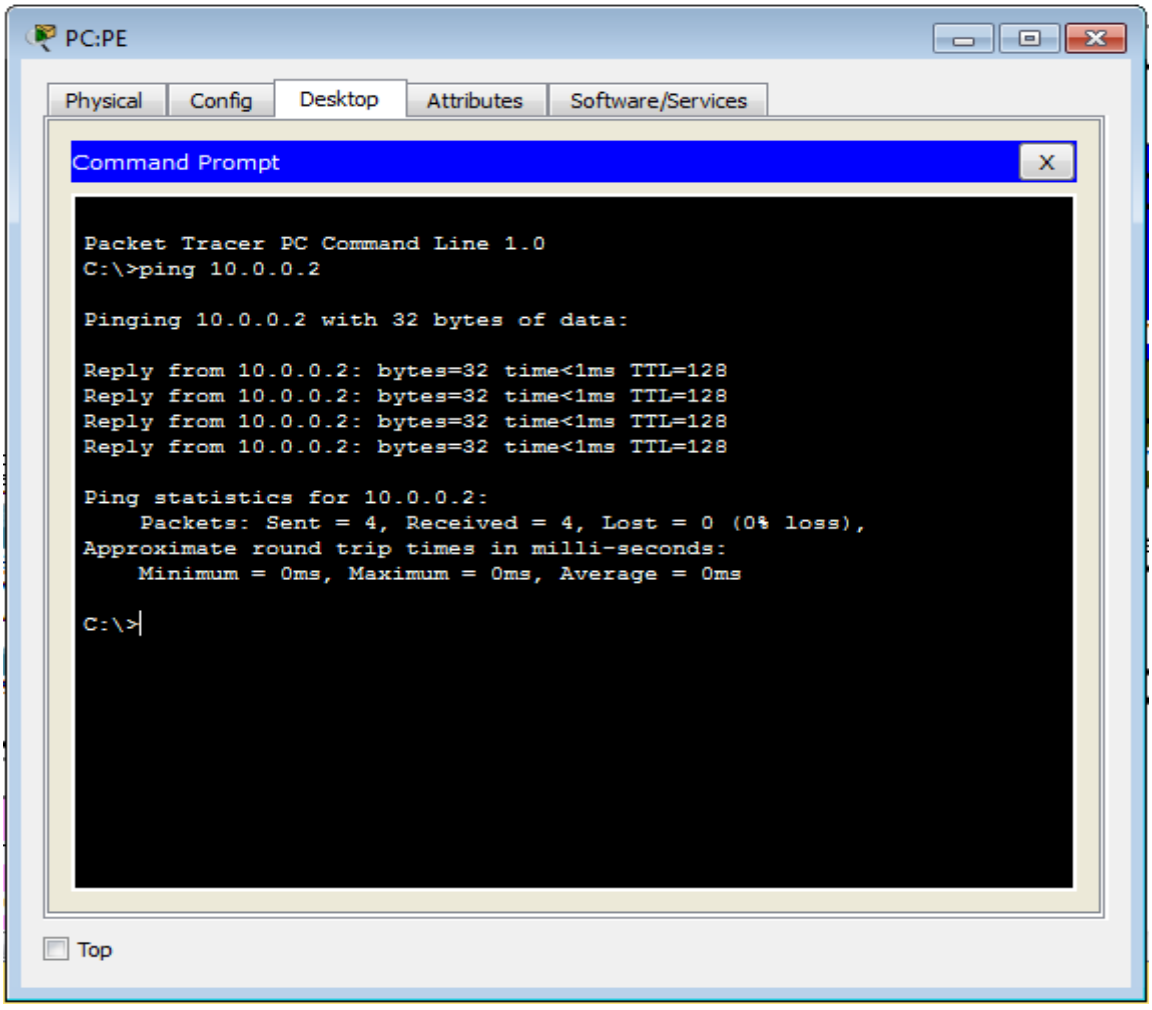


Figure 4.13 : Ping réussi entre PC :PE et PC : DMA

Ce résultat montre que les Pc du vlan 10 communiquent entre eux.

Résultats du test effectué au niveau du vlan 10 et vlan 20 :

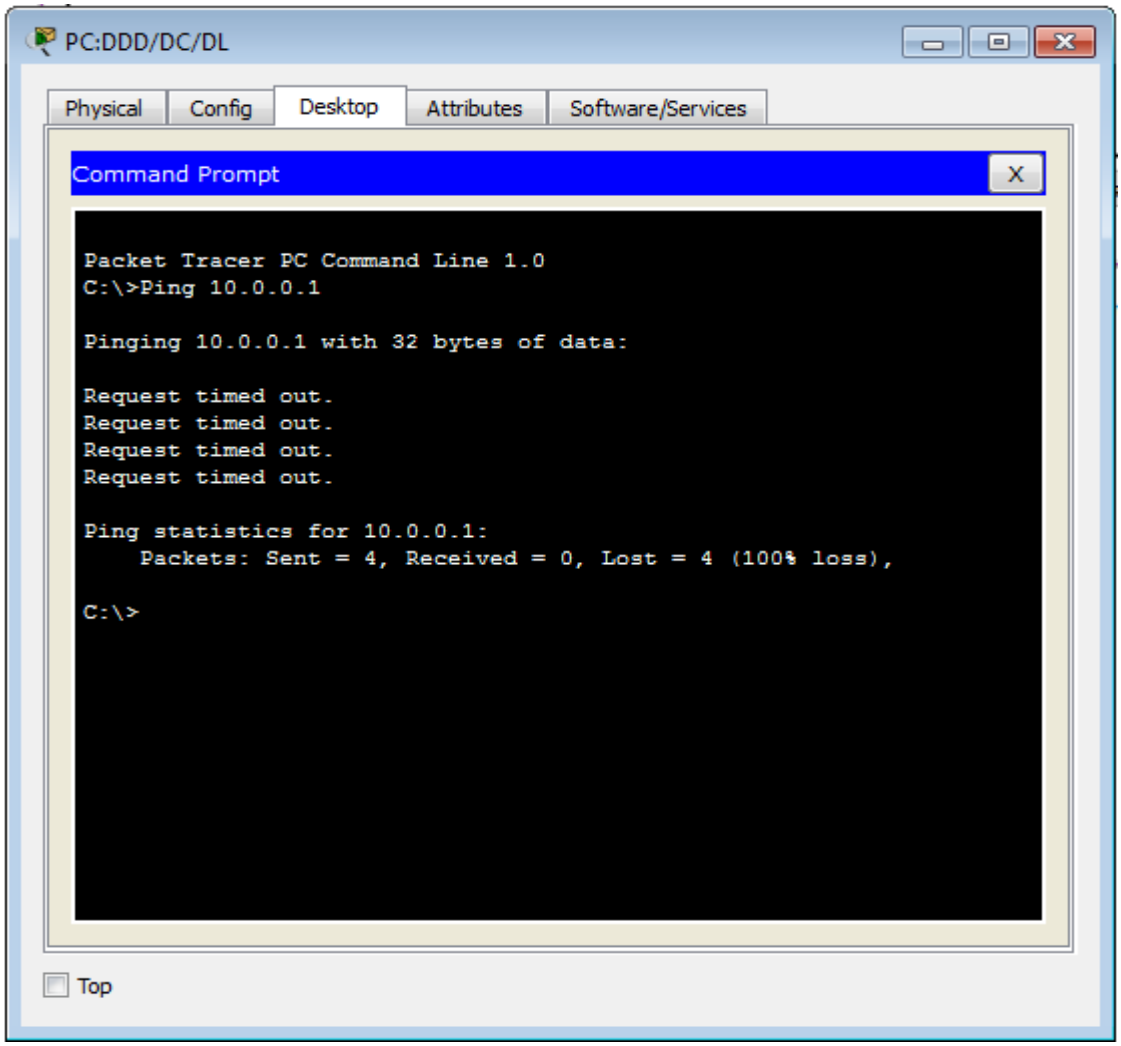


Figure 4.14 : Ping échoue entre PC vlan 10 et PC vlan 20

Ce résultat montre que les Pc du vlan 10 il ne peut pas communique avec les Pc du vlan 20, la mêmechose pour tous les autres vlan qu'on a filtrés, sa montre que notre configuration a réussie.

4.3 Partie 2 : Configuration de pare-feu (PFsense)

4.3.1 Présentation du pare-feu (pfsense)

PfSense : est un routeur / pare-feu opensource basé sur FreeBSD. pfsense peut être installé sur un simple ordinateur personnel comme sur un serveur. Basé sur PF (*packet filter*), comme iptables sur GNU/Linux, il est réputé pour sa fiabilité. Après une installation en mode console, il s'administre ensuite simplement depuis une interface web et gère nativement les VLAN (802.1q) [26].

Les avantages de PFSense que :

- Il est adapté pour une utilisation en tant que pare-feu et routeur
- Il comprend toutes les fonctionnalités de pare-feu coûteux commerciales, et plus encore dans de nombreux cas ;
- Il peut être installé sur un simple ordinateur personnel comme sur un serveur ;
- Il est basé sur PF (PacketFilter), comme iptables sur GNU/Linux généralemet
- Il permet d'intégrer de nouveaux services tels que l'installation d'un portail captif, la mise en place d'un VPN, DHCP et bien d'autres.
- Il offre des option de firewalling /routage plus évoluée qu'IPCop
- Il permet en autre de réaliser :
  - un portail captif (Lorsqu'un utilisateur ouvre son navigateur internet il est redirigé vers une page lui proposant de s'identifier pour se connecter) : solution proposée par les hotspot.
  - Un serveur VPN
  - De réaliser du Load Balancing MultiWAN (utiliser deux connexion Internet avec 2 FAI différents pour avoir une redondance et ainsi éviter les pannes ADSL).
- La configuration se fait dans l'interface web, sans rien toucher à la ligne de commande.

L'installation de pfsenseest détaillée en annexe B.

Les pré-requis matériels pour l'installation sont :

- RAM : 512M (256 min).
- HDD : 1Gb
- Processor : 100Mhz min.
- 2 cartes réseaux.

4.3.2 Configuration Basique de Pfsense

Apres l'installation de pare-feu(pfsense)Notre serveur est maintenant accessible via l'adresse du **WAN**.

Pour se connecter à l'interface de configuration on utilisera l'adresse ip de l'interface WAN http://192.168.8.254, le couple login/pass par défaut est [admin/pfsense].

L'interface WEB :

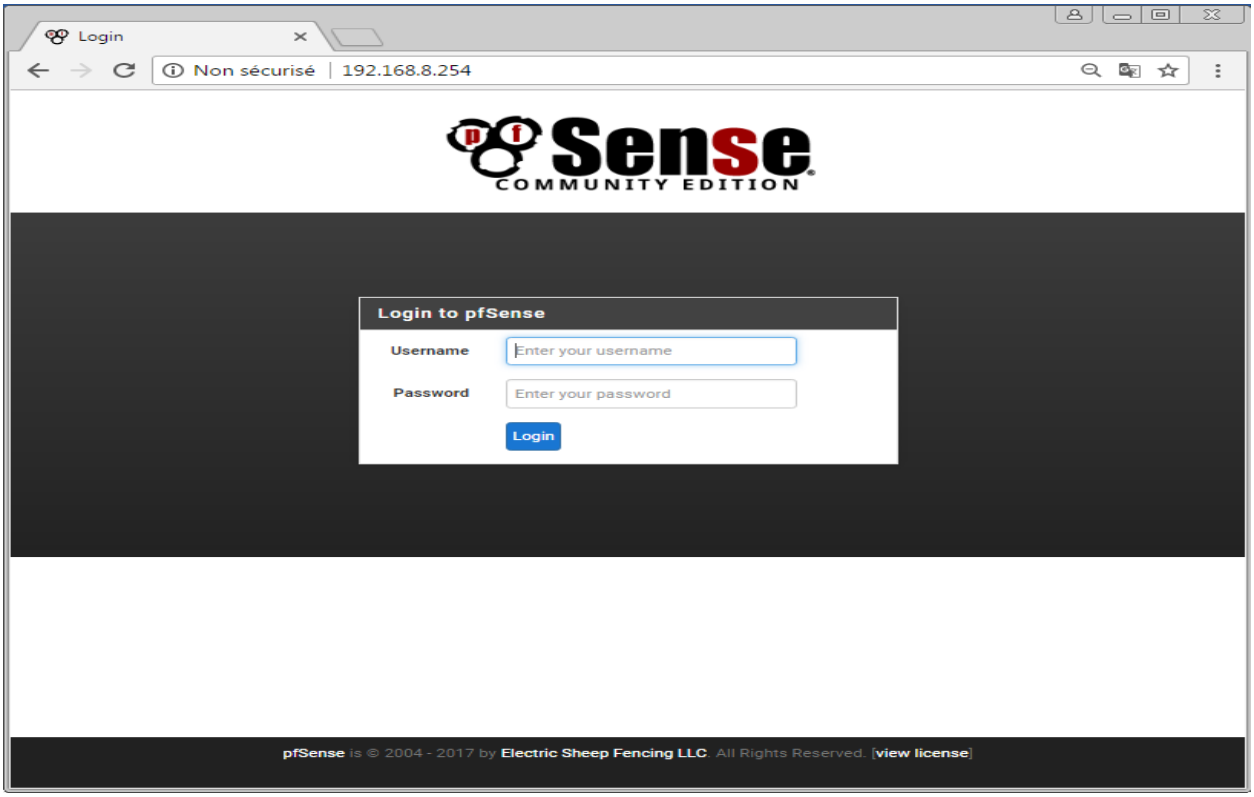


Figure 4.15 : interface de connexion de pfSense

A ce stade-là, on doit configurer basiquement notre serveur, pour faire cela on choisit ***SetupWizard***du menu ***System***, puis on tape ***Next.***

1.Le nom du firewall par la directive hostname **:** pfSense**.**
2. Ensuite le domaine du firewall par la directive domain :EPB.
3. L'adresse des serveurs DNS de votre réseau :8.8.4.4
8.8.8.8
4. Le fuseau horaire à l'aide du menu déroulant Time zone : Africa/algiers;
5. Les changements par le bouton **SAVE :**

Figure 4.16 : Interface tableau de bord de pfsense

Nous nous rendons maintenant dans le menu **System | Advanced** afin de basculer sur un protocolechiffré pour accéder au **pfSense**. Il est en effet préférable d'utiliser un protocole chiffré de manière générale, etindispensable lorsqu'il s'agit d'accéder à l'interface d'administration d'un firewall.

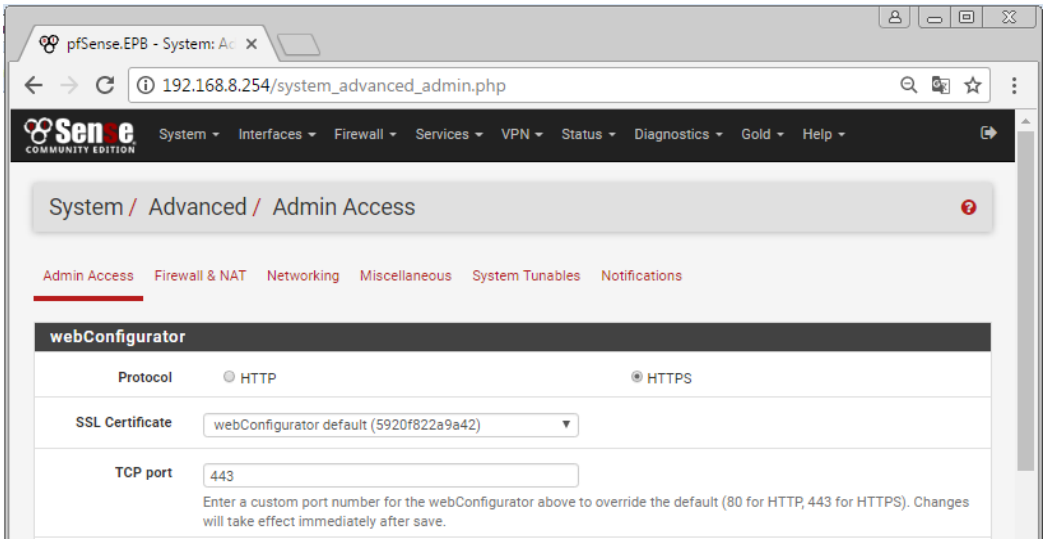


Figure 4.17 : Interface configuration d'un protocole du chiffrement (HTTPs)

Après l'activation du protocole **https**, l'interface d'administration se recharge automatiquement et bascule sur le protocole chiffré.

4.3.2 Configurations avancées de Pfsense

Création d'une passerelle (gateway) :

On ne trouve normalement qu'une seule gateway sur un réseau. Mais pour des besoins spécifiquescomme de l'équilibrage de charge, ou plus simplement des besoins particuliers de routage, il est nécessairede passer par la création de passerelles supplémentaires. Leurs créations restent simples **:**

- ✓ Dans le menu **System | Routing;**
- ✓ Aller dans l'onglet **Gateways;**
- ✓ Cliquer sur le bouton **+Add** pour ajouter une nouvelle règle passerelle ;
- ✓ Sélectionner l'interface sur laquelle la gateway doit être active ;
- ✓ Sélectionner le nom de la passerelle ;
- ✓ Sélectionner l'adresse IP de la passerelle (dans notre cas @ :192.168.8.1) ;
- ✓ Sélectionner éventuellement une adresse demonitoring ;
- ✓ Ajouter une description **;**
- ✓ Valider les changements par le bouton **Save**;
- ✓ Cliquer sur le bouton **Apply**changes;

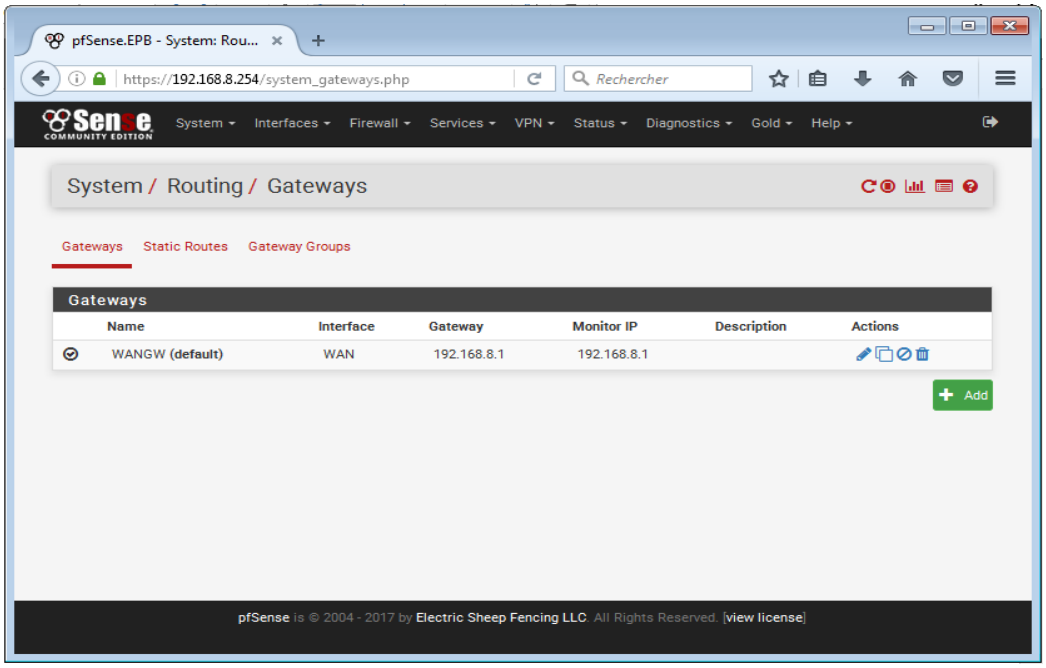


Figure 4.18 : Interface configuration de routage (passerelle)

4.3.2.1 Configuration des vlans

Maintenant, nous devons créer et configurer des VLANs dans pfSense
Pour commencer, nous allons dans le menu "Interface" > "assign" :
Puis, nous nous rendons dans l'onglet "VLANs" et cliquons sur l'icône en forme de "+Add" se trouvant en bas à droite.
Les éléments de configuration sont les suivants :

1. **Parent interface** : l'interface physique à laquelle sera rattachée le VLAN
   - ✓ Les VLANs doit être associé à une interface physique différente de l'interface physique déjà associée au "WAN"
2. **VLAN tag** : l'ID du VLAN (la valeur doit être comprise entre 1 et 4094)
3. **VLAN Priority** : la priorité à appliquer au VLAN (la valeur doit être comprise entre 0 - 7)
4. **Description** : champ optionnel de description du VLAN

Exemple de résultat obtenu :

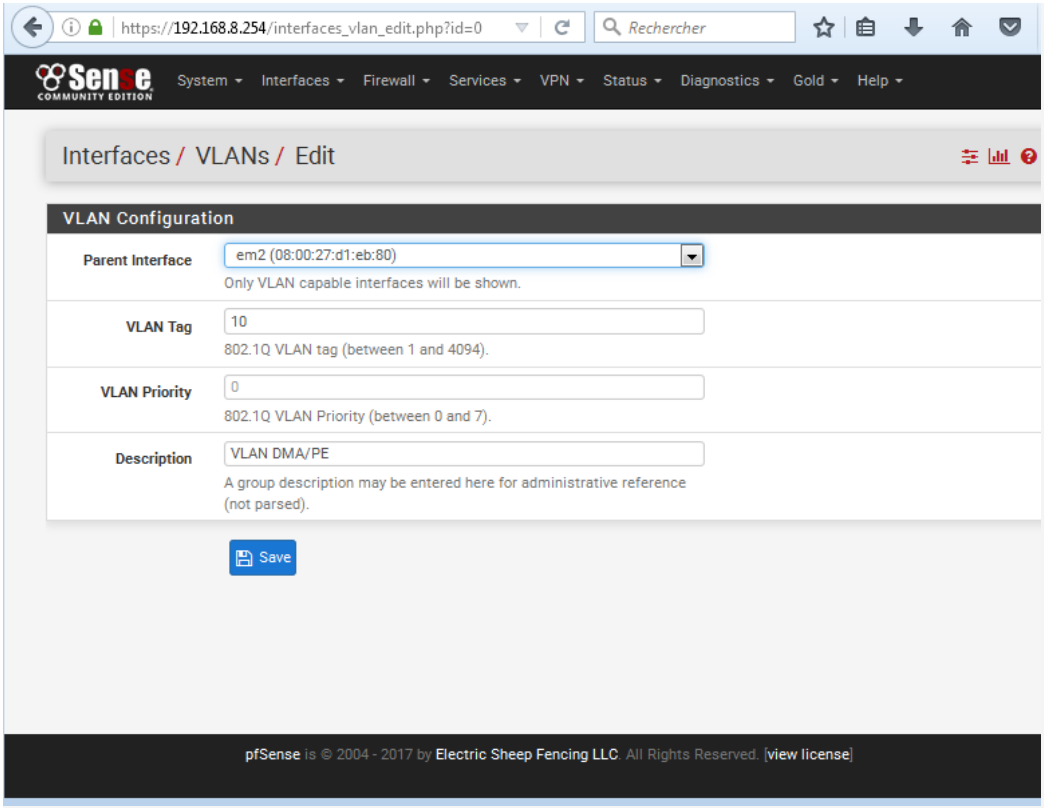


Figure 1.19 : Interface création de vlan

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

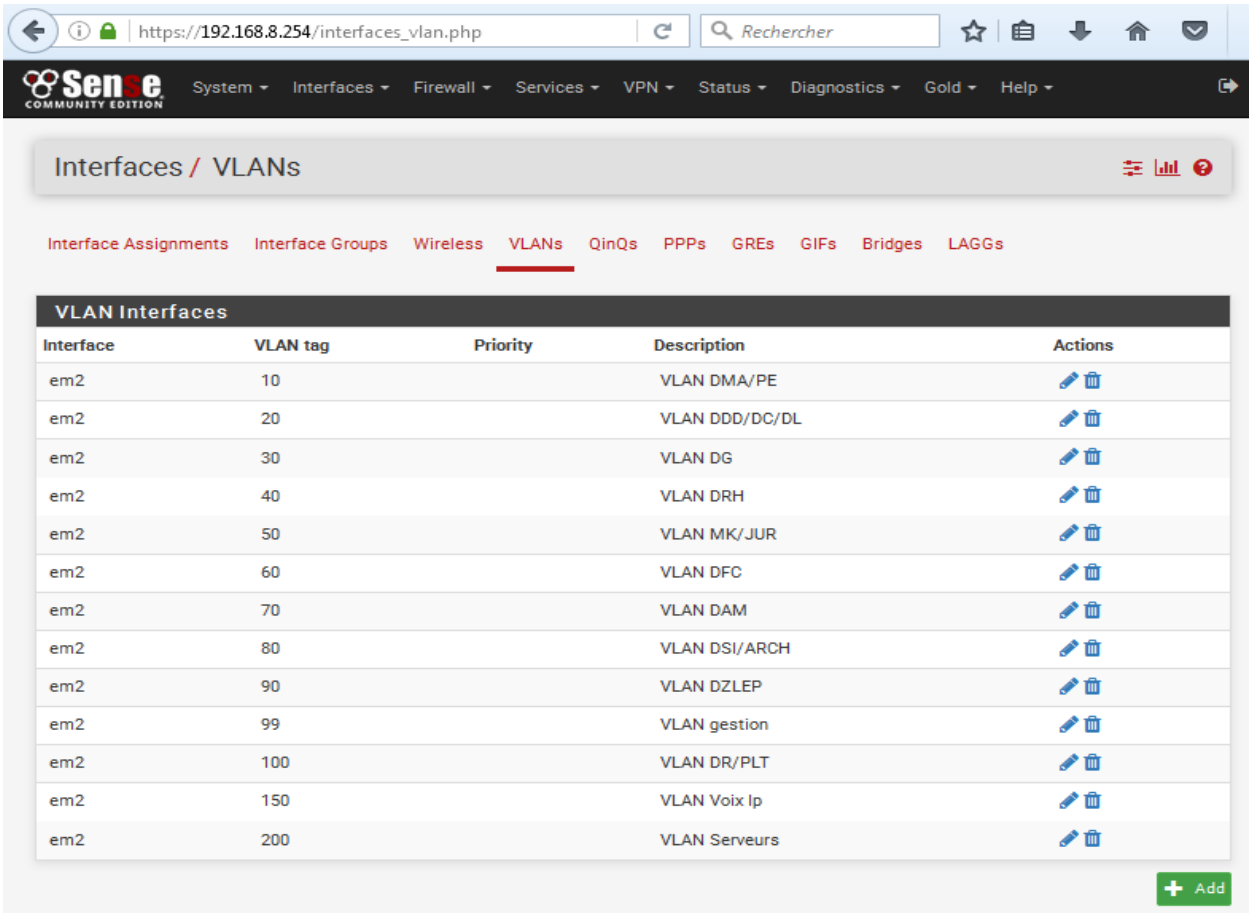


Figure 4.20 : Interface de plusieurs vlans

Afin de configurer nos VLANs, nous devons maintenant associer ces interfaces virtuelles à des interfaces logiques.
Pour cela, nous retournons dans l'onglet "Interface assignments", puis nous cliquons sur l'icône en forme de "+Add" se trouvant un bas à droite 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 créée précédemment :

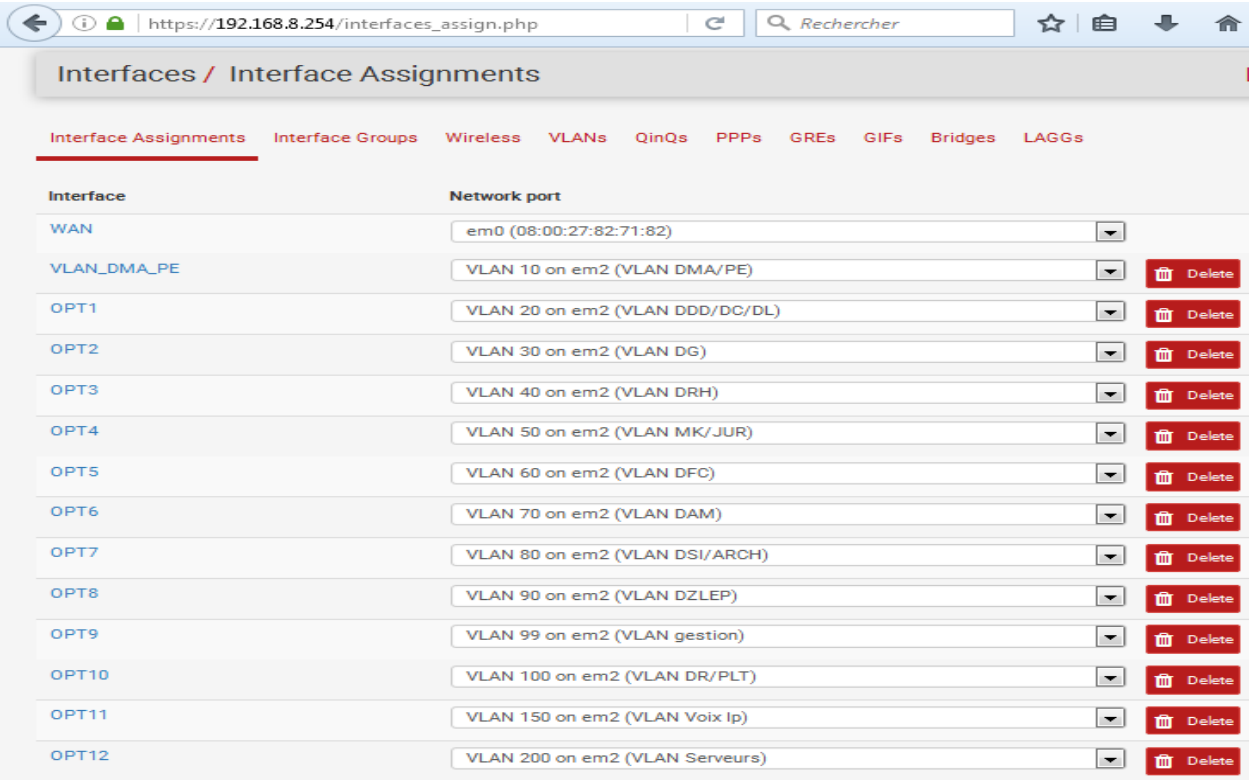


Figure 4.21 : Interface configuration ensemble des vlans

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

1. **Enable Interface** : cocher 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 :

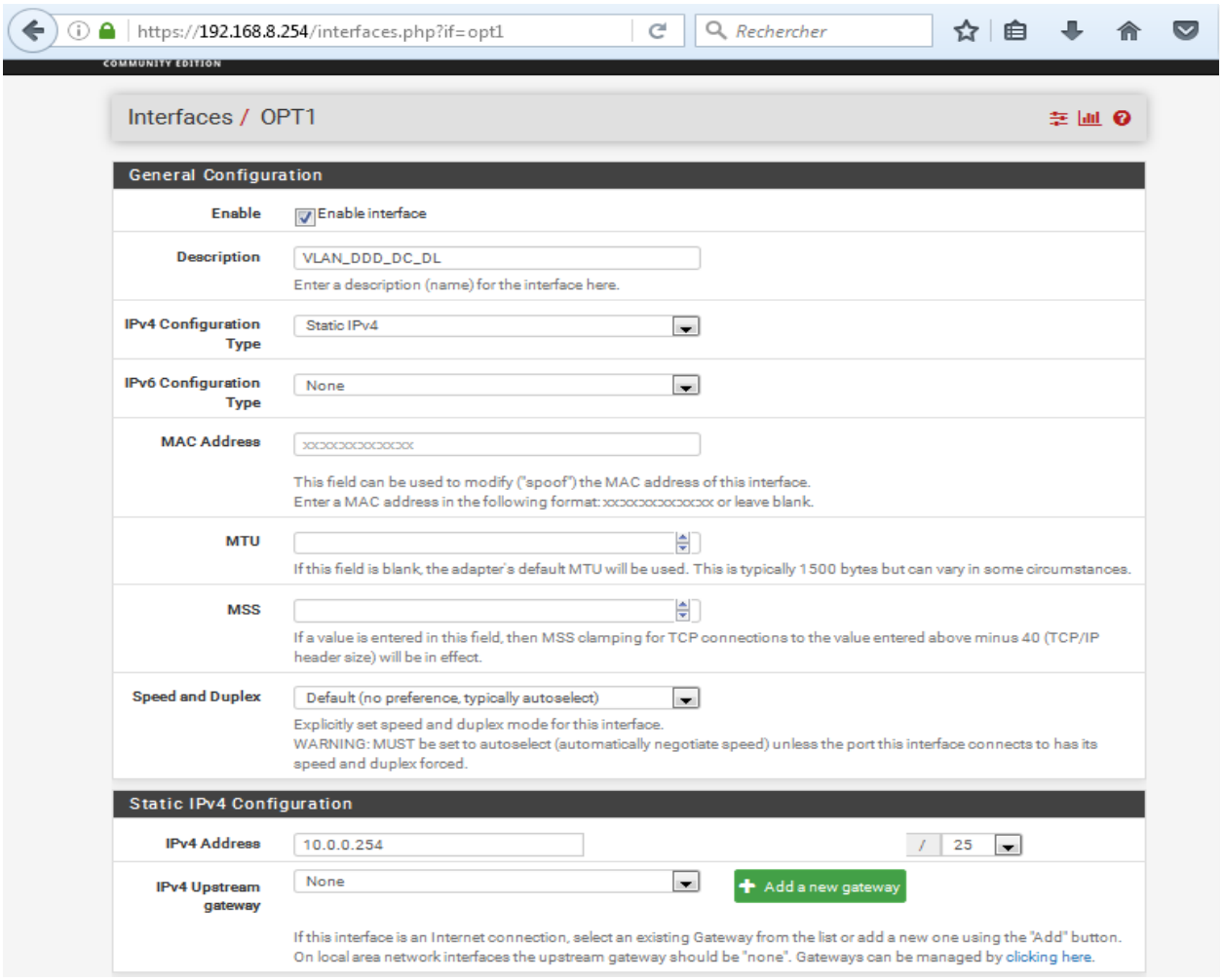


Figure 4.22 : Interface configuration de vlan

4.3.2.2 Inter-VLANs routage avec pfSense

Enfin, nous créons des règles de firewall sur notre nouvelle interfaces logique ("VLAN_DFC/VLAN_DRH/….") afin d'autoriser le trafic.

Règles de pare-feu :

Pour commencer, nous allons dans le menu « Firewall » : « Rules »

Puis, nous nous rendons dans l'onglet "VLAN_DFC" et nous créons des règles d'autorisation pour les deux entrants et sortants sur l'interface "**VLAN_DFC**" pour activer le routage Inter-VLAN avec l'interface "VLAN_DRH".

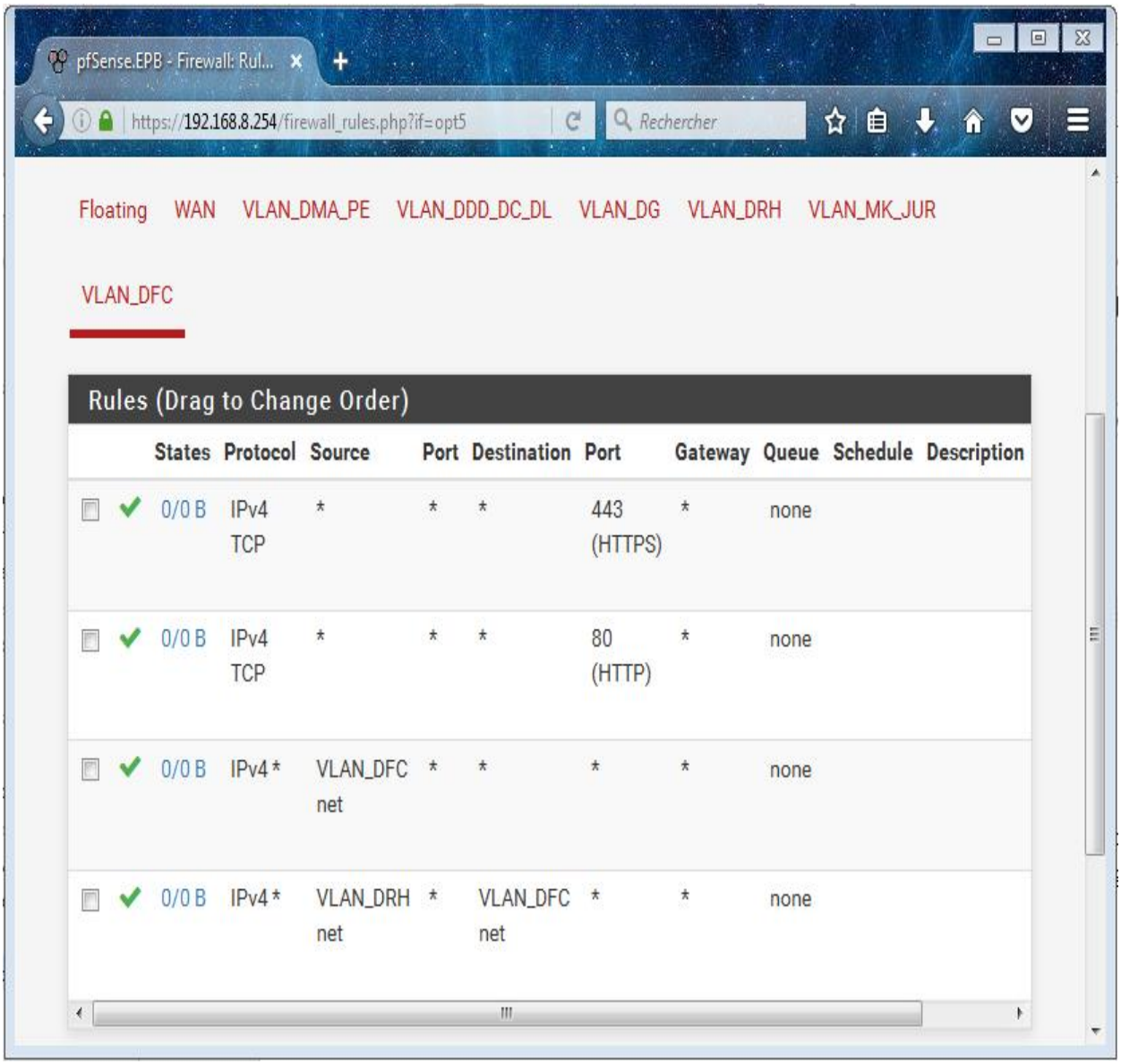


Figure 4.23 : Interface d'activation de routage inter-vlan entre VLAN_DFC et VLAN_DRH

Après avoir entamé la configuration de pfSense, il reste à procéder à une partie de notre topologie sous GNS3 pour faire simuler pfsense avec des machines virtuelles (chaque machine est attribuée à un vlan) et tester le routage inter-vlan sous pfsense.

La figure suivante illustre ce procédé :

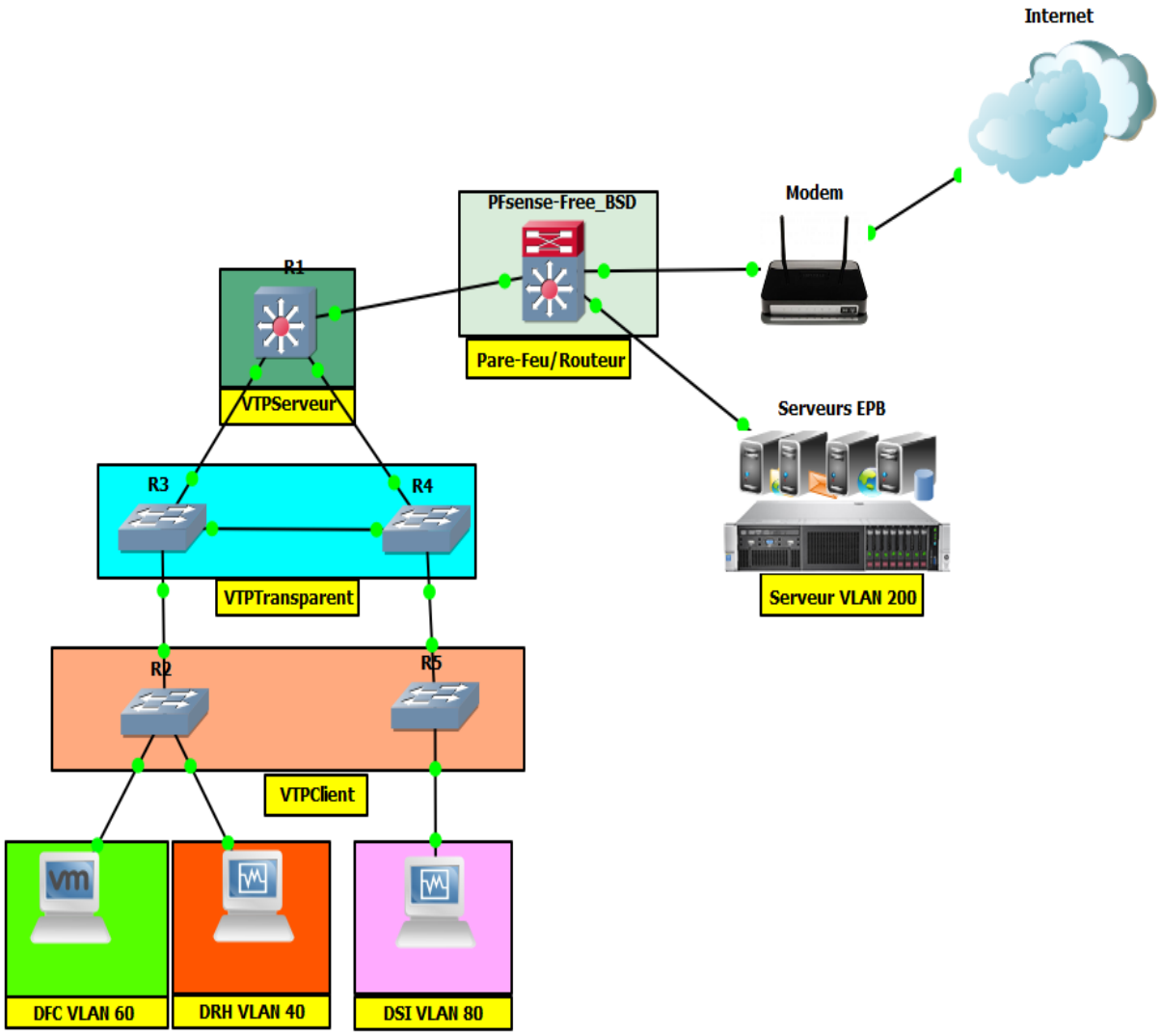


Figure 4.24 : une partie de notre topologie sous GNS3

•Les tests (les pings) :

Après activation le routage inter-vlan entre VLAN_DFC et VLAN_DRH, on va tester la communication entre les deux VLAN.
On va faire un ping d'une machine VLAN_DFC vers une machine VLAN_DRH

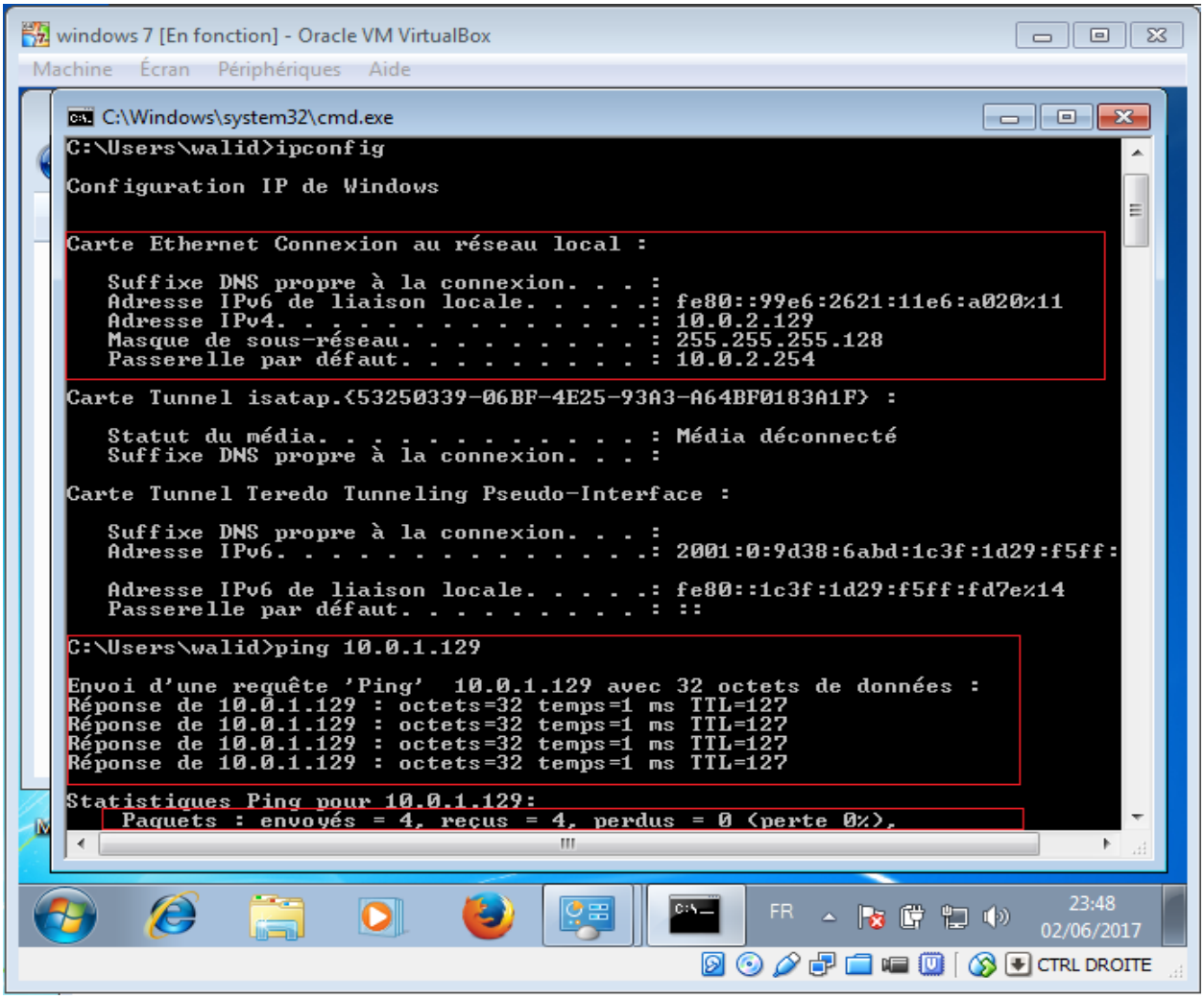


Figure 4.25 : Ping réussi entre PC vlan_DFC et PC vlan_DRH

Ce résultat montre que les machines du VLAN_DFC communiquent avec les machines du VLAN_DRH.

Maintenant on va désactiver le routage inter-vlan entre VLAN_DFC et VLAN_DRH,

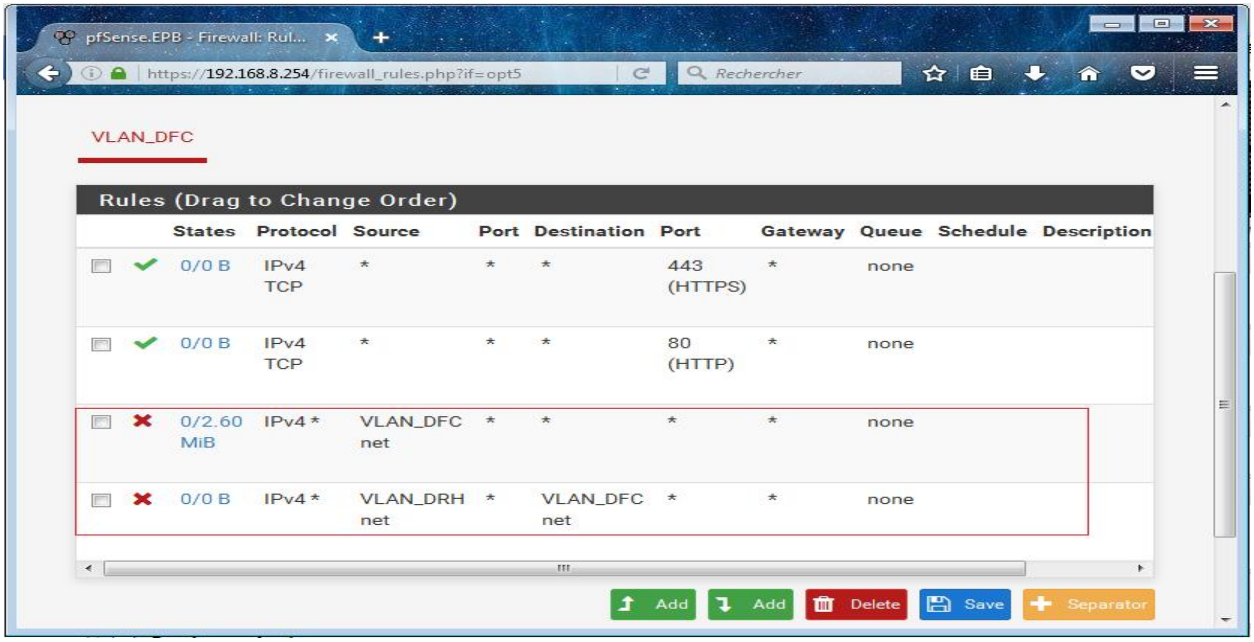


Figure 4.26 : désactivation de routage inter-vlan entre VLAN_DFC et VLAN_DRH

Maintenant en vas faire un Ping d'une machine VLAN_DFC vers une machine VLAN_DRH

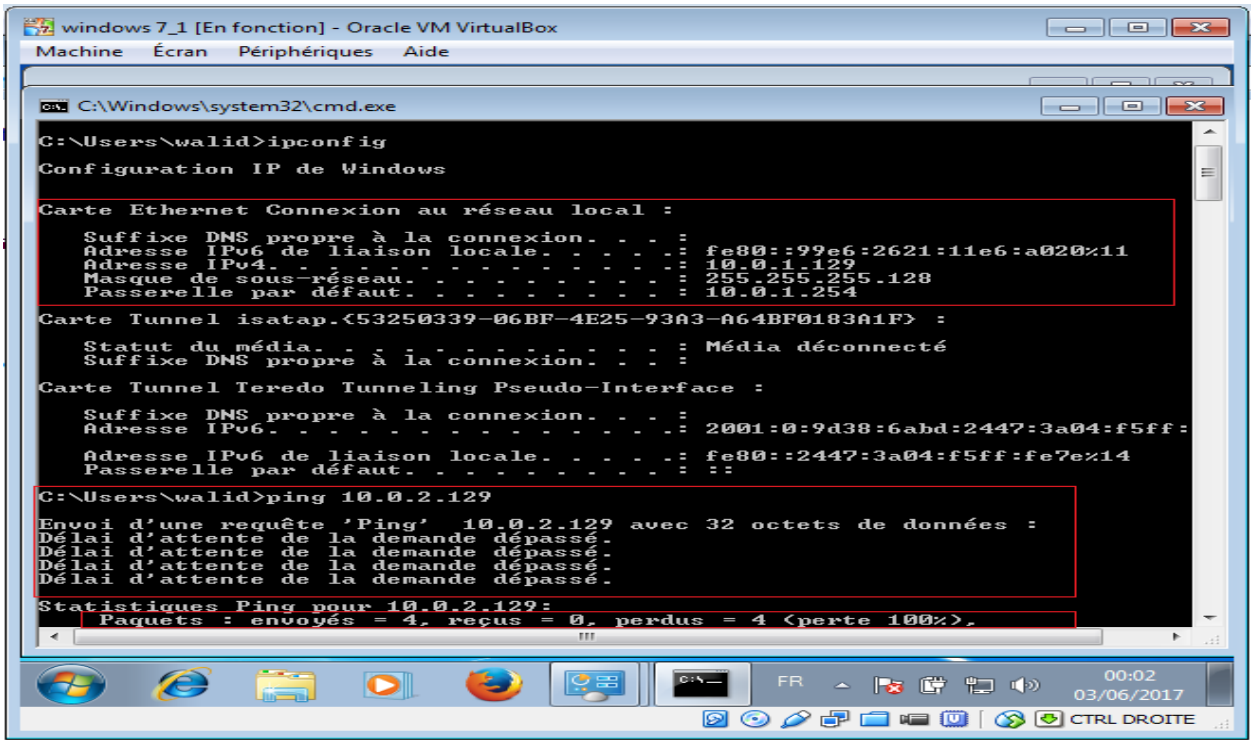


Figure 4.27 : Ping échoue entre PC vlan_DRH et PC vlan_DFC

Ce résultat montre que les machines du VLAN_DRH il ne peut pas communique avec les machines du VLAN_DFC, la mêmechose pour tous les autres vlan qu'on a filtrés, sa montre que notre configuration a réussie.

4.4 Conclusion

Au cours de ce chapitre, nous avons pu décrire la procédure de configuration concernant les VLANs et le pare-feu (pfsense) sur le réseau local et le réseau Internet.

En effet, les résultats obtenus montrent que la segmentation du réseau local en (13) VLANs a offert une sécurisation des données échangées entre les différentes directions de l'entreprise EPB, une amélioration de la gestion l'attribution d'adresses IP, ainsi qu'une meilleure organisation du réseau sans avoir eu recours au réaménagement des équipements.
Pfsense permet de filtrer et contrôler les accès entrant et sortant et protéger l'environnement (vis à vis de l'extérieur et de l'intérieur). Ceci dit, il convient de mentionner que ces configurations restent « théoriques », car leur réalisation au sein de l'entreprise n'a pas encore pris place. Néanmoins, notre vérification et mise en œuvre à l'aide des simulateurs Packet Tracer et GNS3, confirment la fiabilité et l'efficacité des résultats obtenus.

Conclusion générale

Le réseau informatique permet aux entreprises de centraliser ses données, de travailler en équipe de manière productive et limiter les impressions papiers pour le transfert d'informations. En cas de problème de réseau, des ingénieurs des systèmes réseaux et sécurités apportent des solutions qui permettent d'améliorer la performance et la productivité de l'entreprise.

L'étude que nous avons menée au sein de l'entreprise portuaire de la wilaya de Béjaia, nous a conduit à bien cerner les besoins de cette dernière et proposer un système de sécurité à déployer afin d'assurer des services sécurisés au sein de l'entreprise.

1. La mise en place du Réseau Local Virtuel (VLAN), nous a permis de segmenter le réseau d'EPB.
2. La mise en place du pare-feu (pfSense) offre une solution complète de routage, filtrage e*t* de contrôle les accès entrant et sortant et protéger l'environnement (vis à vis de l'extérieur et de l'intérieur).

Ce travail de conception assez importante nécessitait de comprendre le fonctionnement des équipements **Cisco catalyst série 2960, Cisco catalyst série 3560** et leur fonctionnalité et connaitre les différents protocoles à implémenter, afin de résoudre la problématique de lenteur du réseau.

Avec nos connaissances à la fois théoriques et pratiques acquises pendant notre cursus universitaire et associées à la pratique de l'entreprise et notre volonté de relever le défi de proposer une solution pertinente et optimale et afin de satisfaire les besoins de l'ensemble des utilisateurs d'EPB en ce qui concerne l'utilisation convenable des services du réseau, nous avons pu implémenter la solution du VLAN permettant ainsi une amélioration considérable des performances du réseau.

Notre travail aussi nous a permis de réaliser une proposition qui pourra aider l'EPB où nous avons effectué notre stage pratique, il nous a également permis d'améliorer nos connaissances théoriques et pratiques acquises et aussi de nous adapter au monde professionnel.

En conclusion, nous pensons que la mise en œuvre de cette nouvelle architecture réseau est d'une importance capitale pour le bon fonctionnement du réseau informatique de l'EPB. Évolutive, cette architecture pourra faire l'objet d'amélioration et de modification en fonction des besoins futurs de la structure.

Bibliographie

[1] https://www.portdebejaia.dz/index.php/fr/presentation.

[2] Plan du développement informatique Document Interne de l'EPB, 2016.

[3] Claude Servin, Jean pierre Arnaud, Réseaux et télécoms, 2 ème édition,2006

[4] Jacques PHILIPP, l'Architecture des Réseaux TCP/IP ,1er édition, juin 2006.

[5] José DORDOIGNE, Philipe ATELIN, Réseaux informatiques, Notions fondamentales, 3ème édition, Edition ENI, 2006.

[6] http://univers.du.pc.free.fr/pages/c_cartereseau.php , Réseaux informatiques.

[7] Cours CISCO CCNA1, chapitre1, les périphériques finaux. netacad, 2015.

[8] Jean-Luc MONTAGNER, Réseau d'entreprise par la pratique, Edition EYROLLES, juin 2006.

[9] http://hautrive.free.fr/reseaux/architectures/topologie-des-reseaux.html

[10] http://www.courstechinfo.be/Reseaux/Topologie.html, Topologie des réseaux locaux

[11] Joe Habraken et Matt Hayden, les réseaux, 3ème édition, 17 MAI 2005.

[12] http://www.courstechinfo.be/Reseaux/Classif.html, Classification des réseaux selon leur étendue.

[13] CISCO : Djillali SEBA, Installation, configuration et maintenance de réseaux, Edition ENI, 2003.

[14] Cours CISCO CCNA1, apprendre les différendes couche réseaux,Modéles OSI et TCP/IP. netacad, 2015.

[15] Solange GHERNAOUTI, Sécurité Informatique et Réseaux, 4ème édition, Editeur DUNOD, Septembre 2013.

[16] Jérôme DEL DUCA, Alexandre PLANCHE, La sécurité Informatique en Mode Projet, Edition ENI, 01/03/2017.

[17] GILBERT HELD, Les réseaux locaux virtuels, 1998

[18] PEREIRA Philippe et CAZIN Jerome, Sécurité réseau & VLANs, 2013-2014.

[19] P. Sicard - Cours Réseaux-VLAN, 24/09/ 2011.

[20] http:// Memoire Online1 - Etude et optimisation du réseau local de inova si - Toussaint KOUASSI.html

[21] REUSSIRSONCCANA.FR/VTP-VLAN-TRUNKING-PROTOCOL/

[22] HTTP://REUSSIRSONCCNA.FR/TRUNK-802-1Q-ET-ISL-CE-QUIL-FAUT-SAVOIR-POUR-LE-CCNA/

[23] http://www.zardoc.com/les_pare_feu.html, sécurité

[24] https://www.generation-nt.com/firewall-pare-feu-securite-informatique-guide-explication-article-24842-7.html

[25] D. Brent Chapman, Elisabeth D. Wwicky 'La sécurité sur Internet Firewalls' O'Reilly , 1996.

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

[27] ISMAIL RACHDAOUI, ANAS ABOU EL KALAM, pfsense free bsd , Génie Réseaux et Télécommunications ENSA Marrakech 2013

ANNEXE

Annexe A

A.1 Exploitation de l'interface de Packet Tracer :

Lorsque Packet Tracer démarre, il présente une vue logique du réseau en mode temps réel. La figure suivra montre un aperçu général de l'interface de Packet Tracer :

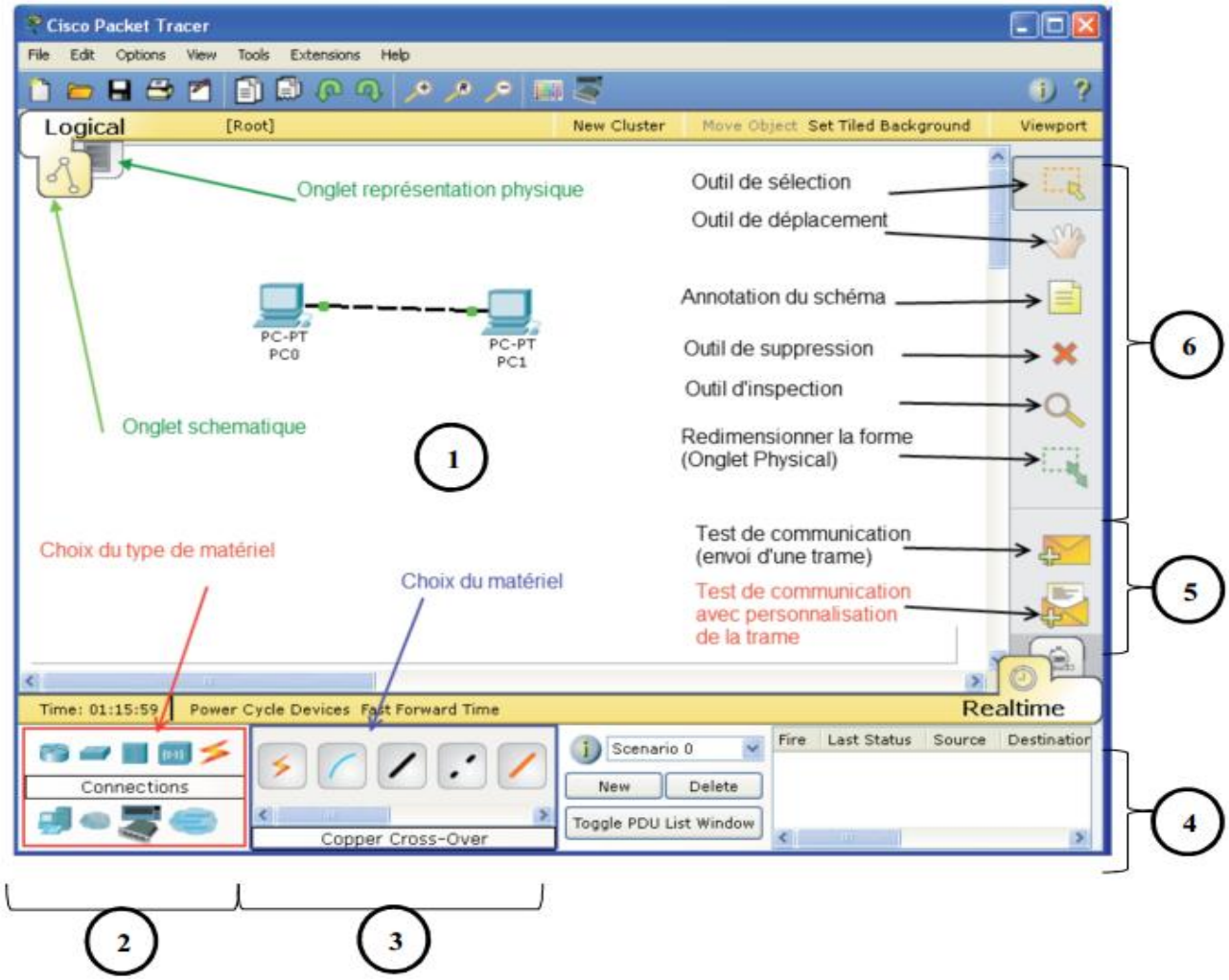


Figure A.1 : L'interface du simulateur Packet Tracer

1 : elle représente le lieu de travail logique. Il s'agit de la zone vierge étendue dans l'laquelle des périphériques peuvent être placés et connectés.
2 : représente la zone ou les équipements sont regroupés en catégories accessibles pour les utilisateurs, elle contient donc des symboles représentent des groupes de périphériques.
3 : une fois la catégorie sélectionnées dans la zone (2), le type d'équipement peut être transmit a la zone (3), le nom du groupe de périphérique d'affiche, il reste qu'à choisir ce dont on a besoin.
4 : permet de passer du mode temps réel au mode simulation.
5 : permet d'ajouter des indications dans le réseau.
6 : cette zone contient un ensemble d'outils :

- **Select** : pour déplacer ou éditer des équipements ;
- **Move layout** : permet de déplacer le plan de travail ;

Annexe A

- **Place note** : place des notes sur le réseau ;
- **Delete** : supprime un équipement ou une note ;
- **Inspect** : permet d'ouvrir une fenêtre d'inspection sur un équipement.

A.2 Construire un réseau :

Pour construire un réseau, l'utilisateur doit faire un choix parmi les 8 catégories proposées par Packet Tracer : les routeurs, les switches, les hubs, les équipements sans-fil, les connexions, les équipements dits terminaux (ordinateurs, serveurs), des équipements personnalisés et enfin, une connexion multiutilisateurs.

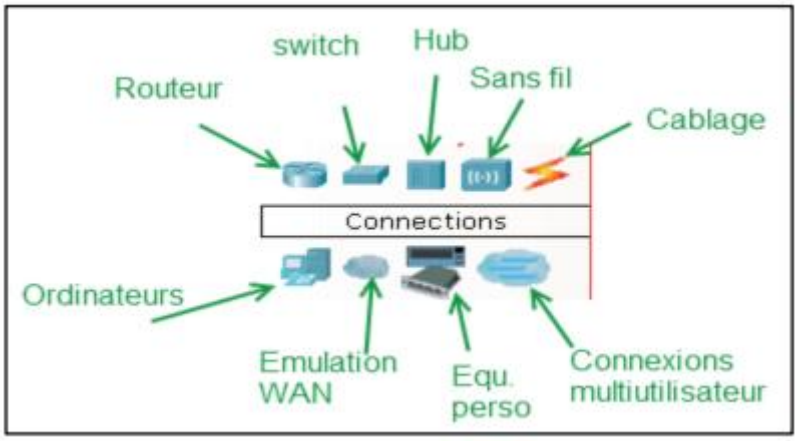


Figure A.2 : Types d'équipements

Lorsqu'une catégorie est sélectionnée, l'utilisateur a alors le choix entre plusieurs équipements différents. Pour ajouter un équipement, il suffit de cliquer dessus puis de cliquer à l'endroit où on veut le mettre. Ensuite on devrait relier deux équipements, il faut donc choisir la catégorie « connections » puis cliquer sur la connexion désirée.

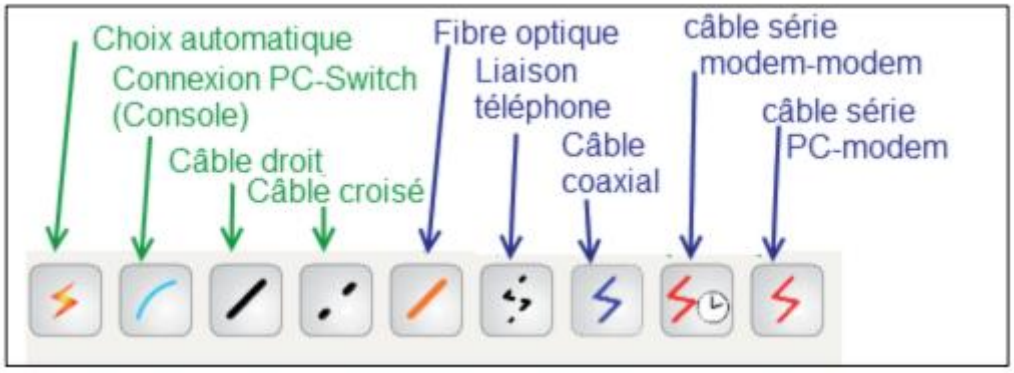


Figure A.3 : Les différentes connexions proposées

Pour les liaisons, voilà les types de câble réseau qu'il faut utiliser :

- **Câble droits :**

PC à Hub	PC à Switch	Switch à Routeur

Annexe A

• **Câbles croisés :**

Switch à Switch	Hub à Hub	Routeur à Routeur
PC à PC	Hub à Switch	PC à Routeur

Pour les liaisons séries entres routeurs, il faudra rajouter le module WIC 2T au routeur. Ce module permet de rajouter une interface série afin de relier deux réseaux. Une des deux extrémités doit fournir une horloge. Pour ajouter ce type d'interface, il faut utiliser la souris en « glisser/déposer » dans un slot libre. Il faut aussi penser à éteindre le module (en cliquer sur l'interrupteur du module).

A.3 Configuration d'un équipement :

L'lorsqu'on veut ajouter un ordinateur (PC-PT), on a la possibilité de le configurer en cliquant dessus, une fois ajouté dans le réseau. On a donc une fenêtre qui s'ouvre et qui contient 3 onglets : Physical (aperçu réel de la machine et de ses modules), Config (configuration passerelle, DNS et adresse IP) et Desktop (ligne de commande ou navigateur web).

Dans l'onglet config, il est possible de configurer la passerelle par défaut, ainsi que l'adresse du serveur DNS. Il est possible aussi de configurer l'adresse IP et le masque de sous-réseau.

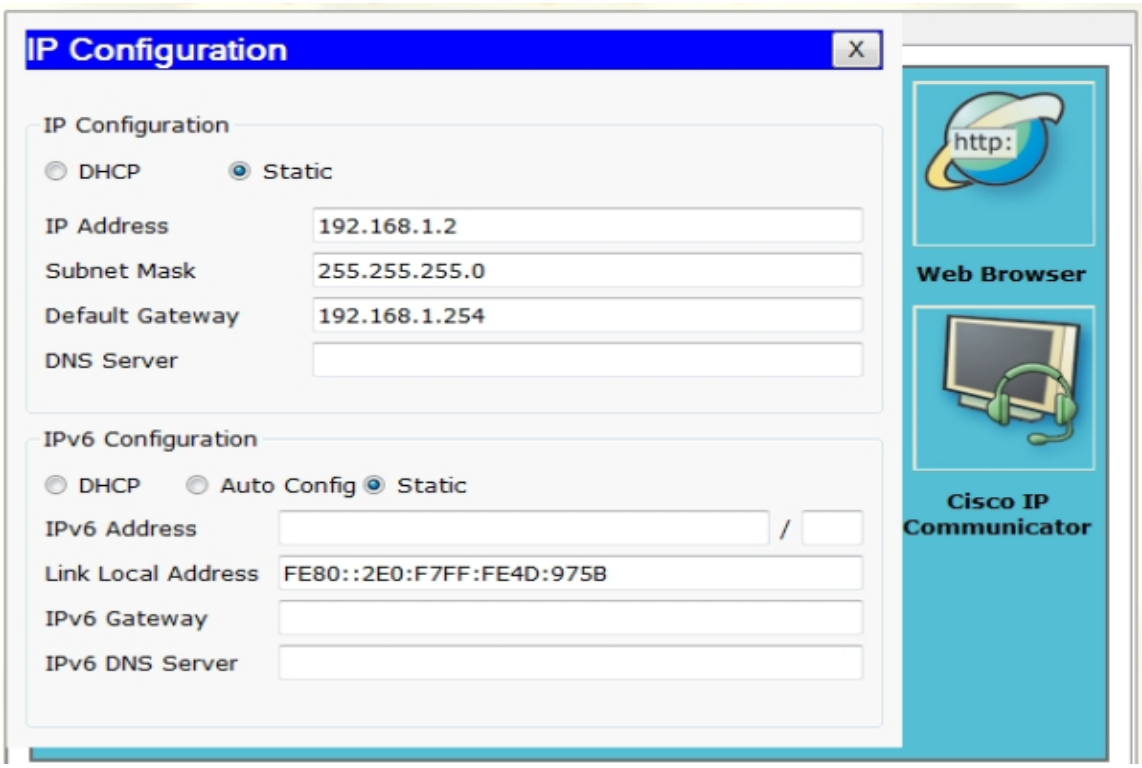


Figure A.4 : Configuration des machines

A.5 Mode simulation :

Une fois qu'on a créé le réseau il est maintenant prêt à fonctionner, il est possible de passer

du mode Realtime en mode simulation, ce qui permet de visualiser tous les messages échanges dans le réseau.

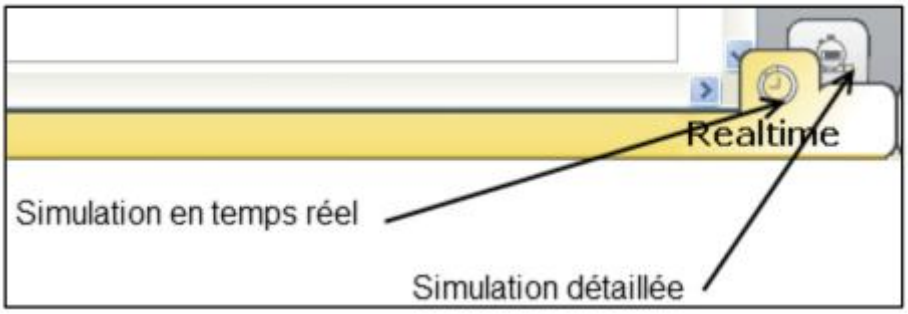


Figure A.5 : Passage entre le mode simulation e mode realtime

En mode simulation, la fenêtre principale est fractionnée en deux, la partie de droite permettant de gérer le mode simulation : exécution pas-à-pas, vitesse de simulateur, protocoles visible.

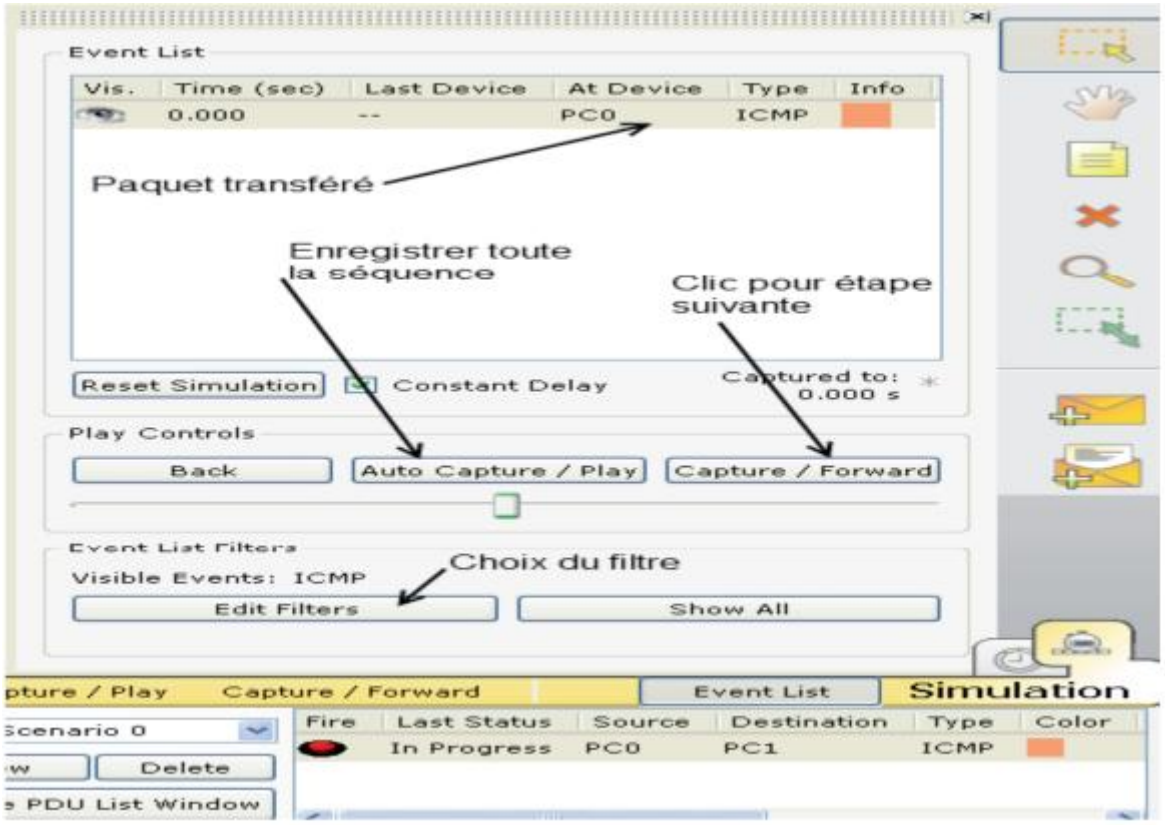


Figure A.6 : La partie simulation

ANNEXE B

INSTALLATION DE PARE-FEU (PFSENSE)

Installation et premiers paramétrages de Pfsense

Installation de PfSense

Ce document traite de l'installation de la version 2.3.4 de Pfsense (la dernière à la date de rédaction)
sur une nouvelle machine.

Tout d'abord, il faut se rendre sur le site http://www.pfsense.org afin de récupérer les images ISO pour installer PfSense :

pfSense-2.3.4-RELEASE-i386.iso.gz pour les Pcs anciens avec des processeurs ne gérant pas le 64 bits

pfSense-2.3.4-RELEASE-amd64.iso.gz pour les Pcs avec des processeurs 64 bits

Lancer installation de pfsense

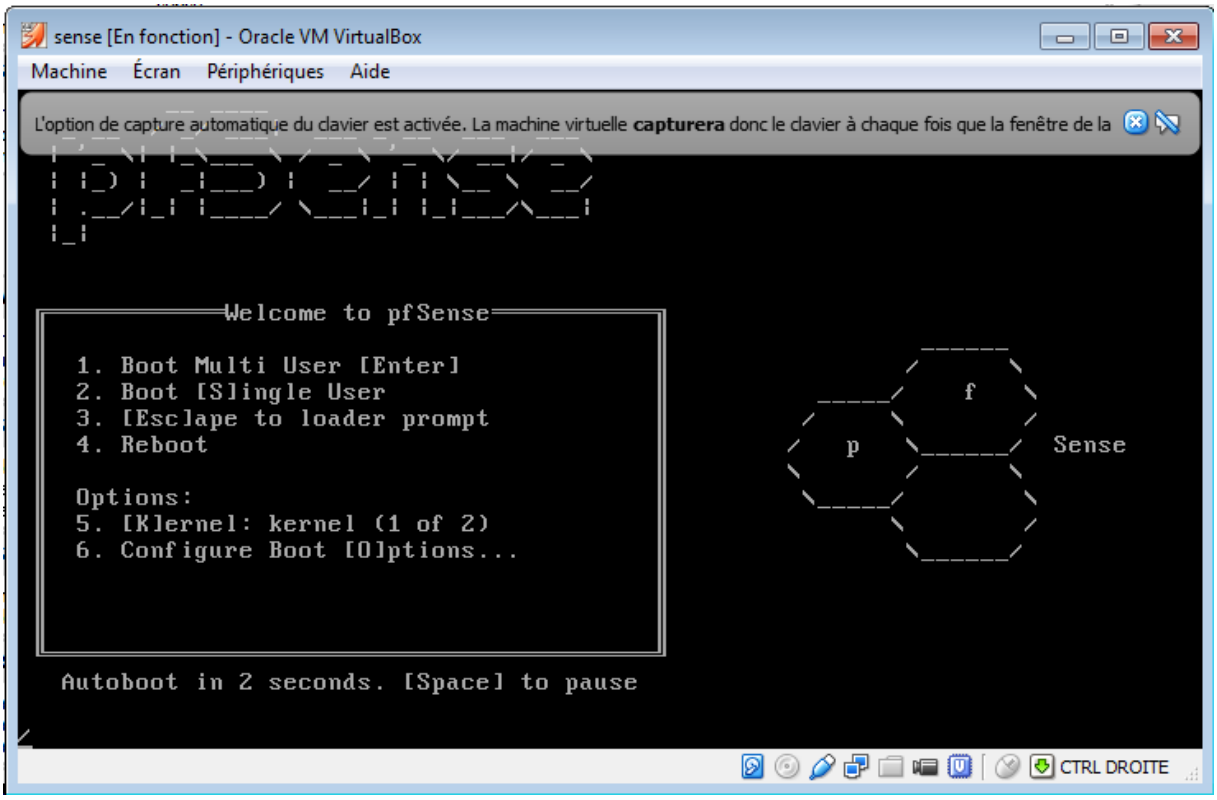


Figure 1 : interface de démarrage sur l'option par défaut

Pressez « Entrée » pour démarrer sur l'option par défaut (1)

Laissez-le pour Autoboot et vous devriez voir l'écran suivant dans un instant.

ANNEXE B

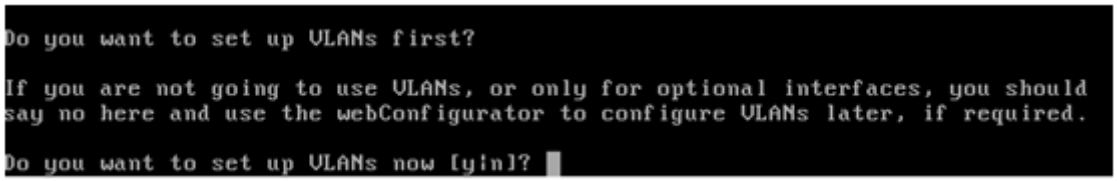


Figure 2 : interface de configuration de vlan en mode commande

Lorsqu'il déclenche une configuration VLAN, tapez "n" car en va créer les vlans avec interface web et appuyez sur Entrée.

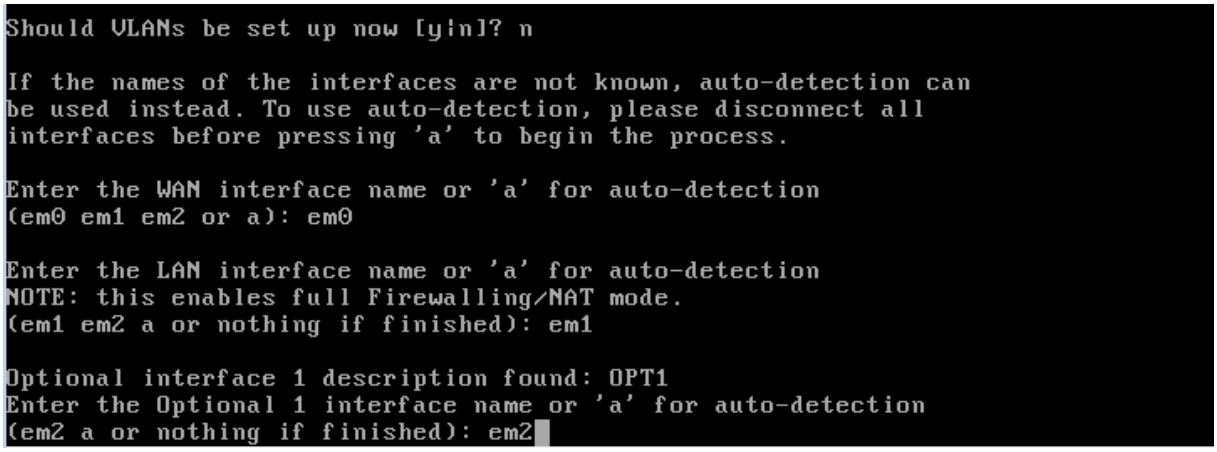


Figure 3 : interface configuration des cartes réseaux

Ensuite, nous serons invités à entrer des noms d'interface pour les trois adaptateurs que nous avons définis.

Pour l'interface WAN, spécifiez "em0" et pour l'interface LAN, spécifiez "em1" et, spécifiez "em2" et pour l'interface des VLANs comme indiqué dans la figure ci-dessus.

Nous pouvons observer clairement dans la note ci-dessus que le réseau interne sera derrière le NAT.

Après avoir rempli les détails requis, appuyez sur Entrée.

Nous devrions voir l'écran suivant pour demander la confirmation de l'utilisateur. Tapez "Y" et appuyez sur Entrée.

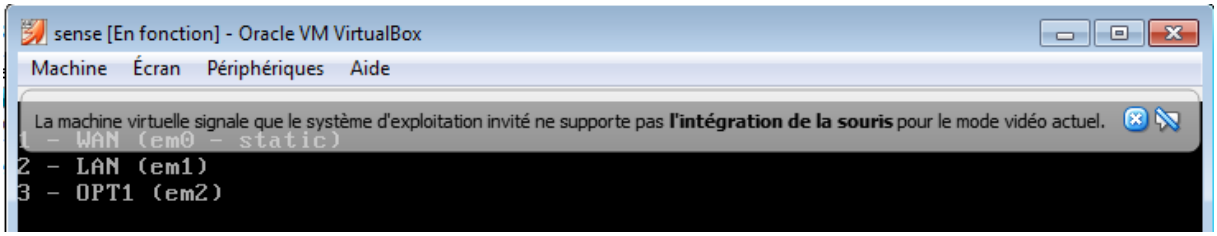


Figure 4 : attribution des cartes réseaux aux interfaces LAN et WAN

ANNEXE B

L'étape ci-dessus crée automatiquement une adresse IP pour l'interface WAN. Ceci est illustré dans la figure ci-dessous.

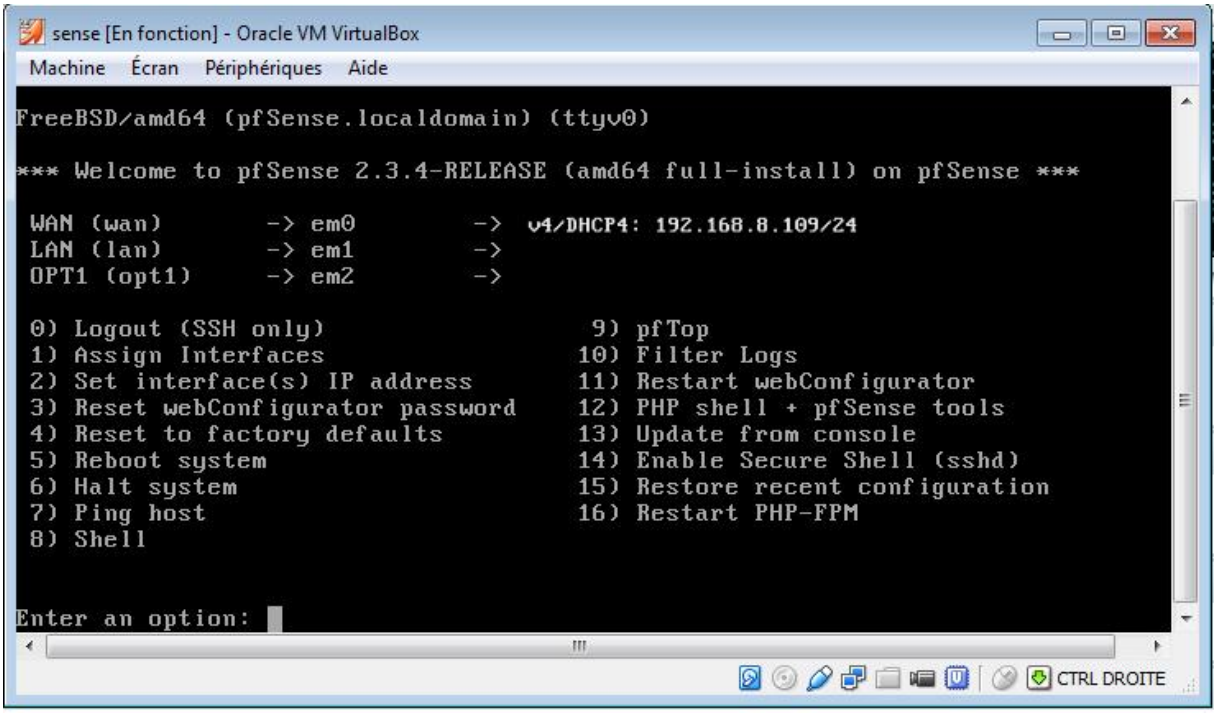


Figure 5 : interface de création automatique une adresse IP pour WAN

Comme on peut le voir sur la figure ci-dessus, pfSense est assigné avec 192.168.8.109 sur l'interface em0.

Maintenant, nous devons configurer interface WAN et la passerelle statiquement.

Pour ce faire, nous allons configurer une adresse IP pour l'interface em0.

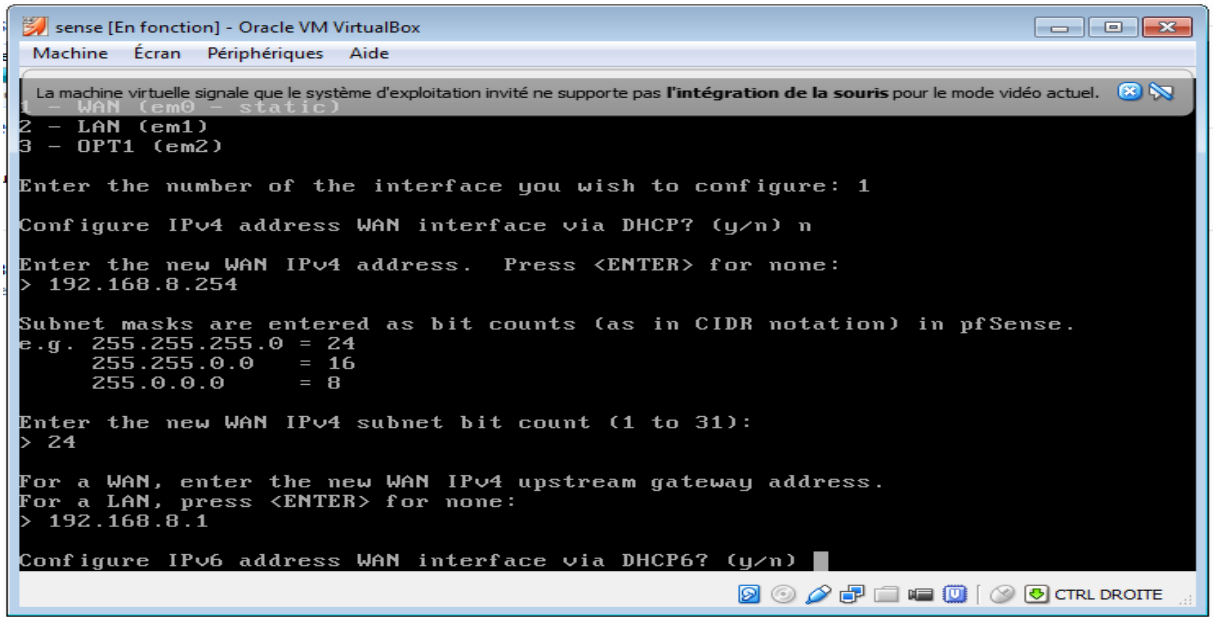


Figure 6 : Configuration interface WAN et passerelle statiquement

ANNEXE B

Dans l'écran ci-dessus, entrez simplement 2 pour sélectionner "Affecter les interfaces". Ensuite, nous devrions voir les interfaces disponibles. Comme nous allons configurer

première interface, nous allons choisir "1". Cela devrait nous permettre de configurer l'interface WAN, qui est em0.

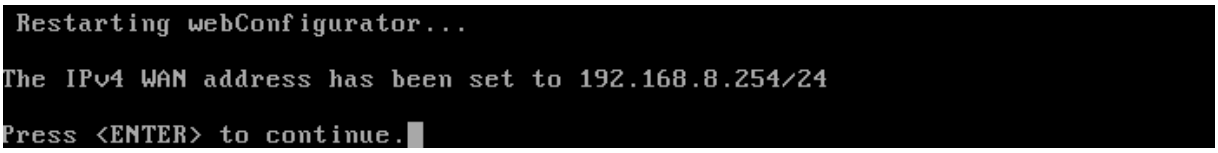
On nous demandera alors l'adresse IP du WAN.
Dans mon cas, je l'ai fourni 192.168.8.254.

On nous demandera le nombre de bits du masque de sous-réseau.

Dans mon cas :24 bits

Figure 7 : interface pour configurer le WEBconfigurator

Une fois terminé, appuyez sur Entrée et tapez "Y" à nouveau pour configurer Webconfigurator pour la configuration pfSense à partir d'une interface graphique, puis appuyez sur Entrée.



Nous devrions voir l'écran ci-dessus avec l'URL où nous pouvons accéder à l'interface utilisateur graphique pour la configuration de pfSense.

Enfin, appuyez sur Entrée pour revenir à l'interface de configuration de la ligne de commande, qui apparaît lors du démarrage de pfSense.

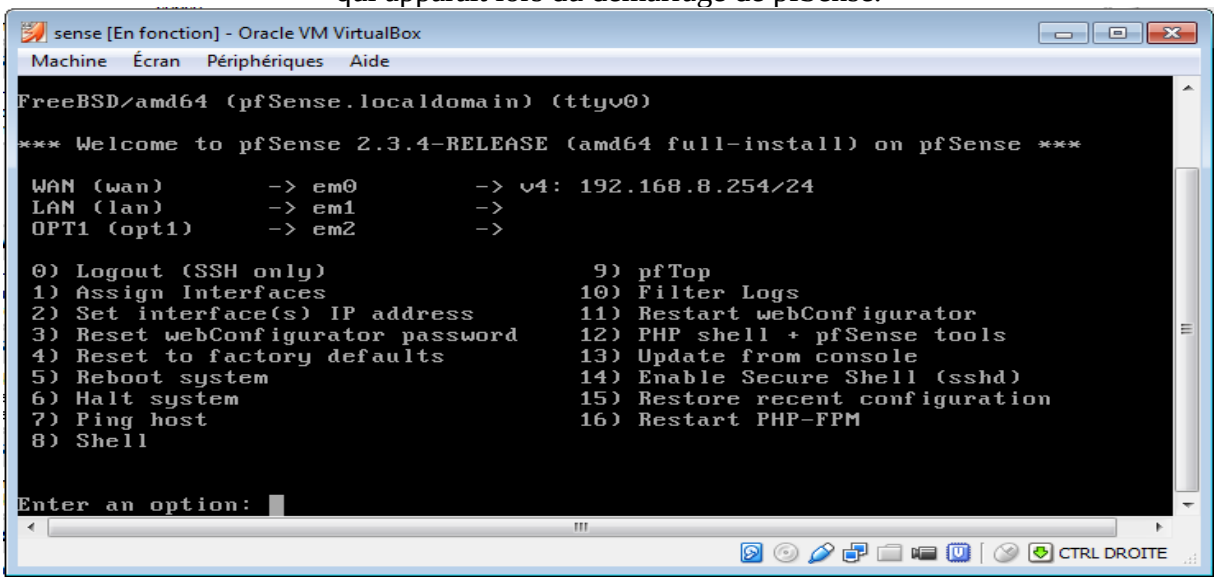


Figure 8 : pour se connecter a interface de configuration on utilisera l'adresse IP de WAN

ANNEXE B

Pour se connecter à l'interface de configuration on utilisera l'adresse ip de l'interface WAN http://192.168.8.254, le couple login/pass par défaut est admin/pfsense

RÉSUMÉ

La virtualisation de réseau permet de combiner des ressources matérielles et logicielles dans une seule unité administrative. L'objectif de notre travail consiste à implémenter une solution des VLANs et un pare-feu afin de segmenter et sécuriser le réseau intranet de l'entreprise portuaire de Bejaia « EPB ». Nous avons choisie de simuler avec PACKET TRACER et GNS 3, afin de fournir aux différentes directions de l'EPB un partage efficace en utilisant le VTP qui permet de gérer de façon centralisé les VLANs et pfsense qui permet de faire un routage inter-vlans et le filtrage trafic réseau.

Mots clés :

VLAN, pfsense, VTP, PACKET TRACER, gns3

ABSTRACT

The virtualization of the network consists in combining material and software resources in a single administrative unit. The objective of our work consists in implementing a solution by using the virtual connection to segment and reassure the intranet network of the harbour company of Bejaia "EPB". We chose the simulate with PACKET TRACER and GNS3, to supply in the various directions managements of the EPB and effective division sharing by using the VTPs who allows to manage in away centralized the VLANs, and pfsense who allows to do routing inter-VLANs and network traffic filtering.

Keywords:

VLAN, pfsense, VTP, PACKET TRACER, gns3.