**République Algérienne Démocratique et Populaire**

**Ministère de l'Enseignement Supérieur et de la Recherche Scientifique**

**Université Abderrahmane Mira de Béjaia**


*Faculté des sciences Exactes*

*Département d'Informatique*

**Mémoire de fin de cycle**

En vue de l'obtention du diplôme de Master Professionnel en Informatique

**Option :** *Administration et Sécurité des Réseaux*

**Thème**

# Proposition d'une configuration sécurisée d'un réseau local avec les VLANs Cas d'étude: Entreprise Bejaia Mediteranean Terminal (*BMT*)

**Réalisé par:**

**M$^{elle}$ DAHMANI Hanane**

**M$^{elle}$ YAKOUBEN Roza**

Devant le jury composé de :

| | | |
|---|---|---|
| Président | M$^{r}$ | AISSANI Sofiane |
| Examinateur | M$^{r}$ | SALHI Nadir |
| Examinatrice | M$^{elle}$ | BENNAI Sofia |
| Promoteur | M$^{r}$ | BAADACHE A/Rahmane |
| Invité | M$^{r}$ | BEN ALI Lyes |

*Année universitaire*

**2016/2017**

# *Remerciements*

*Nous tennons à remercier* ***ALLAH*** *qui nous a donné la force, le courage pour réaliser ce modeste travail et qui nous a mis dans nos chemins les bonnes personnes et nous a confié aux bonnes mains.*

*Un grand merci à toutes nos familles pour leur préoccupation te le souci qu'ils se sont fais pour nous, leur encouragement et leur suivi, avec patience, du déroulement de notre projet.*

*Nous tennons en premier lieu à exprimer nos plus vifs remerciements à Monsieur* ***A.BAADACHE****, notre promoteur pour son aide, sa patience, ses conseils, ses encouragements, et sa disponibilité. Nous adressons nos profondes gratitudes et nos remerciements les plus vifs à Monsieur* ***S.AISSANI****, pour nous avoir fait l'honneur de présider le jury de cette soutenance.*

*Nous tennons à remercier également Monsieur* ***N.SALHI*** *et Mademoiselle* ***S.BENNAI****, qui ont accepté d'examiner ce travail.*

*Nous tennons à remercier également Monsieur* ***L.BEN ALI*** *notre encadreur au sein de l'entreprise BMT pour son aide, sa patience, ces conseils et sa disponibilité.*

*Nous tennons à exprimer nos plus sincères remerciements à tous les membres de la faculté des sciences exactes en général et aux membres du département d'Informatique en particulier, ainsi que tous les enseignants pour les peines et les efforts qu'ils nous ont donné durant notre formation.*

# Dédicaces

Je dédie ce modeste travail à :

*Mes très chers parents en témoignage de ma reconnaissance envers le soutien, les sacrifies et tous les efforts qu'ils ont fait pour mon éducation ainsi ma formation.*

*Mes chers frères, ma chère sœur Khaoula.*

*Mon cher fiancé Nadjim et toute ma futur famille.*

*Mes cousins et cousines.*

*Tous mes enseignants.*

*Ma binôme et sa famille.*

*Mes amis.*

$\mathcal{HANANE}$

# Dédicaces

Je dédie ce modeste travail à :

*Mes très chers parents en témoignage de ma reconnaissance envers le soutien, les sacrifies et tous les efforts qu'ils ont fait pour mon éducation ainsi ma formation.*

*Mes chers frères, mes chères sœurs.*

*Mes beaux-frères et mes belles-sœurs.*

*Mes neveux et ma nièce.*

*Mohamed et mes amis.*

*Tous mes enseignants.*

*Ma binôme et sa famille.*

*Mes collègues du travail.*

*ROZA*

# Table des matières

# Liste des Figures

# Introduction

L'utilisation croissante des réseaux informatiques en entreprise et leur interconnexion à internet font émerger aujourd'hui de nouvelles préoccupations sécuritaires. La majorité des entreprises ne peut plus ignorer désormais d'intégrer la sécurité informatique, et en particulier celle des réseaux, dans leur stratégie de développement si elles ne veulent pas risquer de voir leur outil de travail perturbé par une attaque ciblée qui est généralisée véhiculée par le réseau mondial ou par leur propre réseau local.

Ainsi, les administrateurs réseaux, les responsables sécurité et de manière générale les garants de la sécurité des réseaux locaux d'entreprise, investissent dans des pare-feu et autres équipements de détection d'intrusion et pensent, souvent à juste titre, protéger leur réseau des diverses attaques possibles. Dans le même temps, les constructeurs ne cessent de faire progresser leur équipements et les enrichissent de fonctionnalités qui les rendent toujours plus sécurisant en regard de l'intelligence qu'ils embarquent, et toujours plus attractifs du point de vue de leur facilité d'utilisation.

La sécurité des réseaux est donc devenue un des éléments-clés de la continuité des systèmes d'information de l'entreprise quelles que soient ses activités, sa taille et sa répartition géographique, ainsi l'entreprise BMT ne fait pas exception à cette règle car la communauté de l'entreprise (directions, services...) est un point sensible qui ne cesse d'augmenter, la nécessite de protéger les données stratégiques et la fragilités du réseau actuel aux différentes attaque interne et externe.

L'objectif de notre mémoire de fin de cycle est de renforcer la politique de sécurité du réseau local avec l'implémentation d'une solution basée sur les VLANs (*Virtual local Area Network*).Pour cela nous allons organiser l'ensemble des utilisateurs dans des réseaux virtuels en procédant la segmentation logique du réseau en mettant bien sûr en évidence l'aspect sécuritaire de l'opération par le choix de la bonne segmentation logique,

de la bonne configuration et des outils utilisés. Et pour mener à bien notre travail, nous procédons comme suit :

Tout d'abord, nous présenterons les concepts fondamentaux ainsi que le fonctionnement des réseaux locaux dans le premier chapitre, ensuite dans le second chapitre, nous parlerons de l'impact sécurité informatique sur les réseaux en exposant les objectifs ainsi que les stratégies de sécurité. Au troisième, nous concentrons notre attention sur les concepts de bases des réseaux virtuels, nous mettons en outre l'accent sur la norme 802.1Q ainsi que les protocoles utilisées pour la configuration et l'administration des VLANs. Le quatrième chapitre sera consacré à l'étude du lieu de notre stage ou organisme d'accueil. Dans le dernier chapitre nous avons présenté le principe de la configuration du réseau de l'entreprise BMT ou nous allons proposer une solution et et on le mis en oeuvre.

La conclusion générale résumera les points forts accomplis dans ce travail, pour mener à bien ce travail.

CHAPITRE 1

# Généralités sur les réseaux informatiques

## 1.1 Introduction

Réseau informatique permet de relier un ensemble de matériels par des supports de transmission qui leur permettent d'échanger des données entre eux. Pour bien mener notre projet, comprendre les notions de bases sur les réseaux informatiques est très important afin de bien maitriser notre sujet.

Ce chapitre a pour objectif de présenter quelques concepts de bases sur les réseaux informatiques, pour bien aider à mieux assimiler le fonctionnement des réseaux. Donc, toutes les notions nécessaires seront présentées, tirant exemple de la classification des réseaux, la topologie, le modèle OSI et TCP/IP ainsi les périphériques réseaux pour conclure par l'adressage.

## 1.2 Réseaux informatiques

Un réseau est un moyen de communication qui permet à des individus ou à des groupes de partage des informations et des services.

La technologie des informatiques constitue l'ensemble des outils qui permettent à des ordinateurs de partager des informations et des ressources.

Un réseau est constitué d'équipements appelées nœuds. En fonction de leur étendue et de leur domaine d'application, ces réseaux sont catégorisés[1].

### 1.2.1 Classification des réseaux

Nous distinguons plusieurs catégories de réseaux informatiques, différenciées par la distance maximales séparant les points les plus éloignés de réseau, le débit ou la bonde passante, et le taux d'erreurs.

- **Réseau personnel**

  La plus petite étendue de réseau est nommée en anglais Personal Area Network ($PAN$). Centrée sur l'utilisateur, elle désigne une interconnexion d'équipements informatiques dans un espace d'une dizaine de mètres autour de celui-ci, le Personal Operating Space ($POS$). Deux autres appellations de ce type de réseau sont : réseau individuel et réseau domestique[2]. Cela se figure dans (FIG. 1.1) ci-dessous.

Fig. 1.1- Topologie du réseau Personnel [2].

- **Réseau local**

  De taille supérieure, s'étendant sur quelques dizaines à quelques centaines de mètres, le local Area Network ($LAN$), en français réseau local d'entreprise ($RLE$), relie entre eux des ordinateurs, des serveurs,... il est couramment utilisé pour le partage de ressources communes comme périphériques, des données ou des applica-

tions [2]. Cela se figure dans (Fig. 1.2) ci-dessous.

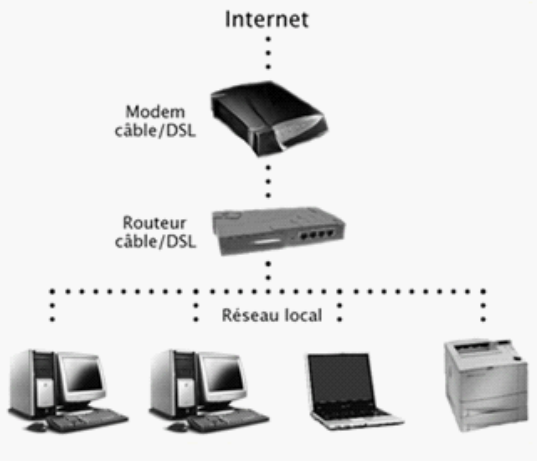


Fig. 1.2 - Topologie du réseau Local

[2].

- **Réseau métropolitain**

  Le réseau métropolitain est ou Metropolitan Area Network (*MAN*) est également nommé réseau fédérateur. Il assure des communications sur de plus longues distances, interconnectant souvent plusieurs réseaux LAN. Il peut servir à interconnecter, par une dizaines de kilomètres[2]. Cela se figure dans (Fig. 1.3) ci dessous.

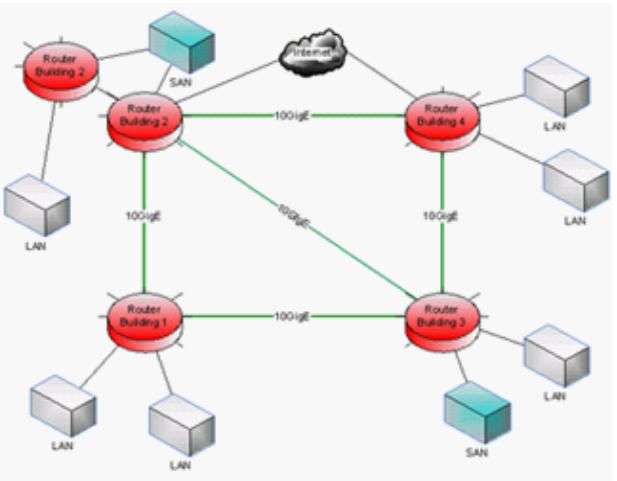


Fig. 1.3 - Topologie du réseau Métropolitain

[2].

- **Réseau étendu**

  Les étendus de réseaux les plus conséquentes sont classées en Wide Area Network (*WAN*). Constitués de réseaux de types LAN, voire MAN, mes réseaux étendus sont capables de transmettre les informations sur des milliers de kilomètres à travers le monde entier. La WAN le plus célèbre est le réseau public Internet dont le nom provient de cette qualité : Inter Networking ou interconnexion de réseaux[2]. Cela se figure dans (Fig. 1.4) ci-dessous.

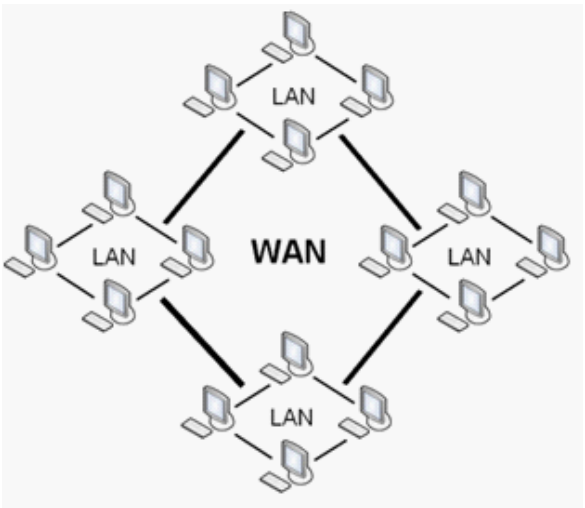


Fig. 1.4 - Topologie du réseau étendu [2].

La figure suivant nous montre l'intersection des différents réseaux :

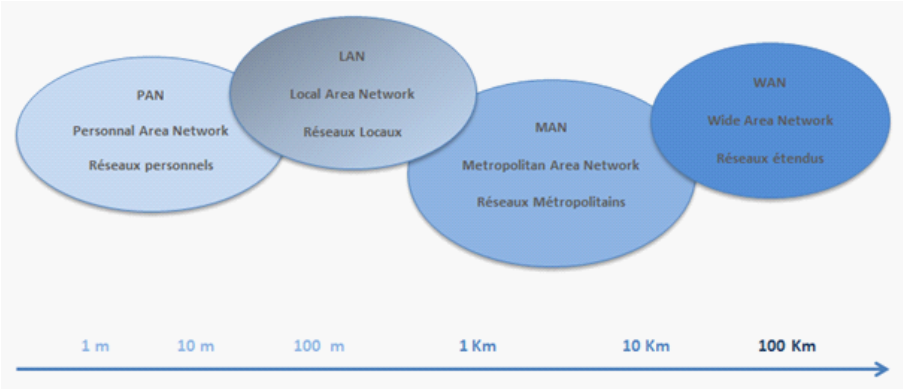


Fig 1.5 - La classification des réseaux.

## 1.3 Réseaux locaux

Un réseau local est un ensemble de moyens autonomes de calculs (*micro-ordinateurs, station de travail, imprimantes, etc.*) Reliés entre eux pour s'échanger et partager des ressources matérielles (*photocopieurs, scanners, graveurs, etc.*) ou logicielles (*programmes, fichiers, messagerie, etc.*)[3].

L'objectif d'un réseau local dans une entreprise est de répondre à un certain nombre de question spécifique aux équipements interconnecter et aux applications à supporter[4].

### 1.3.1 Topologies des réseaux locaux

La topologie caractérise la façon dont les différents équipements sont interconnectés.

Il convient de distinguer[5]:

- **Topologie logique :** elle représente la façon dont les données transitent dans les lignes de communication. les topologies logiques les plus courants Ethernet, Token ring et FDDI.(1)
- **Topologie physique :** c'est le chemin de câblage apparent, donc ce que voit l'utilisateur.

Il existe quatre grands types et topologie physiques dans les réseaux locaux, la topologie en étoile, en anneau, en bus et en arbre. Les topologies plus complexes peuvent être obtenues en combinant ou en décrivant ces topologies de base.

1. **Topologie en bus :**

   La topologie en bus (*support linéaire*) repose sur un câblage, sur lequel viennent de connecter des nœuds (*postes de travail, équipements d'interconnexion, périphérique*). Il s'agit d'un support multipoints. Le câble est l'unique élément matériel constituant le réseau et seuls les nœuds génèrent les signaux.

   La quantité de câbles utilisés est minimales est ne nécessite pas de point central. L'inconvénient majeur repose sur le fait qu'une seule coupure du câble empêche

(1) Technologie développée pour les réseaux métropolitains

toute station d'échanger des informations sur le réseau[2].

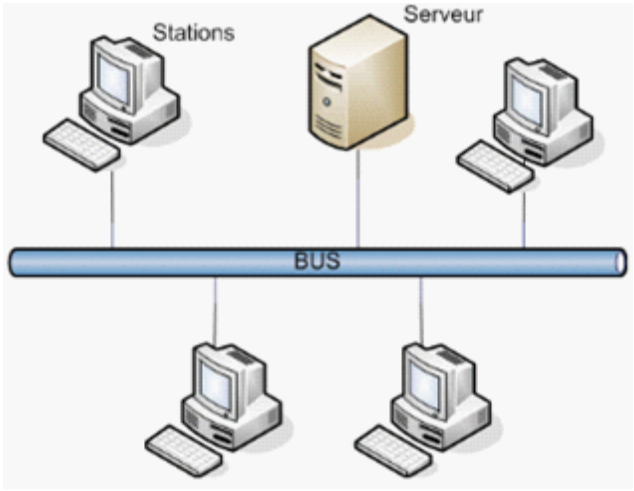


Fig. 1.6 - Topologie en Bus [2].

2. **Topologie en étoile**

   La topologie en étoile repose, quant à elle sur des matériels actifs. Un matériel actif remet en forme les signaux et les régénère. Il intègre une fonction de répéteur.
   Ces points centraux sont appelés des concentrateurs (*hubs*). Il est possible de créer une structure hiérarchique en constituant un nombre limité de niveaux.
   L'exploitation d'un concentrateur dans un réseau Ethernet crée une topologie physique en étoile, alors que la topologie logique associée peut être considérée en bus[2].

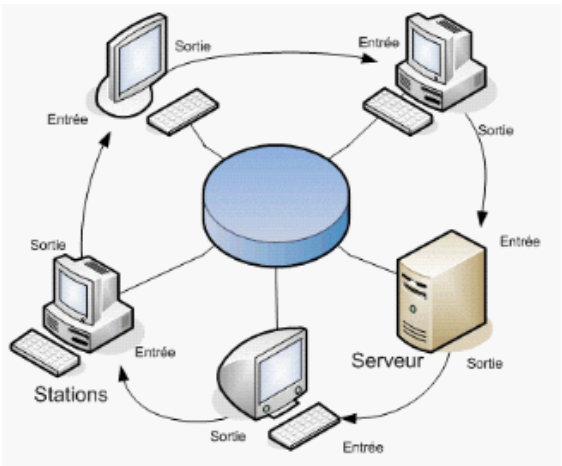


Fig. 1.7 - Topologie en Etoile[2] .

3. **Topologie en anneau**

   Cette topologie repose sur une boucle fermée, en anneau (*ring*), constituée de liaisons point à point entre périphériques. Les trames transitent par chaque nœud, qui ce comporte comme un répéteur (*élément actif*). Les concentrateurs en anneau permettent l'insertion de stations dans un réseau. Ils contiennent non seulement des ports pour ces dernières, mais également deux connecteur hermaphrodites nommés R/I (*Ring In*) et R/O (*Ring Out*) pour faire les boucles entre éléments. Ils acceptent des connexions de câbles cuivre (*RJ45*) ou de fibres. On différencie le MAU (*Multistation Access Unit*), passif, du CAU (*Controlled Access Unit*), actif.

   L'exploitation d'u MAU dans un réseau crée une topologie physique en étoile, alors que la topologie logique associée est en anneau [2].

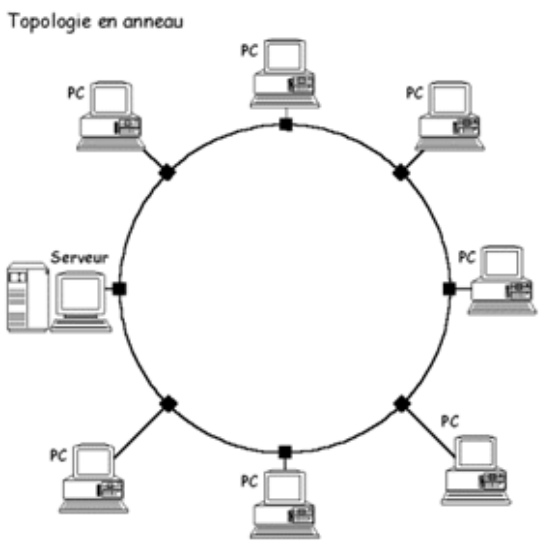


Fig. 1.8 - Topologie en Anneau [2].

4. **Topologie en arbre**

   Dans l'architecture en arbre, les postes sont reliés entre eux de manière hiérarchique, à l'aide de concentrateurs cascadables (*stackable hubs*). Cette connexion doit être croisée.

   En Ethernet sur paire torsadée, il est possible d'interconnecter jusqu'à quatre niveaux

de concentrateurs[2].

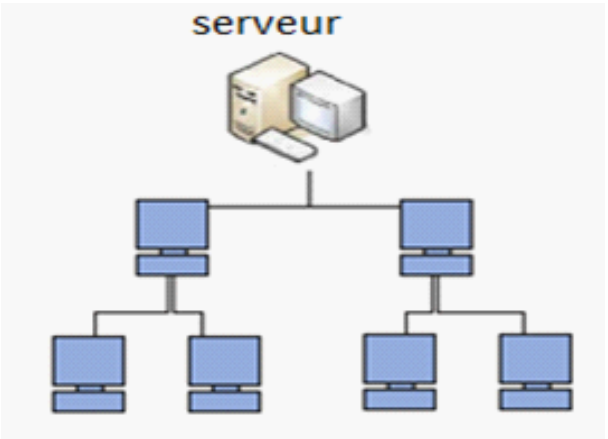


Fig. 1.9 - Topologie en Arbre [2].

## 1.4 Modèles de réseaux

Il existe deux types de modèles de réseau de base : le modèle de référence et le modèle d'application[1].

### 1.4.1 Modèle OSI (Open System Interconnection)

Pour faciliter l'interconnexion des systèmes, un modèle dit d'interconnexion des systèmes ouverts, appelé encore OSI (*Open System Interconnction*) a été défini par ISO (*International Standards Organization*).

Le modèle OSI décrit un ensemble de spécifications pour une architecture réseau permettant la connexion d'équipements hétérogènes. Le modèle OSI normalisation la manière dont les matériels et les logiciels coopèrent pour assurer la communication réseau. Ce modèle est organisé en sept couches successives.

**a. Couche Physique (Physical Layer)**

La couche physique assure un transfert de bits sur le canal physique (*support*). A cet effet, elle définit les supports et le moyen d'y accéder : spécifications mécaniques (*connecteur*), spécifications électriques (*niveau de tension*), spécifications fonctionnelles des éléments de raccordement nécessaires à l'établissement, au maintien et à la libération de la ligne. Elle détermine aussi les moyens d'adaptation (*ETCD*)[6].

**b. Couche Liaison de données (Data Link Layer)**

La couche liaison assure, sur la ligne, un service de transfert de blocs de données (*trames*) entre deux systèmes adjacents en assurant le contrôle, l'établissement, le maintien et la libération du lien logique entre les entités.

Les protocoles de niveau 2 permettent, en outre, de détecter et de corriger les erreurs inhérentes aux supports physiques[6].

**c. Couche Réseau (Network Layer)**

La couche réseau assure, lors d'un transfert à travers un système relais, l'acheminement des données (*paquets*) à travers les différents nœuds d'un sous-réseau (*routage*). Les protocoles de niveau 3 fournissent les moyens d'assurer l'acheminement de l'appel, le routage, le contrôle de congestion, l'adaptation de la taille des blocs de données aux capacités du sous-réseau physique utilisé. Elle offre, en outre, un service de facturation de la prestation fournie par le sous-réseau de transport[6].

**d. Couche Transport (*Transport Layer*)**

La couche transport est la couche pivot du modèle OSI. Elle assure le contrôle du transfert de bout en bout des informations (*messages*) entre les deux systèmes d'extrémité. La couche transport est la dernière couche de contrôle des informations, elle doit assurer aux couches supérieures un transfert fiable quelle que soit la quantité du sous-réseau de transport utilisé[6].

**e. Couche Session (*Session Layer*)**

La couche session gère l'échange de données (*transaction*) entre les applications distantes. La fonction essentielle de la couche session est la synchronisation des échanges la définition de points de reprise.

**f. Couche Présentation (Presentation Layer)**

Interface entre les couche qui assurent la mise en forme des données et celle qui les manipule, cette couche assure la mise en forme des données, les conversions de code nécessaires pour délivrer à la couche supérieure un message dans une syntaxe compréhensible par celle-ci. En outre, elle peut, éventuellement, réaliser des fonctions spéciales, comme la compression des données. . . [6].

**g. Couche Application (Application Layer)**

La couche application, la dernière du modèle de référence, fournit au programme utilisateur, l'application proprement dite, un ensemble de fonctions (*entités d'application*) permettant le déroulement correct des programmes communicants (*transferts de fichiers, courrier électronique...*)[6].

### 1.4.2 Modèle TCP/IP

Le modèle TCP/IP comporte quatre couches : application, la couche transport, la couche Internet et la couche d'accès au réseau. Comme vous pouvez le constater, certaines couches du modèle TCP/IP portent le même nom que les couches du modèle OSI.

Il ne faut pas confondre les couches des deux modèles, car la couche application comporte des fonctions différentes dans chaque modèle.

1. **Couche Application**

   Les concepteurs du modèle TCP/IP estimaient que les protocoles de niveau supérieur devaient inclure les détails des couches session et présentation. Ils ont donc simplement créé une couche application qui gère les protocoles de haut niveau, les questions de représentation, le code et le contrôle du dialogue. Le modèle TCP/IP regroupe en une seule couche tous les aspects liés aux applications et suppose que les données sont préparées de manière adéquate pour la couche suivante[7].

2. **Couche Transport**

   La couche transport est chargée des questions de qualité de service touchant la fiabilité, le contrôle de flux et la correction des erreurs. L'un de ses protocoles, TCP (*Transmission Control Protocol – protocole de contrôle de transmission*), fournit d'excellents moyens de créer, en souplesse, des communications réseau fiables, circulant bien et présentant un taux d'erreurs peu élevé. Le protocole TCP est orienté connexion. Il établit un dialogue entre l'ordinateur source et destination pendant qu'il prépare les informations de couche application en unités appelées segments. Un protocole orienté connexion ne signifie pas qu'il existe un circuit entre les ordinateurs en communication (*ce qui correspondrait à une commutation de circuits*). Ce type de fonctionnement indique qu'il y a un échange de segments de couche 4

entre les deux ordinateurs hôtes afin de confirmer l'existence logique de la connexion pendant un certain temps. C'est ce que l'on appelle la commutation de paquets[7].

3. **Couche Internet**

Le rôle de la couche Internet consiste à envoyer des paquets source à partir d'un réseau quelconque de l'inter réseau et à les faire parvenir à destination, indépendamment du trajet et des réseaux traversés pour y arriver. Le protocole qui régit cette couche est appelé protocole IP (*Internet Protocol*). L'identification du meilleur chemin et la commutation de paquets ont lieu au niveau de cette couche. Pensez au système postal. Lorsque vous postez une lettre, vous ne savez pas comment elle arrive à destinataire (*Il existe plusieurs routes possibles*), tout ce qui vous importe c'est qu'elle arrive à bon port[7].

4. **Couche d'accès au réseau**

Le nom de cette couche a un sens très large et peut parfois prêter à confusion. On lui donne également le nom de couche hôte-réseau. Cette couche de charge de tout ce dont un paquet IP a besoin pour établir une liaison physique avec l'hôte de destination. Cela comprend les détails sur les technologies LAN et WAN, ainsi que tous les détails dans les couche physique et liaison de données du modèle OSI[7].

La comparaison entre les deux modèle OSI et TCP/IP :

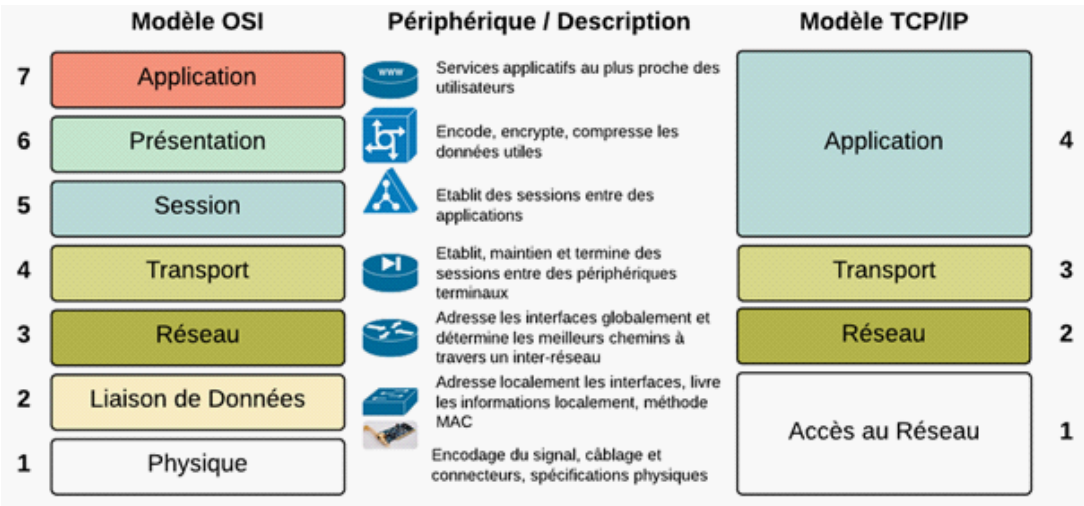


Fig. 1.10 - La comparaison entre le modèle OSI et TCP/IP [7].

## 1.5 Interconnexion d'un réseau local

Des matériels sont utilisés pour interconnecter les réseaux entre eux. Ils permettent également de segmenter les réseaux de tailles importantes, en domaine plus petit[8].

Les éléments d'interconnexion sont :

- **Répéteur** (*Repeater*) : dispositif permettant d'étendre la distance de câblage d'un réseau local. Il amplifie et répète les signaux qui lui parviennent.
- **Routeur :** Un routeur (*Router*) est un dispositif permettant de relier des réseaux locaux de telle façon à permettre la circulation de données d'un réseau à un autre de façon optimale.
- **Passerelle :** Une passerelle (*Gateway*) est un dispositif permettant traduction d'un protocole d'un haut niveau à un autre.
- **Concentrateur :** Un concentrateur (*Hub*) est un dispositif permettant de connecter divers éléments de réseau.
- **Commutateur :** Un commutateur (*Switch*) est un dispositif permettant de relier divers éléments tout en segmentant le réseau.
- **Adaptateur :** Un adaptateur (*Adapter*) est destiné à être insérés dans un poste de travail ou un serveur afin de les connecter à un système de câblages.
- **Pont :** Un pont(*Bridge*) est un dispositif permettant de relier des réseaux de même nature.

## 1.6 Adressage IP

### 1.6.1 Protocole IP

Le protocole IP (*Internet Protocol*) s'agit d'un protocole réseau de niveau trois, ce protocoles permet d'émettre des paquets d'informations à travers le réseau ; il est utilisé pour dialoguer les machines entres elles. Ainsi, il offre un service d'adressage unique pour l'ensemble des machines. Il n'est pas orienté connexion, c'est-à-dire qu'il n'est pas fiable, cette fiabilité dépend de la couche de transport[9].

### 1.6.2 Format des adresses IP

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

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

   - **Masque réseau :** Le masque de réseau sert à séparer les parties réseau et hôtes d'une adresse. On retrouve l'adresse du réseau on effectuant un ET logique bit à bit entre une adresse complète et le masque de réseau.
   - **Les classes des adresses IP :** Le but de la division des adresses IP en classes, est de facilité la recherche d'un ordinateur sur le réseau. En effet, avec cette notation il est possible de rechercher dans un premier temps le réseau à atteindre puis de chercher un ordinateur sur celui-ci. Ainsi, l'attribution des adresses IP se fait selon la taille du réseau.
     En effet, il existe cinq classes des adresses IP, à savoir : classe A, classe B, classe C, classe D et classe E, telle que, chaque classe a un format spécial de son adresse IP. " Adresse réseau et Adresse machine".
   - **Adresses Spécifiques**
     Dans l'ensemble des adresses IP, il existe certaines adresses qui sont spécifiques, c'est-à-dire, qu'elles ont un usage particulier. Parmi ces adresses, citant : les adresses privées et les adresses de diffusion.
   - **Adresses privée**
     Il existe des adresses privées, dans chaque classe :
     A → 10.0.0.0 à 10.255.255.255
     B →172.16.0.0 à 172.31.255.255
     C → 192.168.0.0 à 192.168.255.255

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

- **Adresse de diffusion**

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

2. **Format IPV6 :** Une adresse IPV6 est longue de de 128 bits, soit 16 octet, c'est une notation hexadécimale, ou les groupes de 2 octets (*16 bits par groupe*) sont séparés par un signe deux-points ":".

   Dans une adresse IPv6, une unique suite de un ou plusieurs groupes consécutifs de 16 bits tous nuls peut être omise, en conservant toutefois les signes deux-points de chaque côté de la suite de chiffres omise, c'est-à-dire une paire de deux points "::" . Les réseaux sont notés en utilisant la notation CIDR (*Classless Inter-Domain Routing*) : la première adresse du réseau est suivie par une barre oblique et un nombre Qui indique la taille en bits du réseau. La partie commune des adresses est appelée préfixe.

## 1.7 Conclusion

Ce chapitre nous a permet d'avoir une idée bien claire sur les réseaux informatiques et de mieux comprendre les raisons pour lesquelles les spécialistes en réseau ont élaboré le modèle de référence OSI et TCP/IP, en passant par l'adressage IP.

Dans le chapitre suivant, nous allons aborder la sécurité des réseaux informatiques qui est devenue un sérieux problème et que la majorité des entreprises ne peuvent plus ignorer.

CHAPITRE 2

# Généralité sur la sécurité informatique

## 2.1 Introduction

L'univers des systèmes d'informations composé de réseaux et de systèmes informatiques prend un rôle et une place chaque jour plus important dans les entreprises.

Cependant, l'actualité présentée par les médias nous démontre que le système d'information est vulnérable et qu'il peut subir des piratages, des attaques (*virus*), des pertes de données, des sinistres. Il est donc indispensable pour les entreprises de savoir définir et de garantir la sécurité de ses ressources informatique.

Nous entamerons ce chapitre par une définition et une exposition des objectifs de la sécurité, nous parlerons ensuite des différentes menaces, vulnérabilité et attaques qui pèsent sur les réseaux, et enfin, nous bouclerons ce chapitre par une présentation des différents mécanismes de défense et de sécurité tels que les pare-feu, les DMZ, les VLAN, les VPN, etc.

## 2.2 Sécurité Informatique

La sécurité des réseaux informatiques est nécessaire pour protéger le réseau d'une entreprise et de se prémunir contre tout type d'attaques pouvant perturber le réseau. La sécurité informatique (*SI*) est l'ensemble des moyens (*méthodes, techniques et outils*) mises en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles. Elle a pour objectif d'assurer les propriétés suivantes[10] :

- **La confidentialité :** Assurer que l'information ne soit divulguée ou révélée qu'aux personnes autorisées.
- **L'authentification :** C'est la propriété qui assure que seules les entités autorisées ont accès au système.
- **L'intégrité :** Assurer que l'information contenue dans les objets ne soit ni altéré, ni détruite de manière non autorisée.
- **La disponibilité :** L'accès par un sujet autorise aux ressources et informations du système doit être toujours possible.
- **Non répudiation :** C'est la propriété qui assure la preuve de l'authenticité d'un acte c'est-à-dire que l'auteur d'un acte ne peut ensuite dénier l'avoir effectué.

### 2.2.1 Terminologie de la sécurité informatique

1. **Vulnérabilité :** c'est une faille ou un point ou le système et susceptible d'être attaqué.
2. **Les attaques:** représentent les moyens d'exploiter une vulnérablité. Ils s'appuient sur divers types de faiblesses telles que les Faiblesse des protocoles, Faiblesse d'auhentification, Faiblesses d'implémentation ou bogues et les Mauvaises configurations.
3. **Les contre-mesures :** Ce sont les procédure ou techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique.
4. **Une politique de sécurité :** La politique de sécurité d'un réseau se fonde avant tout sur une analyse des risques décrivant les ressources critiques du réseau, ses vulnérabilités, les probabilités d'occurrences des menaces sur ces ressources vitales, ainsi que leurs conséquences. A partir de cette politique de sécurité, une architecture, des outils et des procédures sont définis et déployés afin de protéger les ressources critiques et de répondre aux objectifs de sécurité.
   L'établissement d'une politique de sécurité se fait selon les étapes suivantes :
   - Identification des vulnérabilités.
   - Evaluation des probabilités associées à chacune des menaces.

- Evaluation du cout d'une intrusion réussie.
- Choix des contres mesures.
- Evaluation des couts des contre mesure.
- Décision.

## 2.3 Outils de sécurité

### 2.3.1 Solutions de sécurité minimum

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

- Authentification des utilisateurs par login et mot 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 mis-à-jour.

### 2.3.2 Cryptographie

La cryptographie est une science qui utilise les concepts mathématique pour cryptage (*chiffrement*) et le décryptage (*déchiffrement*) des données. Elle permet ainsi de stocker des informations confidentielles ou de transmettre sur des réseaux non sécurisés (*tel que l'internet*), afin qu'aucune personne autre que le destinataire ne puisse les lire.

Alors que la cryptographier consiste à sécuriser les données, la cryptanalyse est l'étude des informations cryptées, afin de découvrir le secret. La cryptanalyse classique implique une combinaison intéressante de résonnement analytique, d'application d'outils mathématique, de recherche de modèle, de patience, de détermination et de chance. Ces cryptanalyses sont également appelés des pirates. La cryptographier est divisées en deux axes majeurs [12] :

1. **Cryptographie symétrique**

   Une même clé est utilisée pour crypter et décrypter le message, très efficace et assez

économe en ressources CPU cette technique pose le problème de la distribution des clés dans un réseau étendu (*exemple DES, triple DES ou le récent AES*) [13].

2. **Cryptographier asymétrique**

   Chaque utilisateurs dispose d'un jeu unique de clés, dosent l'une est privée (*secrète*) et l'autre publique (*RSA*). Pour recevoir des documents protégés, le détenteur d'un jeu de clés envoie sa clé publique à ses interlocuteurs, qui l'utilisent pour chiffrer les données avant de les lui envoyer. Seul le destinataire et détenteur des clés peut lire les informations en associant sa clé privée à sa clé publique. Cette technique nécessite des clés plus longues pour une sécurité équivalente [13].

   Voici ce schéma ci-dessous qui récapitule les différents termes et mots utilisés dans le vocabulaire de la cryptographie :

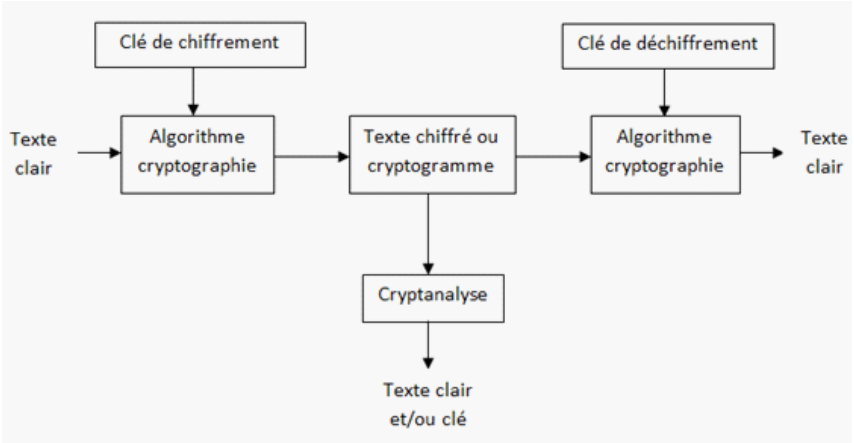


Fig. 2.1 - Récapitulatif du lexique de la cryptographie [13].

- **Fonctions de hachage**

  Ce type de fonction est très utilisé en cryptographier, principalement dans le but de réduire la taille des données à traiter par la fonction de cryptage. En effet, la caractéristique principale d'une fonction de hachage est de produire un haché des données, c'est-à-dire un condensé de ces données. Ce condensé est de taille fixe, dont la valeur diffère suivant la fonction utilisée (*MD5, SHA*) [14][15].

- **Signature numérique**

  Les signatures numérique permettent à la personne qui reçoit une information de contrôle l'authenticité de son origine, et également de vérifier que l'information en

question est intacte.

Ainsi, les signatures numériques des systèmes à des clés publiques permettent l'authentification et le contrôle d'intégrité des données. Le principe de la signature consiste à appliquer une fonction mathématique sur portion de message, cette fonction mathématique s'appelle fonction de hachage et le résultat appelé code de hachage, ce code de hachage est ensuite crypté avec les clés privées de l'émetteur et rajouter au message ensuite le destinataire décrypte le code grâce à la clé publique puis il compare ce code qu'il calcule grâce au message reçus [16].

Le destinataire sait aussi que le message provient de l'émetteur, puisque seul le dernier possède la clé privée qui a crypté le code (Fig. 2.2).

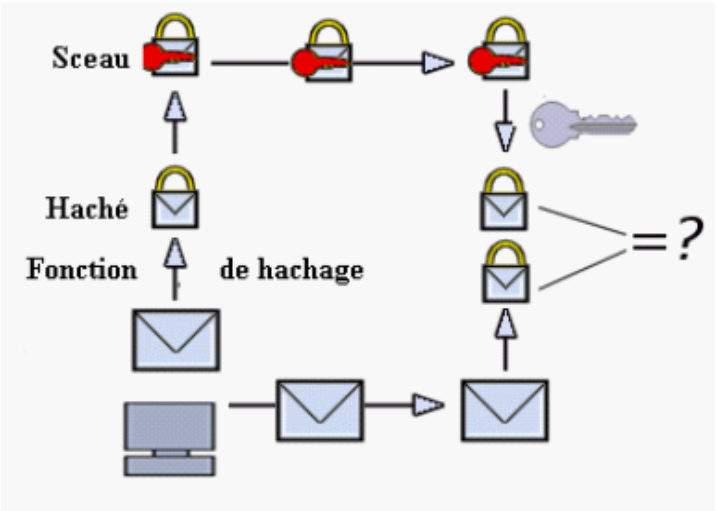


Fig. 2.2 - Architecture de la signature numérique [16].

- **Certificat électronique**

Un certificat est un fichier émis par une autorité de certification contenant un ensemble de données prouvant l'existence et l'intégrité d'une entité virtuelle ; il est comparable à une carte d'identité ou un passeport d'une personne.

La première utilité d'un certificat électronique est de garantir la confiance entre deux interlocuteurs distants qui partagent des informations confidentielles.

Pour vérifier un certificat il faut et il suffit de connaître la clé publique de l'autorité émettrice [17].

### 2.3.3 Firewall et proxy

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

1. **Firewall (pare-feu) :** un système permettant de protéger un ordinateur ou un réseau d'ordinateur, des intrusions provenant d'un réseau tiers (*notamment Internet*). Il s'agit d'une passerelle qui opère en filtrant les paquets de données échangés avec le réseau (Fig. 2.3).

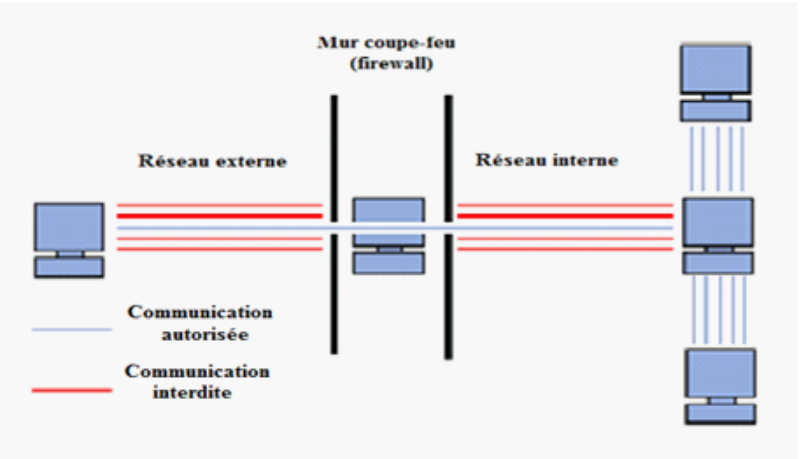


Fig. 2.3 - Architecture du Firewall [16].

2. **Serveur Proxy (serveur Mandataire) :** un intermédiaire entre les ordinateurs d'un réseau local et Internet. Utilisé la plus part du temps par le web, il s'agit alors d'un proxy HTTP qui permet :

   - D'accélérer la navigation : mémoire cache, compression de données, filtrage des publicités ou des contenus lourds.
   - La journalisation des requêtes (*login*).
   - Lé sécurité des réseaux local.

- Le filtrage et l'anonymat [18].

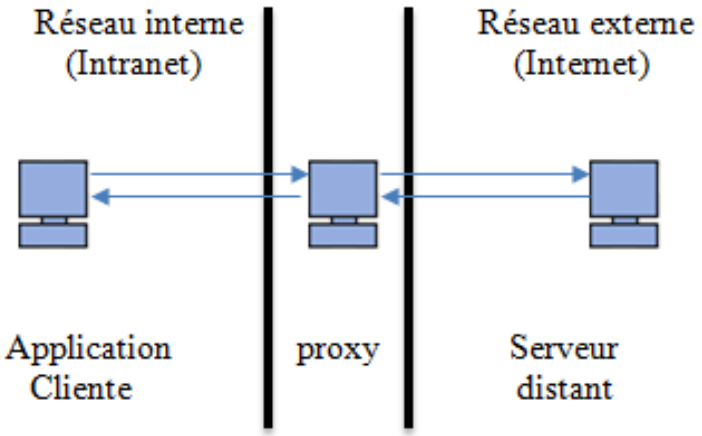


Fig. 2.4 - Architecture du Proxy [18].

### 2.3.4 Zone démilitarisée

Une DMZ (*DeMilitarized Zone*) est une interface située entre un réseau connu (*réseau interne*) et un réseau externe (*internet*). Une série de règles de connexion configurées sur le pare-feu font de cette interne une zone physiquement isolée entre les deux réseaux. Cette séparation physique permet d'autoriser les accès internet à destination des serveurs placés dans la DMZ et non à ceux destinés au réseau privé (*interne*) [5].

La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante

- Trafic du réseau externe vers la DMZ autorisé.
- Trafic du réseau externe vers le réseau interne interdit.
- Trafic du réseau interne vers la DMZ autorisé.
- Trafic interne vers le réseau externe autorisé.
- Trafic de la DMZ vers le réseau interne interdit.

- Trafic de la DMZ vers le réseau externe refusé.

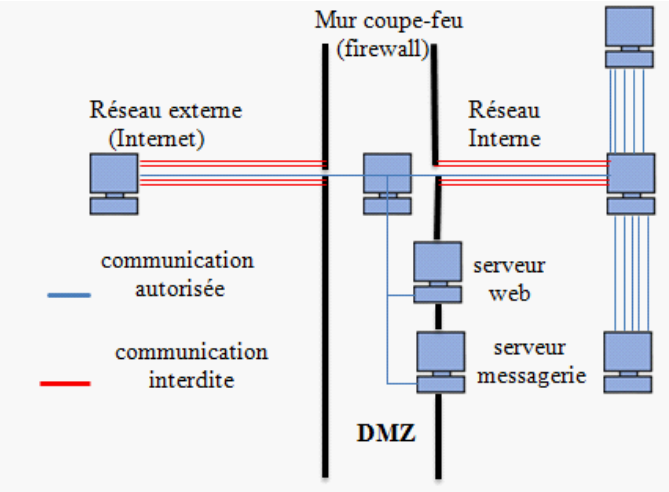


Fig. 2.5 - Architecture DMZ [5].

### 2.3.5 La technologie AAA

Nous vivons dans un monde ou presque tout doit être protégé contre une utilisation abusive ou impropre et ou rien n'est gratuit. Que vous soyez administrateur système, responsable, ingénieur réseau vous êtes toujours confronté aux trois aspects suivants [19]:

- **Authentification(*Authentication*) :** Il s'agit de la vérification de l'identité d'un utilisateur, elle est généralement assuré au moyen d'un secret partagé ou d'un logiciel approuvé (*protocole RADIUS*).

- **Autorisation (*Authorisation*) :** Elle intervient à l'issue de l'authentification. Une fois l'utilisateur authentifié, il faut s'assurer qu'il est autorisé à accomplir les actions qu'il demande, tels que l'accès à des fichiers, le droit d'écrire, etc. l'autorisation est gérée au moyen de liste ACL[(1)] ou des stratégies.
  1 Liste mentionnant les utilisateurs autorisés à atteindre une information.

- **Comptabilité (*Accounting*) :** Elle permet de collecter des informations sur les utilisateurs et les actions qu'ils accomplissent lorsqu'ils sont connectés aux équipements du réseau.

[(1)] Liste mentionnant les utilisateurs autorisés à atteindre une information.

### 2.3.6 Système de détection d'intrusion

Divers raison peuvent conduire un attaquant (*pirate*) à vouloir d'introduire sur un réseau : défi personnel, espionnage, motivation politique, gain financier ou simplement nuisance. Surveiller le réseau pour détecter les attaques éventuelles relève non seulement du bon sens mais constitue également un impératif pour n'importe quelle entreprise. D'où l'utilisation des systèmes de détection d'intrusion, ou IDS (*Instruction Detection System*).

Par définition un IDS est le système d'alarme du réseau. Ce dernier a beau être protégé par des moyens divers, seul l'IDS permet de savoir qu'un intrus tente d'y accéder. Les sondes de détection d'intrusion constituent le complément d'un pare-feu. Elles permettent d'analyser les actions ou les flux pour y détecter une tentative d'intrusion.

Les IDS peuvent être déployés en plusieurs endroit du réseau afin d'augmenter la sécurité, ils généralement de deux types :

- **Les N-IDS (*Network Based Intrusion Detection System*) :** Ils assurent la sécurité au niveau au niveau du réseau.
- **Les H-IDS (*Host Based Intrusion Detection System*):** Ils assurent la sécurité au niveau des hôtes [5].

### 2.3.7 VLAN (*Vitual Local Area Network*)

Un VLAN (*Virtual Local Area Network ou Virtual LAN*) est un réseau local regroupant un ensemble des machines utilisant la technologie Ethernet pour regrouper les éléments du réseau (*utilisateurs, périphériques, etc.*) selon des critères logiques (*fonction, partage de ressources, appartenance à un département, etc.*), sans se heurter à des contraintes physiques (*dispersion des ordinateurs, câblage informatique inapproprié, etc.*) [15].

### 2.3.8 VPN (*Virtual Private Network*)

Les réseaux privés virtuels permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Grace à un principe de tunnel (*tunnelling*) dont chaque extrémité est identifiée, les données transitent après avoir été éventuellement chiffrées [20].

Un des grands intérêt des VPN est de réalises des réseaux privés à moindre cout. En chiffrant les données, tout se passe exactement comme si la connexion se faisait en dehors d'internet. Il faut par contre tenir compte de la toile, dans le sens ou aucune qualité de service n'est garantie [21].

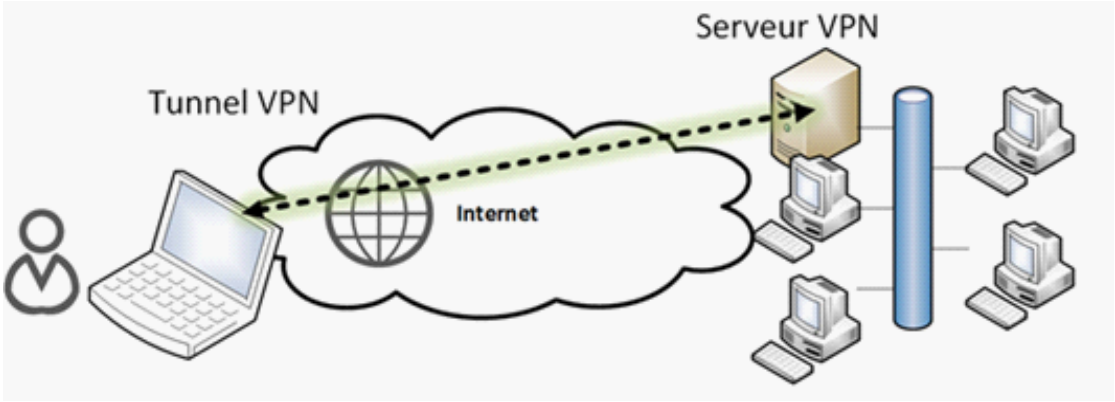


Fig. 2.6 - Architecture du fonctionnement des VPN [21].

1. **Types de réseau VPN**

   Il existe trois types de réseau VPN :

   - **Site à site (LAN to LAN) :** Le site à site permet de relier deux réseaux de façon transparente. Généralement les deux sites ont des tranches IP différentes ce qui oblige les postes clients à passer par le routeur. Celui-ci est directement relié à l'équipement responsable du VPN ou implante directement les protocoles choisit pour la mise en place du VPN [22]
   - **Poste à site (Host to LAN) :** Il existe le type nomade, également appelé "Road Warrior (chemin de guerrier)" qui permet à un utilisateur distant de son entreprise de se connecter à celle-ci pour pouvoir profiter de ses services. Ainsi, il pourra lire ses mails, récupérer des fichiers présents sur le réseau de son entreprise [22].
   - **Poste à poste (Host to Host) :** Dans ce cas de figure, on veut connecter deux ordinateurs distants entre eux pour des raisons de confidentialité. On crée donc un VPN entre eux, et toutes les données y transmises sont encryptées et compréhensibles que par les deux paires correspondantes[22].

2. **Protocoles utilisés pour l'établissement d'un VPN :**

   Il existe cinq protocoles principaux permettant l'établissement d'un VPN :

   - **PPP (*Point to Point Protocol*)**: Est un protocole qui permet le transfert des données sur un lien synchrone ou asynchrone. Il est full duplex et garantit l'ordre d'arrivée des paquets. Il encapsule les paquets IP dans les trames PPP, puis transmet ces paquets encapsulés au travers de la liaison point à point. PPP est employé généralement entre un client d'accès à distance et un serveur d'accès réseau. Le protocole PPP est défini dans la REF 2153.

     PPP est le fondement des protocoles PPTP et L2TP utilisés dans les connexions VPN sécurisés .PPP est la principale norme de la plupart des logiciels d'accès distant [23].

   - **le protocole PPTP (*Point To Point Tunneling Protocol*) :** Est un protocole réseau (*de niveau 2*) permettant un transfert sécurisé entre un client et un serveur privé. Il permet la création de VPN sur demande à travers des réseaux basés sur TCP/IP. Il peut de même être utilisé pour créer VPN entre deux ordinateurs dans le même réseau local [24].

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

   - **Le protocole L2TP (*Layer Two Tunneling Protocol*):** C'est un protocole de niveau 2, on peut accéder à un réseau privé par l'intermédiaire d'Internet ou d'autre réseau public au moyen d'une connexion à un VPN utilisant le L2TP. Ce dernier est protocole de tunneling standard qui possède pratiquement les memes fonctionnalités que le protocole PPTP [26].

   - **Le protocole IPSec (*Internet Protocol Security*) :** Est un protocole fournissant un mécanisme de sécurisation au niveau de la couche réseau du modèle OSI. Il assure la confidentialité, l'authentification et l'intégrité des données. IPSec permet de protéger les données et également l'en-tête d'une trame, en

masquant le plan d'adressage grâce à l'ajout d'un en-tête IPSec à chaque datagramme IP [27].

## 2.4 Conclusion

Nous avons vu à travers ce chapitre l'impact de la sécurité informatique sur les réseaux, en exposant l'objectif de la sécurité et quelques attaques qui peuvent infectées un réseau local et l'importance d'une politique de sécurité qui devra prendre en compte les besoins des utilisateurs, ainsi que les risques encourus dans le but d'énergie une vraie stratégie de sécurité. Enfin nous avons résumé quelques stratégie de sécurités telles que l'utilisation d'un pare-feu qui permet de vérifier la confidentialité et l'intégrité des ressources sur le réseau et l'authentification du trafic mais ne permet pas de se protéger contre les attaques provenant de l'intérieur et qui représentent 80% des attaques globales, ainsi on doit le compléter avec d'autres entités telles que les DMZ et les proxys pour une meilleurs sécurité. Nous avons vu aussi les VLANs et les VPN et le technologie AAA qui permettent un meilleur contrôle d'accès.

Dans le chapitre suivant nous détaillerons la stratégie des VLANs afin de l'implémenter au réseau local de Bejaia Mediteranean Terminal (BMT).

CHAPITRE 3

# Réseaux Locaux Virtuels (VLANs)

## 3.1 Introduction

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

En effet, dans un réseau local, la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels(*Vlans*), il est possible de s'affranchir des limitations de l'architecture physique (*contraintes géographique, contraintes d'adressage*). En définissant une segmentation logique (*logicielle*) basée sur un regroupement de machines grâce à des critères (*adresses MAC, numéros de port, protocole*).

Dans ce chapitre, nous allons présenter les principales notions d'un réseau local virtuel en commençant par la commutation, protocoles de transport (*la norme 802.1Q, protocole ISL*) et les protocoles d'administration et de gestion des VLANs (*VTP, DHCP, Spanning-Tree*).

## 3.2 Rappel sur la commutation

Contrairement à un concentrateur, un commutateur ne diffuse pas les trames. Il met en relation les seuls postes concernés par l'échange. Avant de réémettre les trames, le

commutateur vérifié que le support de communication est libre. Un commutateur évite donc les collisions contrairement à un concentrateur.

A chaque fois qu'un message lui parvient, le commutateur associe le port par lequel arrive la trame à l'adresse matérielle (*adresse MAC*) de l'émetteur de la trame. Ainsi après un certain nombre de trames, le commutateur connaît l'emplacement (*c'est-à-dire le port de rattachement*) des postes sur le réseau et peut les mettre en relation deux à deux.

Cette association adresse MAC/port est gérée dans des tables d'association présentes dans chaque commutateur. Cette table est construite progressivement par apprentissage. Si une trame contient une adresse de destination qui n'est pas présente dans la table, cette trame est transmise sur tous les ports du commutateur à l'exception du port émetteur de la trame, c'est ainsi que sont traités les trames de diffusion. On distingue deux modes de fonctionnement du commutateur [28].

- **Store and forward :** il stocke les trames entièrement avant de les réémettre. Il ne réémet donc pas les trames erronées (*CRC "Control Redundancy Check" innatendu*) ou en collision. Par contre ces commutateurs sont plus lents et nécessitent des mémoires tampons importantes.

- **Store and forword**[1] : à la volée, les commutateurs réémettent immédiatement après lecture de l'adresse MAC destinataire, c'est plus rapide mais on propage les trames erronées - notamment les trames en collision et celles le CRC indique une erreur de transmission.

## 3.3 VLAN (*Virtual Local Area Network*)

Le développement rapide d'internet a mené de nombreuses entreprises à étendre leur installation informatique. La technologie VLAN apporte des solutions nouvelles dans la segmentation et la sécurisation des réseaux locaux, tout en augmentant leurs performances, par définition un VLAN ou réseau virtuel est un regroupement de postes de travail indépendamment de la localisation géographique sur le réseau. Ces stations pourront communiquer comme si elles étaient sur le même segment. Un VLAN est assimilable

[1] appelé aussi cut through

à un domaine de diffusion (*Broadcast Domain*). Ceci signifie que les messages de diffusion émis par une station d'un VLAN ne sont reçus que par les stations de ce VLAN. Ces derniers n'ont été réalisables qu'avec l'apparition des commutateurs (*Switches*).

En effet, dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels, il est possible de s'affranchir des limitations de l'architecture physique (*contrainte géographique, contraintes d'adressages, etc.*) en définissant une segmentation logique (*logicielle*) basé sur un regroupement de machines grâce à des critères (*adresses MAC, numéros de port, protocole, etc.*), ces derniers permettent d'identifier les différents types de VLAN [29]. (voir la figure ci-dessous)

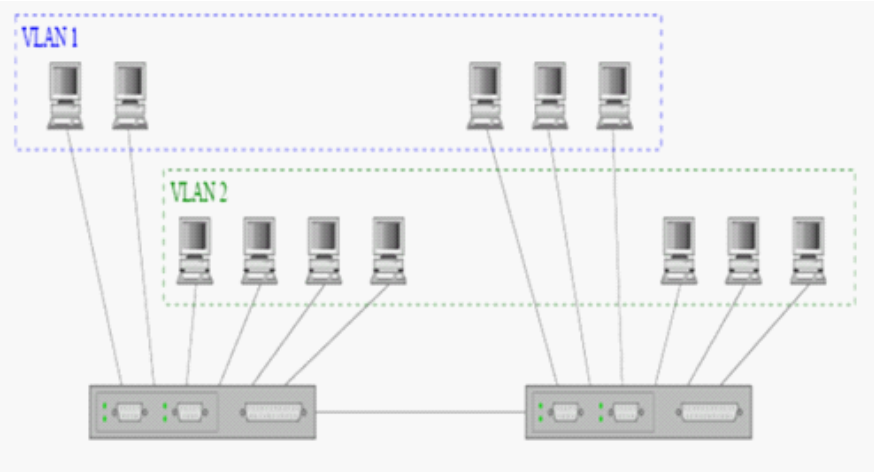


Fig. 3.1 - Plusieurs VLAN dans un réseau Ethernet.

## 3.4 Types de VLAN

Les VLANs diffèrent selon les informations utilisées pour regrouper les stations. Il en existe généralement quatre modèles, respectivement basés sur le port, sur l'adresse Mac, sur le protocole et l'adresse réseau [30].

**a. Les VLAN basés sur le port :** Dans ce modèle, chaque port d'un commutateur est attribué à un VLAN (voir figure ci-dessous). Toutes les stations connectées à un port appartiennent au VLAN correspondant. Lorsqu'une station est déplacée sur un autre port, celui-ci est également attribué au VLAN de la station de même, si une station change de VLAN, le port auquel elle est connecté est attribué à son

nouveau VLAN. Ainsi, le changement est complètement transparent à la station, et n'est pas nécessaire de modifier le câblage du réseau. Ce modèle de VLAN manque de flexibilité car toutes les stations connectées au même port d'un commutateur appartiennent à un seul et même VLAN.

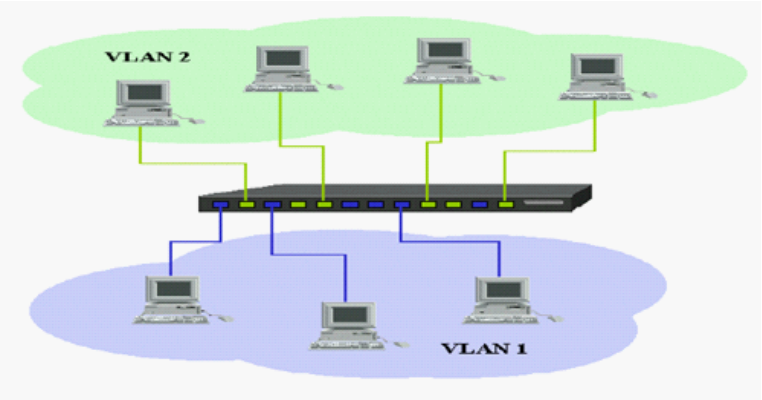


Fig. 3.2 - Construction des VLANs par port.

**b. Les VLAN basés sur l'adresse MAC :** Dans ce modèle, le VLAV auquel appartient une station est déterminé par son adresse MAC. Les adresses MAC étant physiquement liée aux stations, ce modèle permet de conserver la répartition des VLAN même après le déplacement d'une station. Contrairement au modèle de VLAN basé sur le port, des stations appartenant à des VLAN différents peuvent être connectées au même port commutateur. Une station peut théoriquement être membre de plusieurs VLAN différents. Le principal inconvénient de ce modèle est la mise à jour des correspondances entre les VLANs et les adresses MAC, qui peut être ardue dans

des réseaux de grande taille.

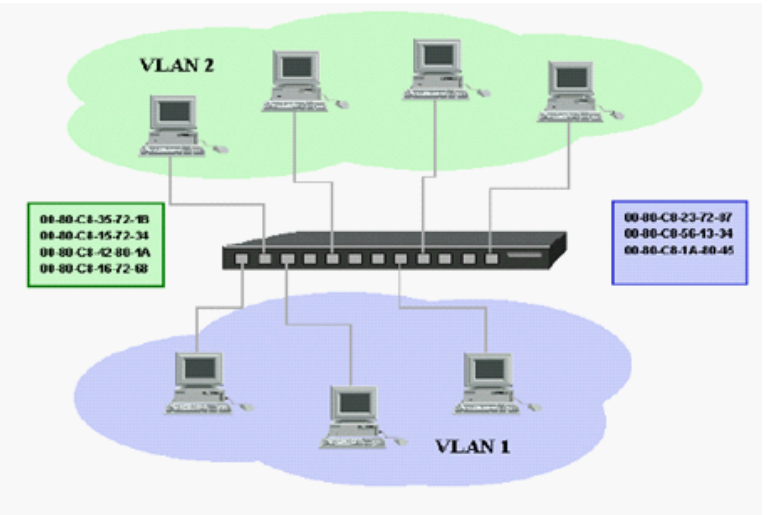


Fig. 3.3 - Construction des VLANs par adresse MAC.

**c. Les VLANs basés sur le protocole :** Un VLANs par protocole ou VLAN e niveau 3, est obtenu en associant réseau virtuel par type de protocole rencontré sur le réseau. On peut ainsi constituer un réseau virtuel pour les stations communiquant avec le protocole TCP/IP, un réseau virtuel pour les stations communiquant avec le protocole IPX,...

Dans ce type de VLAN, les commutateurs apprennent automatiquement la configuration des VLAN. Par contre, elle est légèrement moins performante puisque les commutateurs sont obligés d'analyser des informations de niveau 3 pour fonctionner. Les VLAN par protocole sont surtout intéressant dans des environnements hétérogènes multi-protocoles (*Novell Netware avec IPX, Unix avec TCP/IP, Macintosh avec Appletalk...*). La généralisation de TCP/IP leur a fait toutefois perdue de l'intérêt.

**d. VLAN par sous-réseau :** Egalement appelé VLAN de niveau 3, un VLAN par sous-réseau utilise les adresses IP sources des datagrammes émis. Un réseau virtuel

est associé à chaque sous-réseau IP (Fig. 3.4).

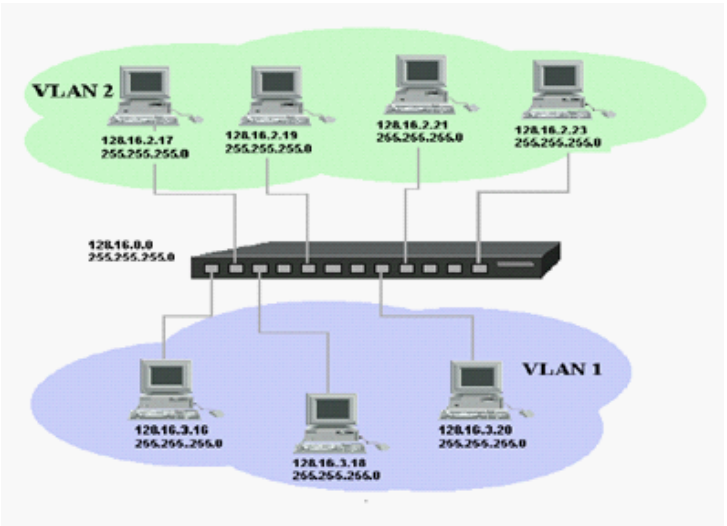


Fig. 3.4 - construction des VLANs par sous réseau.

Dans ce cas, les commutateurs apprennent automatiquement la configuration des VLAN. Cette solution est l'une des plus intéressantes, malgré une légère dégradation des performances de la commutation due à l'analyse des données de niveau réseau (*niveau 3*).

Plus récemment est apparue une nouvelle méthode de définition de réseaux virtuels basée sur la possibilité des commutateurs d'analyser le contenu des trames. Les possibilités sont multiples, allant des réseaux virtuels par type de service (*ports TCP*) aux réseaux virtuels par adresse multicast IP.

### 3.4.1 Avantages des VLANs

Ce nouveau mode de segmentation des réseaux locaux modifie radicalement la manière dont les réseaux sont conçus, administrés et maintenus. La technologie de VLAN comporte ainsi de nombreux avantages et permet de nombreuses applications intéressantes.

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

- **Flexibilité de segmentation du réseau :** Les utilisateurs et les ressources entre lesquels les communications sont fréquentes peuvent être regroupés sans devoir prendre en plusieurs VLAN en même temps.

- **Simplification de la gestion :** L'ajout de nouveaux éléments ou le déplacement d'éléments existants peut être réalisé rapidement et simplement sans devoir manipuler les connexions physiques dans le local technique.

- **Augmentation considérable des performances du réseau :** Comme le trafic réseau d'un groupe d'utilisateurs est confiné au sein du VLAN qui lui est associé, de la bande passante est libérée, ce qui augmente les performances du réseau.

- **Meilleure utilisation des serveurs réseaux :** Lorsqu'un serveur possède une interface réseau compatible avec le VLAN, l'administrateur a l'opportunité de faire appartenir de serveur à plusieurs VLAN en même temps. Cette appartenance à de multiples VLAN permet de réduire le trafic qui doit être routé (*traité au niveau du protocole de niveau supérieur, par exemple IP*) de et vers de serveur, et donc d'optimiser de trafic. Tout comme le découpage d'un disque dur en plusieurs partitions permet d'augmenter les performances (*la fragmentation peut être diminuée*) de son ordinateur, la VLAN améliore considérablement l'utilisation du réseau.

- **Renforcement de la sécurité du réseau :** Les frontières virtuelles créées par les VLAN ne pouvant être franchies que par le biais de fonctionnalités de routage, la sécurité des communications est renforcée.

- **Technologie évolutive et à faible cout :** La simplicité de la méthode d'accès et la facilité de l'interconnexion avec les autres technologies ont fait d'Ethernet une technologie évolutive à faible cout quelles que soient les catégories d'utilisateurs.

- **Régulation de la bande passante :** Un des concepts fondamentaux des réseaux Ethernet est la notion d'émission d'un message réseau vers l'ensemble (*broadcast ou multicast*) des éléments connectés au même commutateur (*hub/Switch*). Malheureusement, ce type d'émission augmente sérieusement le trafic réseau au sein du composant de connexion. Même si les vitesses de transmission ne cessent d'augmenter, il est important de pouvoir contrôler ce gaspillage de capacité de trafic disponible au sein de l'infrastructure [31].

### 3.4.2 Marquage ou étiquetage

Pour savoir à quel VLAN appartient telle trame il est nécessaire de les repérer. C'est le rôle du marquage ou étiquetage de trames qui attribue à chaque trame un code d'identification VLAN unique. Le marquage peut être :

- **Implicite (*VLAN non taggé – untagged VLAN*) :** Dans le cas où l'appartenance à tel ou tel VLAN peut être déduite de l'origine de la trame (*VLAN par port*) ou des informations normalement contenues dans la trame (*adresse MAC, adresse IP ou protocole*).

- **Explicite (*VLAN taggé – tagged VLAN*):** Dans le cas où un numéro de VLAN est inséré dans la trame.
  En effet, dès lors qu'il s'agit de faire circuler la trame à travers plusieurs commutateurs ou routeurs, on doit gérer son appartenance à tel ou tel VLAN. On utilise en effet la commutation à l'intérieur du VLAN, mais pour les interconnecter, on doit utiliser des routeurs ou des commutateurs supportant les fonctions de routage [32].

## 3.5 Protocoles de transport des VLANs

### 3.5.1 Norme 802.1q (ou l'art du tag)

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

Le principe consiste à ajouter dans l'en-tête de la trame Ethernet un marqueur qui va identifier le VLAN. Il existe quelques solutions propriétaires pour réaliser ceci, mais le système s'est avéré tellement intéressant qu'une norme a été définie, il s'agit de la norme 802.1q qui est née en 1998 pour répondre à un besoin de normalisation sur transport des VLANs [33].

- **Description de la norme**

La figure suivante illustre la modification de la trame Ethernet et l'ajout d'un champ sur 4 octets par la norme 802.1Q :

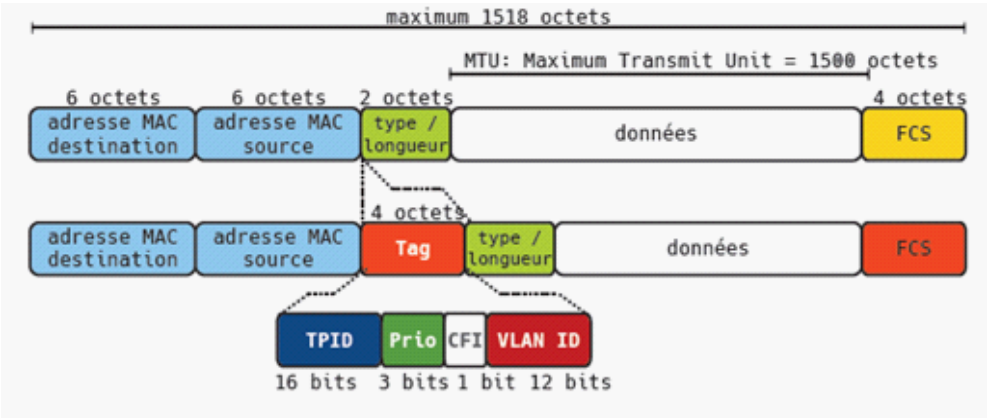


Fig. 3.5 - Extension de la trame Ethernet modifiée par la norme 802.1 Q [33].

- **Tag Protocol Identifier (*TPID*)**

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

- **Tag control Information (*TCI*)**

Cette partie se compose de trois champs :

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

**Canonical Format Identifier (*CFI*) :** Ce champ d'un bit assure la compatibilité entre adresses MAC Ethernet et Token Ring. Un commutateur Ethernet fixe cette valeur à 0 [34].

**VLAN ID (*VID*) :** c'est le champ d'identification du VLAN auquel appartient la trame par l'intermédiaire de ce champ de 12 bits, on peut coder 4094 VLAN (les valeurs 0 et FFF sont réservées). La valeur par défaut est 1(Fig. 3.6).

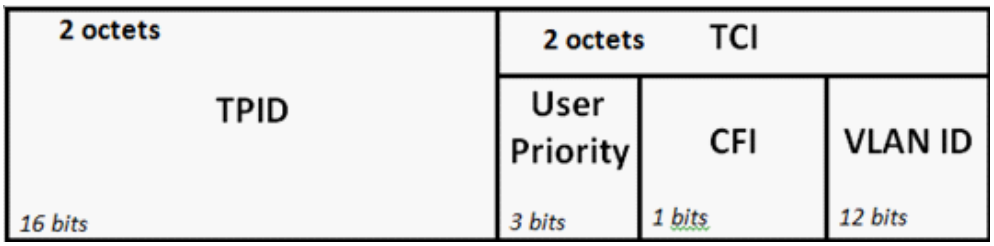


Fig. 3.6 - Détails du champ 802.1Q [34].

### 3.5.2 Protocole ISL (Inter Switch Link Protocol)

Pour étendre les réseaux virtuels sur plus d'un commutateur, CISCO a mis au point son propre protocole ISL. Ce protocole achemine les informations d'appartenance aux réseaux virtuels. ISL représente en fait une structure de trame et un protocole qui en plus de transport des informations d'appartenance aux réseaux virtuels, permet à ces réseaux d'échanger des trames [3].

- **Présentation générale**

Pour identifier les réseaux virtuels, ISL utilise un mécanisme de marquage explicite des paquets. Un commutateur qui utilise de marquage encapsule la trame reçue dans un paquet dont l'en-tête contient un champ d'appartenance aux VLAN et l'adresse MAC de la trame, permettent d'acheminer le paquet vers le routeur et les commutateurs appropriés. Lorsqu'elle atteint le réseau destinataire, on supprime l'en-tête et la trame est acheminée vers l'équipement récepteur [3].

- **Structure des trames ISL**

Les trames ISL comprennent trois champs principaux :

- Un en-tête qui est constituée de plusieurs champs illustrés dans la figure ci-dessous.

- Trame encapsulé dont la longueur est comprise entre 1 et 24575 octets.

- Champ CRC, ce champ qui est ajouté à la fin du paquet ISL, porte sur l'intégrité du paquet.

La figure ci-après illustre la structure d'une trame ISL :

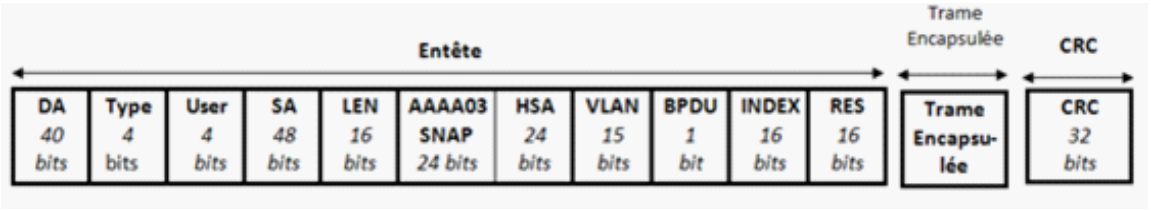


Fig. 3.7 -Structure de la trame ISL [3].

### 3.5.3 Notion des Trunks

Le réseau local est distribué sur différents équipements via des liaisons dédiées appelées Trunks. Un trunk est une connexion physique unique sur laquelle on transmet le trafic de plusieurs réseaux virtuels. Les trames qui traversent le trunk sont complétées avec un identificateur de réseau local virtuel (*VLAN id*). Grâce à cette identification, les trames sont conservées dans un même VLAN (*ou domaine de diffusion*) [35].

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

Ce schéma ci-dessous (Fig. 3.8), nous illustre la liaison de Trunk entre des commutateurs :

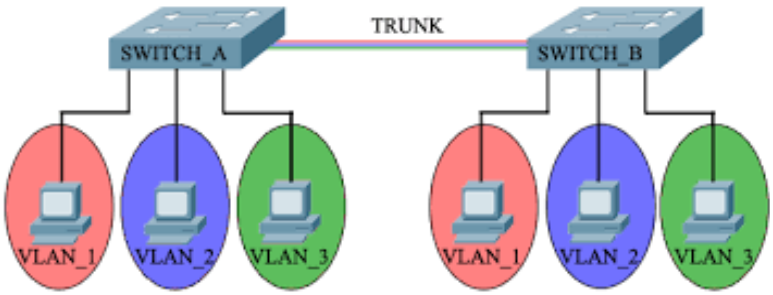


Fig. 3.8 - Utilisation de trunk entre deux commutateurs [35].

## 3.6 Protocoles d'administration et de gestion des VLANs

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

### 3.6.1 Protocole VTP (VLAN Trunking Protocol)

Afin de ne pas redéfinir tous les VLANs existant sur chaque commutateur, CISCO a développé un protocole permettant un héritage de VLANs entre commutateurs. C'est le protocole VTP, ce protocole est basé sur la norme 802.1q et exploite une architecture client-serveur avec la possibilité d'instancier plusieurs serveurs [36].

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

  Un commutateur doit alors être déclaré en serveur, on lui attribue également un nom de domaine VTP. C'est sur ce commutateur que chaque nouveau VLAN devra être défini, modifié ou supprimé. Ainsi chaque commutateur client présent dans le domaine héritera automatiquement des nouveaux VLANs crées sur le commutateur serveur. La mise en place d'un domaine VTP permet de centraliser la gestion des

VLANs, ce qui peut s'avérer plus que plaisant dans un environnement abondamment commuté et comprenant de multiples VLANs.

Les dispositifs de VTP peuvent être configurés pour fonctionner suivant les trois modes suivants [37]:

- **Mode serveur :** Dans lequel le commutateur est chargé de diffuser la configuration aux commutateurs du domaine VTP.

- **Mode client VTP :** Dans lequel le commutateur applique la configuration émise par un commutateur en mode serveur.

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

- **Exemple d'utilisation des VTP**

  Pour comprendre le fonctionnement des VTP, nous allons l'illustrer dans cet exemple ci-dessous (Fig. 3.9).

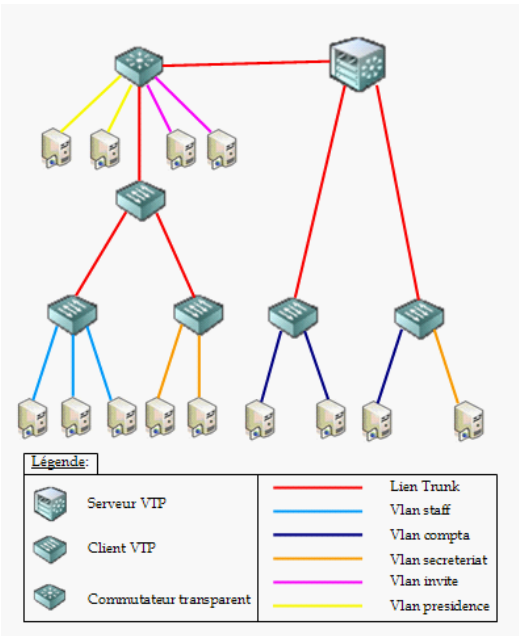


Fig. 3.9 - Fonctionnement du protocole VTP [37].

Les administrateurs peuvent changer les informations de VLAN sur les switchs fonctionnant en mode serveur uniquement. Une fois que les modifications sont appliquées, elles sont distribuées à tout le domaine VTP au travers des liens "Trunk". En mode transparent, les modifications sont locales mais non distribuées. Les switchs en mode client appliquent automatiquement les changements reçus du domaine VTP.

- Les configurations VTP successives du réseau ont un numéro de révision. Si le numéro de révision reçu par un switch client est plus grand que celui en cours, la nouvelle configuration est appliquée. Sinon, elle est ignorée. Quand un nouveau switch est ajouté au domaine VTP, le numéro de révision de celui-ci doit être réinitialisé pour éviter les conflits.

### 3.6.2 Protocol DHCP

DHCP signifie Dynamic Host Configuration Protocol. S'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau local d'obtenir dynamiquement (*c'est-à-dire sans intervention particulière*) sa configuration (*principalement, sa configuration réseau*). Vous n'avez qu'à spécifier à l'ordinateur de se trouver une adresse IP tout seul par DHCP. Le but principal étant la simplification de l'administration d'un réseau.

Le protocole DHCP sert principalement à distribuer des adresses IP sur un réseau, mais il a été conçu au départ comme complément au protocole BOOTP (*Bootstrap Protocol*) qui est utilisé par exemple lorsque l'on installe une machine à travers un réseau (*BOOTP est utilisé en étroite collaboration avec un serveur TFTP sur lequel le client va trouver les fichiers à charger et à copier sur le disque dur*). Un serveur DHCP peut renvoyer des paramètres BOOTP (*Bootstrap Protocol*) ou de configuration propres à un hôte donné [38].

- **Fonctionnement du protocole DHCP**

  Il faut dans le premier temps un serveur DHCP qui distribue des adresses IP. Cette machine va servir de base pour toutes les requêtes DHCP, aussi elle doit avoir une adresse IP fixe.

  Dans un réseau, on peut donc n'avoir qu'une seule machine avec adresse IP fixe, le serveur DHCP.

Le mécanisme de base de la communication est BOOTP (*avec trame UDP*). Quand une machine est démarrée, elle n'a aucune information sur sa configuration réseau, et surtout, l'utilisateur ne doit rien faire de particulier pour trouver une adresse IP. Pour faire ça, la technique utilisée est le broadcast : pour trouver et dialoguer avec un serveur DHCP, la machine va simplement émettre un paquet spécial de broadcast (*broadcast sur 255.255.255.255*) avec d'autres informations comme le type de requête, les ports de connexion sur le réseau local. Lorsque le serveur DHCP recevra le paquet de broadcast contenant toutes les informations requises pour le client.

### 3.6.3 Protocole Spanning-Tree

Le protocole Spanning-Tree (*STP*) est un protocole de conche 2 (*liaison de données*) conçu pour les switchs et les bridges. La spécification de STP est définie dans le document IEEE 802.1q.

Sa principale fonction est de s'assurer qu'il n'y a pas de boucles dans un contexte de liaisons redondantes entre des matériels de couche 2. STP détecte et désactive des boucles de réseau et fournit un mécanisme de liens de backup. Il permet de faire en sorte que des matériels compatibles avec le standard ne fournissent qu'un seul chemin entre deux stations d'extrémité [39].

### 3.6.4 ACLs (*Access Control Lists*)

Une liste de contrôle d'accès permet d'autoriser ou de refuser des paquets en fonctions d'un certain nombre de critères, tels que :

- L'adresse d'origine.
- L'adresse de destinataire.
- Le numéro de port.
- Les protocoles de conches supérieures.
- Autres paramètres (*exemple Horaire*).

Les listes de contrôle d'accès permettent à un administrateur de gérer le trafic et d'analyser des paquets particuliers. Elles sont ainsi associés à une interface du routeur, et tout trafic acheminé par cette interface est vérifié afin d'y déceler certains conditions faisant partie de la liste de contrôle d'accès.

1. **Types d'ACL**

   Il existe trois types de liste de contrôle d'accès :

   - **Listes de contrôle d'accès standard :** Utilisent des spécifications d'adresses simplifiées et autorisent ou refusent un ensemble de protocole. Les ACLs standard sont à appliquer le plus proche possible de la destination raison de leur fiable précision.
   - **Listes de contrôle d'accès étendues :** Utilisent des spécifications d'adresses plus complexes et autorisent ou refusent des protocoles précis. Les ACLs étendues sont à appliquer le plus proche possible de la source.
   - **Listes de contrôle d'accès nommées :** Peuvent être soit standard, soit étendues, elle n'a pour but que de faciliter la compréhension et de connaitre la finalité de l'ACL [40].

2. **Intérêt d'utilisation des ACLs :**

Voici des principales raisons pour lesquelles il est nécessaire de créer des listes de contrôle d'accès :

- Limiter le trafic réseau et accroître les performances, en limitant le trafic vidéo, par exemple, les listes de contrôle d'accès permettant de réduire considérablement la charge réseau et donc d'augmenter les performances.
- Fournir un niveau de sécurité d'accès réseau de bases, les lites de contrôle d'accès permettent à un hôte d'accéder à une section du réseau tout en empêchant un autre hôte d'avoir accès à la même section.
- Déterminer le type de trafic qui sera acheminé ou bloqué au niveau des interfaces de routeur. Il est possible d'autoriser l'acheminement des messages électroniques et de bloquer tout le trafic via Telnet.

- Autoriser un administrateur à contrôler les zones auxquelles un client peut accéder sur un réseau.

- Filtrer certains hôtes afin de leur accorder ou de leur refuser l'accès à une section de réseau. Accorder ou refuser aux utilisateurs la permission d'accéder à certains types de fichiers, tels que FTP ou http [41].

## 3.7 Conclusion

Nous avons vu tout au long de ce chapitre que la technologie des VLANs repose sur des concepts principaux et essentiels tels que la limitation des domaines de diffusion, la mobilité des utilisateurs et sans oublier le point important de notre but qu'est la sécurité. En effet, cette technologie est une nouvelle manière de mettre à profit la technique de la commutation pour donner plus de flexibilité aux réseaux locaux tout en gardant une sécurité assez fiable et moins coûteuse au sein de l'entreprise.

Toutes ces raisons nous ont motivées à proposer une solution pour sécuriser le réseau internet de Bejaia Mediteranean Terminal à base des VLANs, mais avant tout, nous devons d'abord étudier l'architecture actuelle du réseau de BMT afin de savoir comment organiser l'ensemble des utilisateurs dans des réseaux virtuels, et tout ça sera abordé dans le chapitre suivant.

CHAPITRE 4

# Présentation de l'organisme d'accueil

## 4.1 Introduction

L'objectif de ce chapitre est d'introduire l'organisme d'accueil par une brève description et d'encercler les missions principales de cet organisme, à savoir BMT (**Bejaia Mediteranean Terminal**).

Avant d'entamer notre étude, il convient de commencer par la présentation de l'entreprise et la détermination de notre position au sein du système d'information. On doit cependant donner un aperçu des améliorations finales de la démarche qu'on va mener, et montrer les objectifs à attendre par notre travail.

## 4.2 Spécification générales

Pour faire connaitre l'entreprise prestataire de services BMT, nous allons évoquer, tout d'abord, son historique, la situation géographique, ses structures, son organigramme, ses activités, ses missions, ses objectifs et enfin la présentation de département informatique.

### 4.2.1 Création l'entreprise de Bejaia Méditerrané Terminal

Dans son plan de développement 2004-2006, l'entreprise portuaire de Bejaia avait inscrit à l'ordre du jour le besoin d'établir un partenariat pour la conception, le financement, l'exploitation et l'entretien d'un terminal à conteneurs au port de Bejaia.

Dès lors L'EPB s'est lancée dans la tâche d'identifier les partenaires potentiels et a arrêté son choix sur le groupe PORTEK[(1)] une société Singapourienne spécialisée dans le domaine de la gestion des terminaux à conteneurs, et présente dans plusieurs ports à travers le monde. Le projet a été présenté au Conseil de la Participation de l'Etat (*CPE*[(2)]) en février 2004, le CPE a donné son accord au projet, en mai 2004.

Le CPE a donné son accord au projet, en mai 2004. Sur accord du gouvernement "BMT" a vu le jour avec la jointe venture de l'EPB à 51% et PORTEK à 49% [42].

### 4.2.2 Présentation de l'entreprise

BMT est une société par action (*SPA*), prestataire de services spécialisée dans le fonctionnement, l'exploitation, et la gestion du terminal à conteneurs. Pour atteindre son objectif, elle s'est dotée d'un personnel compétant, particulièrement formé dans les opérations de gestion du terminal. Elle dispose d'équipements d'exploitation les plus perfectionnées pour les opérations de manutention et d'acconage ,afin d'offrir des prestations de services de qualité, d'efficacité et de fiabilité en des temps records et à des coûts compétitifs [42].

1. **Situation géographique**

   L'entreprise BMT se situe au niveau du port de Bejaia, ce dernier est implanté au centre du pays et jouit d'une situation géographique stratégique.

   Elle se trouve à proximité de la gare ferroviaire, à quelques minutes de l'aéroport de Bejaia et est reliée au réseau routier national, ce qui facilite le transport des

[(1)] Fondé en 1988 à Singapour, le Groupe Portek est un opérateur portuaire spécialisé dans :

- La gestion des ports commerciaux

- La conception de solutions globales pour améliorer la capacité et la productivité portuaire

-La vente/leasing d'équipement portuaire

-L'ingénierie portuaire

[(2)] Est une instance gouvernementale instituée par l'ordonnance n°01-04 du 20 août 2001 relative à l'organisation, la gestion et la privatisation des entreprises publiques économiques.

marchandises conteneurisées de toutes natures vers l'arrière-pays et vers d'autres destinations telles que la banlieue d'Alger.

2. **Structure de l'entreprise**

   BMT possède cinq directions :

   **a. Direction Générale (*DG*) :**

   La direction dicte la stratégie à suivre par l'entreprise (*court, moyen et long terme*) et fixe les objectifs à atteindre. A sa tête le directeur général qui gère l'entreprise, a le pouvoir de décision, administre l'entreprise, assigne des directives pour les différentes structures et fait la liaison entre les directions d'entreprise.

   **b. Directions des Ressources Humaines (*DRH*)**

   Elle comprend les services suivants:

   - **Service personnel :** Mettre en œuvre des systèmes de gestion intégré à la stratégie de l'entreprise et qui traduisent une adéquation entre les impératifs économiques et les attentes du personnel. Pour cela la véritable importance de cette structure réside dans la recherche de meilleur potentiel et sa conservation en lui offrant les meilleures conditions (*salaire, formation, climat et environnement de travail,...*).
   - **Service des moyens généraux (*Achats et Projets*) :** Chargé des achats et de la gestion des stocks de l'entreprise.
   - **Administration et moyens (*Service hygiène et sécurité*) :** Assure la sécurité de la marchandise, du parc à conteneurs et la propreté de l'entreprise et de son environnement.

   **c. Direction des Opérations (*DO*)**

   Assure la planification des escales et du parc à conteneurs, et la planification des ressources (*humaines et matériels*).

   Elle prend en charge les opérations de manutention, comme la réception des navires porte- conteneurs et leurs chargement et déchargement, comme elle suit les opérations d'acconage telles que : les livraisons, les dépotages, les mises à disposition des conteneurs vides, et le traitement des conteneurs frigorifiques.

**d. Direction Marketing (DM)**

Veille à la marque de l'entreprise en se préoccupant en permanence d'entretenir des relations avec les clients. Elle vise à faire connaitre ses missions, ses programmes, ses orientations et ses performances auprès de ses clients. Elle amène son environnement externe à prendre conscience de l'importance de la démarche qu'elle entreprend dans le développement et l'amélioration de la qualité des services.

Elle comprend les services suivants :

- **Service commercial :** Suit la facturation, la gestion de portefeuille client et le recouvrement des créances.
- **Département informatique :** Assure le bon fonctionnement du CTMS, la maintenance du parc informatique de l'entreprise et le développement de nouvelles applications aux différentes structures.

**e. Direction des Finances et de Comptabilité (*DFC*)**

Procède à l'enregistrement de toutes les opérations effectuées par l'entreprise au cours de l'année. Elle est constituée de deux services :

- **Service de comptabilité :** Procède au contrôle et l'enregistrement de toutes les factures d'achat, de présentation et d'investissement.
- **Service des finances :** Procède au règlement de toutes les factures d'une part et à l'encaissement de toutes les créances de l'entreprise d'autre part.

**f. Direction Technique (*DT*)**

Assure une maintenance préventive et curative des engins du parc à conteneurs.

3. **Organigramme de l'entreprise :**

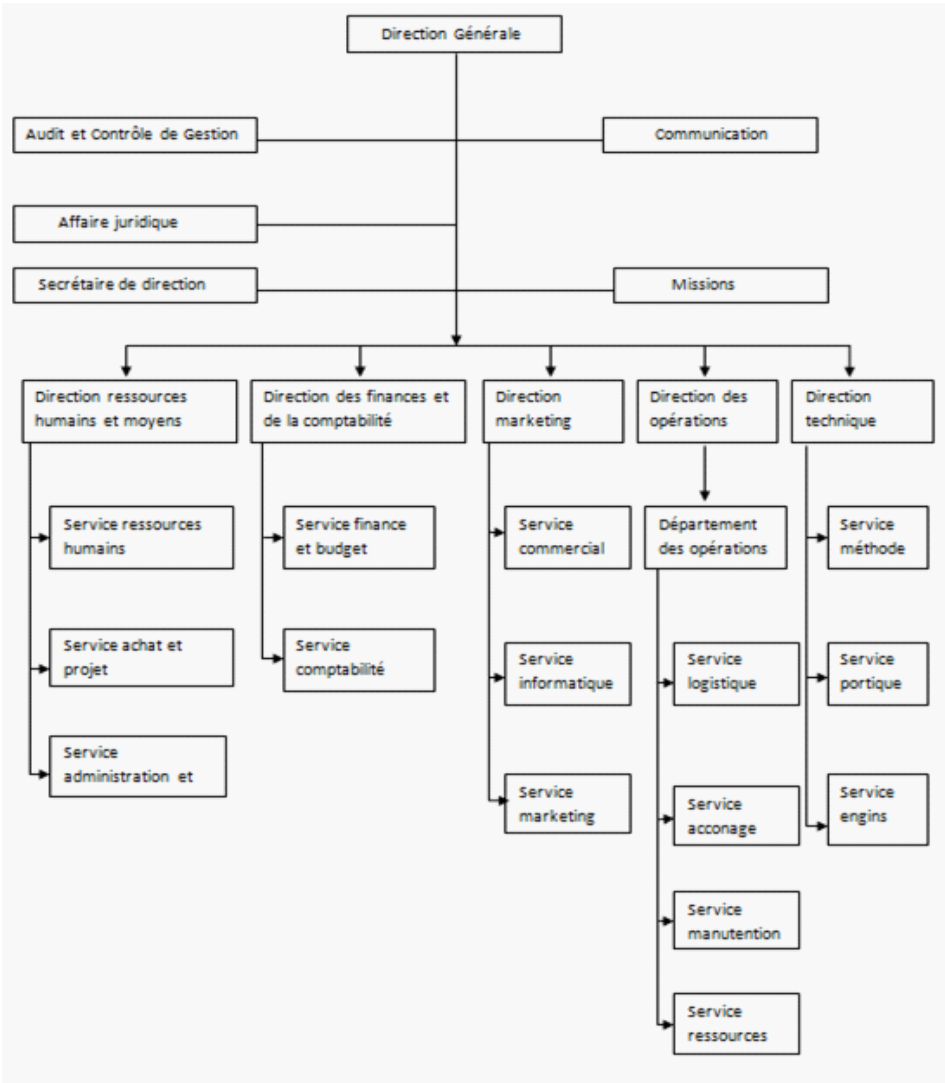


Fig 4.1 Organigramme général de BMT.

4. **Les activités de BMT et ses missions**

   L'activité principale de BMT est le suivi, la gestion et l'exploitation du terminal à conteneurs [43].

   BMT a pour mission principale de :

   - Traiter dans les meilleurs conditions de délais, de coûts et de sécurité, l'ensemble des navires porte-conteneurs et les conteneurs.
   - La manutention sur navire aussi bien que le chargement et déchargement des conteneurs et leurs entreposages dans les zones de stockage.

- Le service d'acconage sur les aires spécialisées ainsi que leurs livraisons.
- Le déchargement des céréales selon les capacités de BMT.

  Pour se faire, elle est dotée d'équipements performants et de système informatisé (*CTMS*) liés à la logistique pour pouvoir à la fois offrir des services de qualité, avec efficacité et fiabilité, et satisfaire ainsi aux différents besoins de ses clients.

5. **Objectifs de BMT**

   Faire du terminal à conteneurs de BMT une infrastructure moderne et répondre aux exigences les plus sévères en matière de qualité dans le traitement des conteneurs. La mise à disposition d'une nouvelle technologie dans le traitement des conteneurs pour [43] :

   - Un gain de productivité.
   - Une réduction des coûts d'escale.
   - Une fiabilité de l'information.
   - Un meilleur service.
   - Sauvegarder la marchandise des clients.
   - Faire face à la concurrence nationale et internationale.
   - Propulser le terminal au stade international.
   - Gagner des parts du marché :
     - Pour les conteneurs le passage de 20 à 30 conteneurs l'heure.
     - La réalisation de 150.000 EVP à l'horizon de 2015.
     - La création et la gestion d'un centre de formation.

## 4.3 Présentation du service d'accueil (Département Informatique)

### 4.3.1 Organisation

L'organigramme suivant (Fig.4.2) nous illustre les différentes sections du département Informatique:

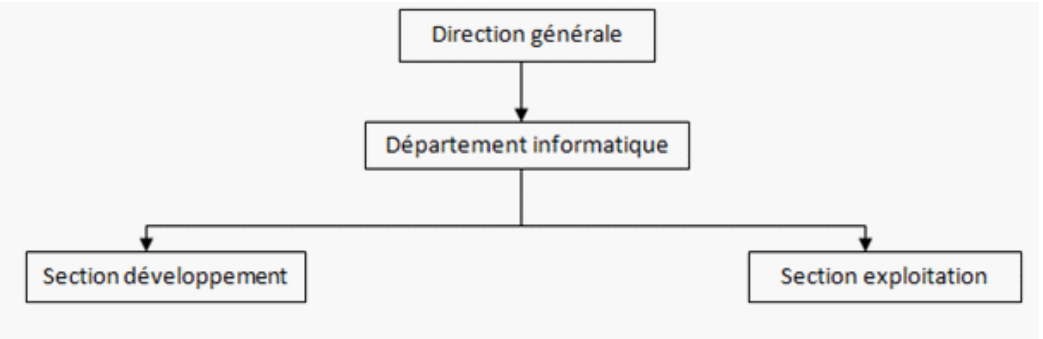


Fig. 4.2 - Organigramme du département informatique.

### 4.3.2 Activités de département d'informatique

C'est un service qui appartient à la direction marketing. Il est organisé en deux sections :

**a. Section développement :** ses principales fonctions sont [43]:

- Etudes et mise en place des nouvelles solutions.
- Maintenance et suivie des applications de gestions.
- Audit et amélioration du système d'information.
- Sauvegarde et contrôle des données de l'entreprise.
- Administration des serveurs de bases de données de l'entreprise.

**b. Section d'exploitation :**

- Administration des serveurs de la plateforme CTMS (*Container Terminal Management System*).
- Assurer les travaux reliés aux systèmes de communication.
- Assurer la maintenance préventive et curative du parc informatique.

## 4.4 Etude de l'existant

Une meilleure compréhension de l'environnement informatique aide à déterminer la portée du projet et la solution à implémenter [43].

Il est indispensable de disposer d'informations précises sur l'infrastructure réseau et les problèmes qui ont une incidence le fonctionnement du réseau.

En effet ces informations vont affecter une grande partie des décisions que nous allons prendre dans le choix de la solution et de son déploiement.

### 4.4.1 Réseau de BMT

1. **Présentation du réseau**

   Le réseau de BMT est un réseau Ethernet, il est basé sur la topologie étoile. La norme de câblage utilisée est T568B selon les types de périphériques à connecter, et d'une connexion Internet avec une antenne d'émission en mode WIMAX (World Wide Interoperabilite for Microware Access), elle sert à transmettre des données à haut débit par voie hertzienne en utilisant une fréquence radio privé et sécurisé [43].

   Le WIMAX est un standard de transmission de données sans fil, donné pour fonctionner à 70 Mb/s sur une portée de 50Km. Plus concrètement, le WIMAX ressemble de près au WIFI, mais avec des performances nettement supérieures.

2. **Architecture du réseau de BMT**

   Le réseau BMT est composé de deux réseaux [43] :

   - Le réseau CTMS LAN.
   - Le réseau INTERNET LAN.

     Le réseau CTMS (*Container Terminal Management System*) se présente sous l'architecture client/serveur. Il est composé de deux serveurs de bases de données sur lesquels est hébergée l'application CTMS qui tourne sous Oracle, et de deux serveurs d'application TOMCAT ainsi que de deux serveurs web Apache. Les serveurs web sont reliés à un Switch auquel sont branchés les postes de travail pour solliciter ces derniers, l'utilisateur passe une requête au serveur web en lui spécifiant l'information souhaitée, le serveur web à son tour passe la commande au serveur d'application qui consulte de la base de données et récupère le résultat de la requête, ce dernier renvoi le résultat au serveur web qui les affiche à l'utilisé.

     Le réseau LAN à un réseau WIFI et un réseau filière. Son adresse est 192.168.10.0 avec un masque 255.255.255.0, il a un serveur de fichier et un serveur d'intranet qui a pour but de gérer les applications de messageries et

d'internet. Un serveur de camera qui gère les camera de l'entreprise, un serveur NAS qui est un serveur de fichiers, il stocke des données

Le réseau LAN à un point d'accès qui est relié à un Switch CISCO avec 24 ports. Ce réseau à une connexion virtuelle avec une entelle WIMAX qui distribue la connexion pour le récepteur et émetteur Indoor, qui distribue la connexion à son tour d'une façon numérique pour le routeur Fortigate, ce dernier a pour rôle de pare feu, on suite la connexion passe ou Switch qui à 24 port puis ou post client.

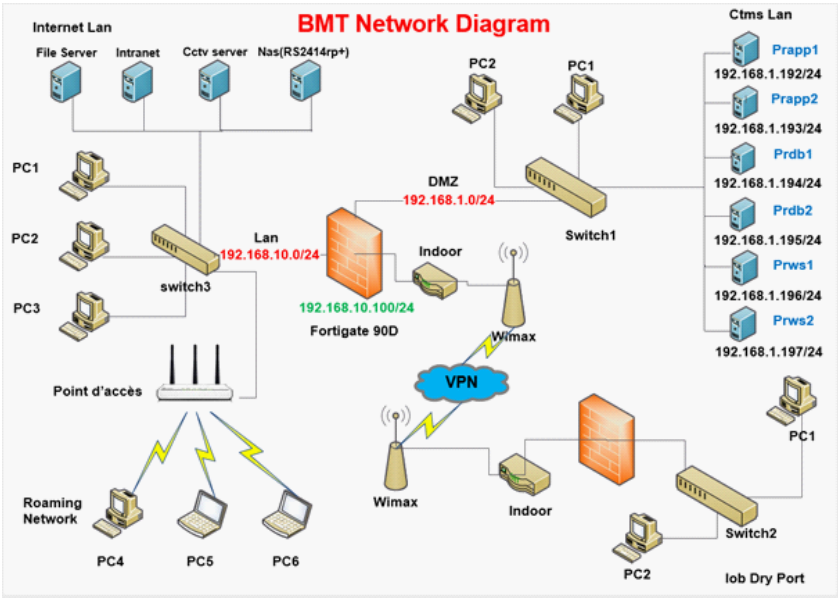


Fig. 4.3 - Architecture du réseau de BMT [43].

3. **Politique de sécurité du réseau en place**

La gamme de firewalls Fortigate est une solution Appliance complète dont les fonctions de sécurité sont très développées. Fortinet est aujourd'hui le leader reconnu sur le marché des firewalls UTM (*Unified Threat Management*) [43].

- **Firewall :** règles de filtrage simples pour n'accepter que les flux autorisés.
- **VPN ipsec :** La fonction VPN ipsec vous permet de mettre en place des tunnels chiffrés vers d'autres sites ou bien pour des nomades.
- **VPN SSL :** Accès chiffrés pour vos nomades, en mode tunnel ou portail web (*seul un navigateur suffit*).

- **Antivirus réseau :** filtre antiviral de flux web (*TTTP, HTTPS, FTP*) et de messagerie (*SMTP, SMTPS, IMAP,... etc.*)
- **Anti-spam :** fonction Anti-spam pour vos flux de messagerie.
- **Filtrage URL :** Filtrage des accès WEB à l'aide de 76 catégories référençant de 2 milliards de pages web. Avec une authentification Idap (*Active Directory et Edirectory sont supportés en mode d'authentification transparente*), possibilité de mettre en place une politique d'accès par type de population.
- **Détection d'intrusions :** Sécurisation des accès entrants et sortants. La remise à jour automatiquement.
- **Contrôle applicatif :** Filtrage direct des applications afin de maitriser avec une très forte granularité votre politique de sécurité.
- **Optimisation Wan :** Optimisation des liaisons Wan pour économiser de la bande passante. Seuls les modèles Fortigate disposant d'un espace de stockage supportent cette fonction.
- **Inspection SSL :** Déchiffrage des flux pour analyser le contenu et contrer attaquent malware. Seuls les modèles les plus récents permettent ce traitement.
- **D'autres fonctions :** Possibilité d'utiliser plusieurs liaisons internet, routage par la source, routage dynamique, équilibrage de charge et haute disponibilité d'une application, gestion de bande passante.

## 4.5 Problématique

Lors de l'étude du réseau BMT, de nombreuses insuffisances ont été découvertes, qui nous a permis également de définir un nombre important de contraintes pouvant réduire ses performances voir le dégrader. Ainsi on note:

1. 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.

2. Un seul domaine de diffusion

    - Un seul et unique domaine de diffusion ce qui implique une surcharge du réseau de l'entreprise.

3. 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.

## 4.6 Solutions proposées

L'objectif de notre travail est de renforcer la sécurité du réseau local et renforcer une meilleure gestion, pour cela:

Nous devons faire quelques modifications dans l'architecture du réseau BMT, et utiliser les VLANs afin d'améliorer la sécurité du réseau local.

En effet cette solution est adéquate, en vue des avantages qu'elle offre.

Il nous faudra également insérer des listes de contrôles d'accès dans le routeur afin d'offrir une couche de sécurité supplémentaire.

## 4.7 Conclusion

Ce chapitre nous a permet une bonne compréhension des services de l'entreprise BMT dans laquelle nous avons suivi notre stage pratique, et d'acquérir de nouvelles connaissances dans la mise en place et l'administration de réseau actuel de BMT, ce qui nous a conduit à voir des lacunes et ses faiblesses, l'étude de ces dernières nous a conduit à proposer des solutions pour les paliers.

Dans le chapitre qui suit nous allons présenter le simulateur Packet Tracer et décrire les étapes de la mise en œuvre des solutions proposées

CHAPITRE 5

# Proposition d'une solution et mise en oeuvre

## 5.1 Introduction

Dans le but d'illustrer et de compléter ce qui a été traité dans la partie théorique de notre mémoire, plus exactement dans le deuxième et troisième chapitre, nous faisons une simulation de réseau informatique de l'entreprise BMT, en commençant par une étude de l'existant puis en configurant sur ce dernier les équipements utilisés en appliquant le sécurité des VLANs.

Dans ce chapitre, nous présentons le logiciel utilisé et l'environnement de travail ainsi que les différentes configurations utilisées, enfin nous donnerons les résultats obtenus de la configuration.

## 5.2 Présentation de simulateur "Cisco Packet Tracer"

Packet tracer est un simulateur de réseau puissant développé par Cisco Systems pour faire des plans d'infrastructure de réseau en temps réel. il offre la possibilité de créer, visualiser et de simuler les réseaux informatiques. l'objectif principal de simulateur est de schématiser, configurer et de voir toutes les possibilités d'une future mise en oeuvre réseau. Cisco Packet Tracer est un moyen d'apprentissage de la réalisation de divers réseaux et découvrir le fonctionnement des différents éléments constituant un réseau informatique [44].

La figure 5.1 est une image montrant l'nterface pricipale du simulateur Cisco Packet Tracer:

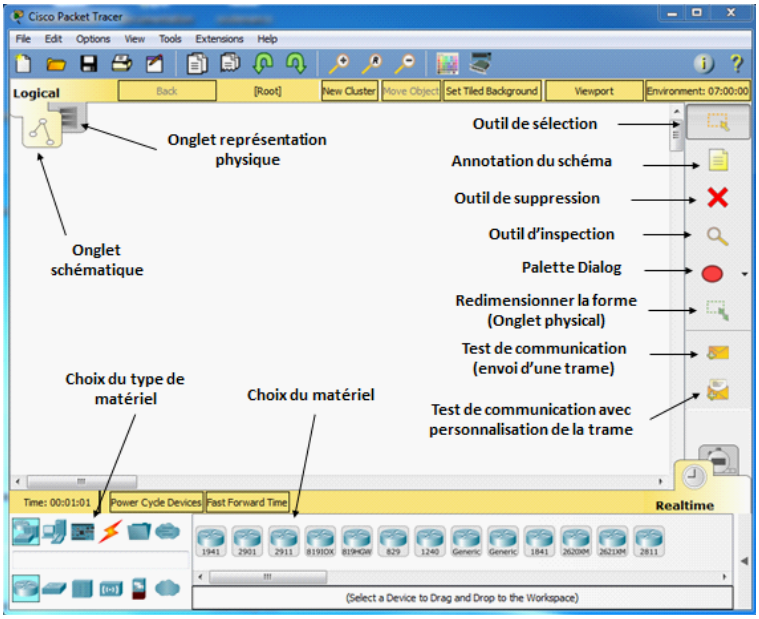


Fig. 5.1 - L'interface de simulateur "Cisco Packet Tracer".

## 5.3 Interface commande de Packet Tracer

Toutes les configurations des équipements du réseau, c'est au niveau de CLI(Command Language Interface) quelques seront réalisées. CLI est une interface de simulateur Packet Tracer qui permet la configuration des équipements du réseau à l'aide d'un langage de commandes, c'est-à-dire qu'à partir des commandes introduites par l'utilisateur du ligiciel, que la configuration est faite [44].

La figure 5.2 est l'interface CLI du Packet Tracer:

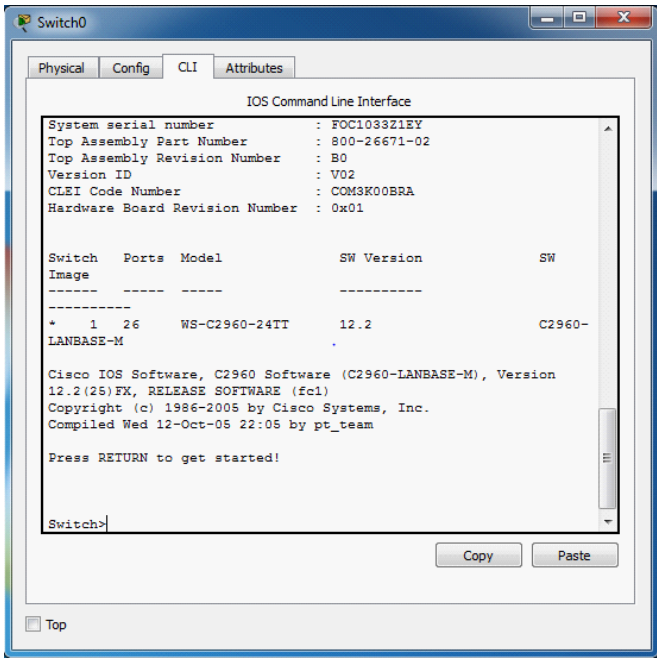


Fig. 5.2 - Interface CLI.

## 5.4 VLANs du réseau de l'entreprise de BMT et leur plan D'adressage

l'adresse du réseau est 192.168.10.0/24 avec une possibilité de création de 255 sous réseaux, avec un masque 255.255.255.0 l'adressage du réseau local et de toutes stations, se basera sur une adresse privée. les machines affiliées a un VLAN, vont prendre toutes les adresses IP d'une mêê adresse sous-réseau. les VLANs du réseau BMT sont: Serveur, DG, DRH, DO, DM, DFC, DT et Wifi.

## 5.5 Structure générale du réseau de l'entreprise de BMT

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

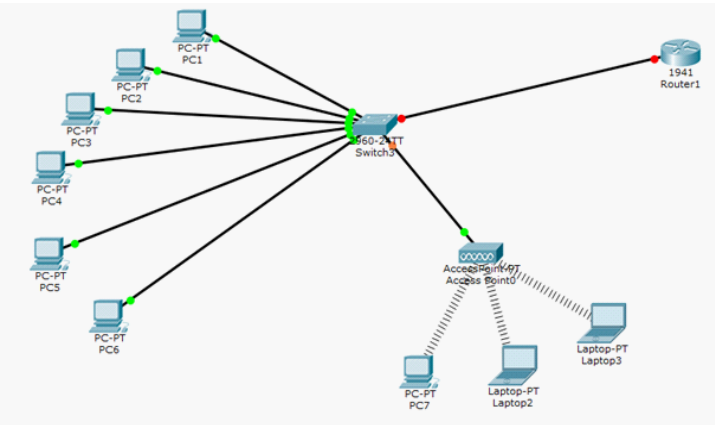


Fig. 5.3 - Architecture du réseau de BMT avant l'amélioration.

On a proposé de relier le Switch fédérateur aux deux Switch de la couche d'accès qui seront relié à leur tour aux Switch de distribution qui se trouve dans chaque service comme le montre la figure ci-dessous.

L'utilisation des VLANs pour la segmentation de réseau nous permettra de créer un ensemble logique isolé pour augmenter le niveau de la sécurité en isolant les utilisateurs accédant aux données sensibles.

On découpe le LAN en plusieurs VLANs en utilisant la segmentation par sous-réseau, chaque direction aurais son propre VLAN, ça permettra un échange d'informations plus sécuriser et augmente la qualité de la bande passante. La figure (Fig. 5.3) suivante illustre

la nouvelle architecture aprés l'amélioration.

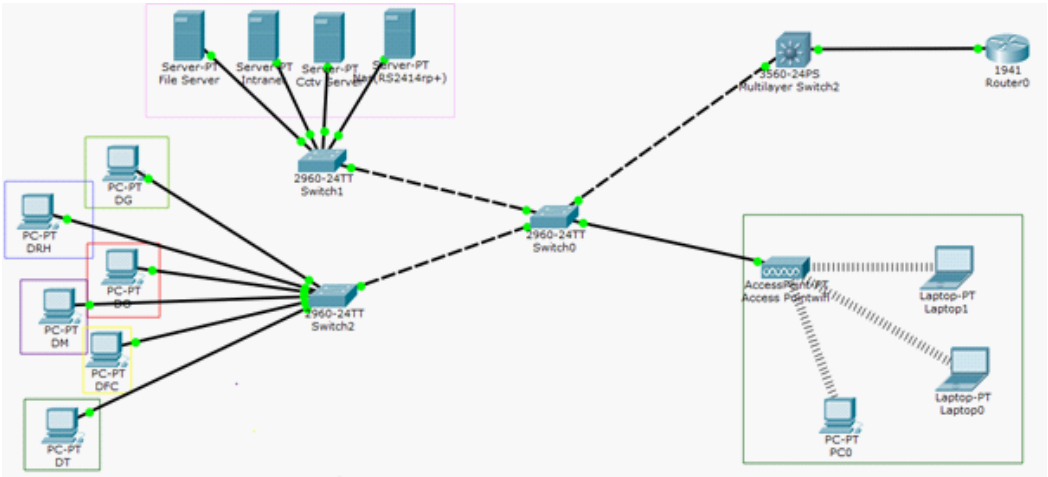


Fig. 5.4 - La nouvelle Achitecture du réseau BMT.

## 5.6 Configuration des équipements

La configuration des équipements du réseau sera au niveau du commutateur de niveau 3 du modèle OSI (réseau) constituants le réseau local des stations. En effet, une série de configuration sera réalisée à travers ces équipements, en montrant un exemple de chaque configuration.

### 5.6.1 Sécuriser l'accès aux périphériques

Il faut savoir qu'ISO[(1)] utilise des modes organisés hiérarchiquement pour faciliter la protection des périphériques. Dans le cadre de ce dispositifs de sécurité, ISO peut accepter plusieurs mots de passe, ce qui nous permet d'établir différent privilèges d'accès au périphérique.

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

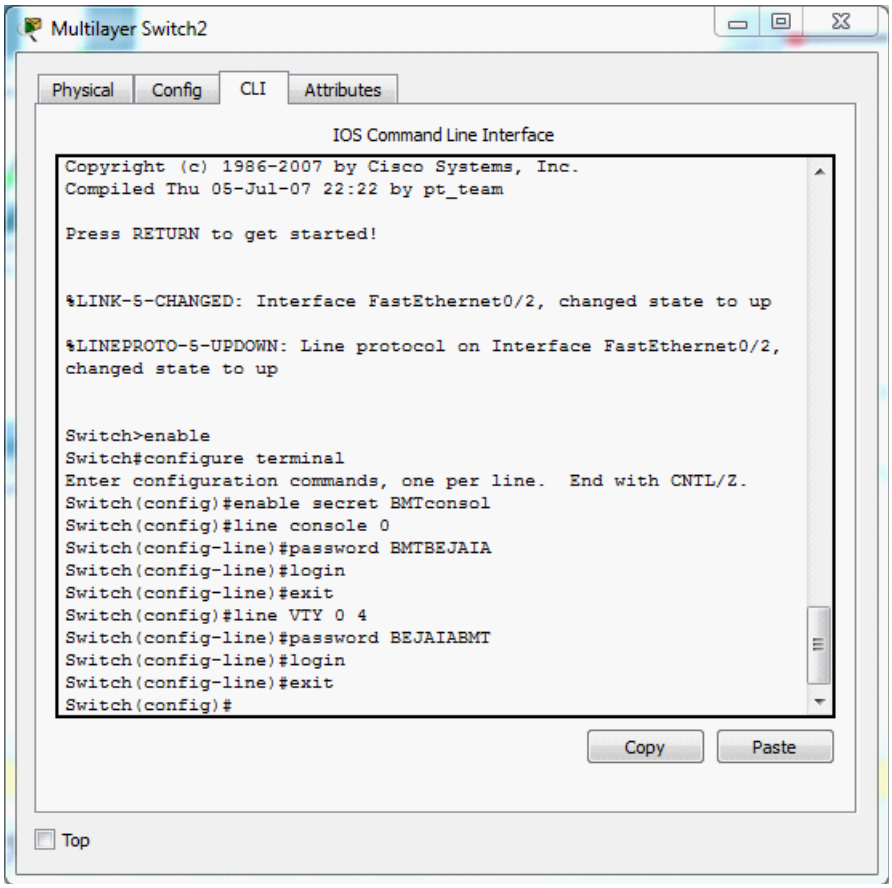


Fig. 5.5 - Configuration de mot de passe.

### 5.6.2 Configuration du serveur VTP sur le switch multifonction

le protocole VTP est propriétaire Cisco permet aux commutateurs et routeurs qui l'implémentent, d'échanger des informations de configuration des VLANs. La figure suivante nous permet de voir la configuration du VTP server:

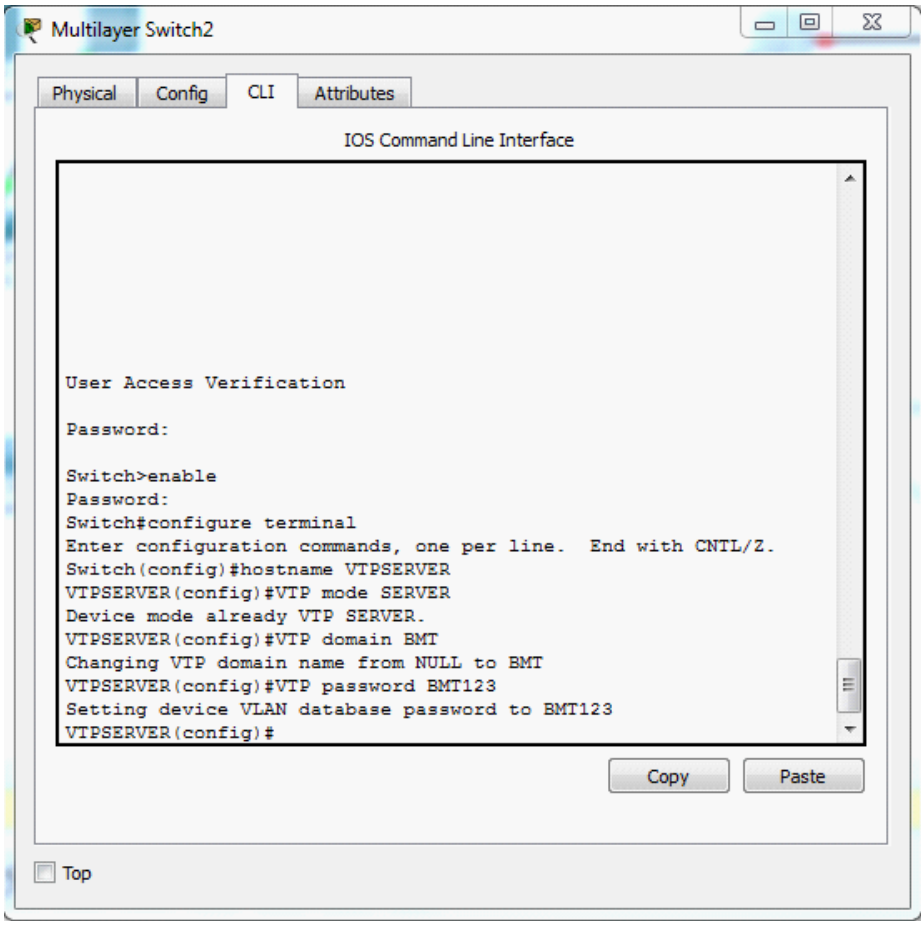


Fig. 5.6 - Configuration du serveur VTP sur le switch Multifonction

### 5.6.3 Configuration des VLANs

La configuration des VLANs est faite au niveau des commutateurs dans le réseau, comme le montre le figure ci-dessous:

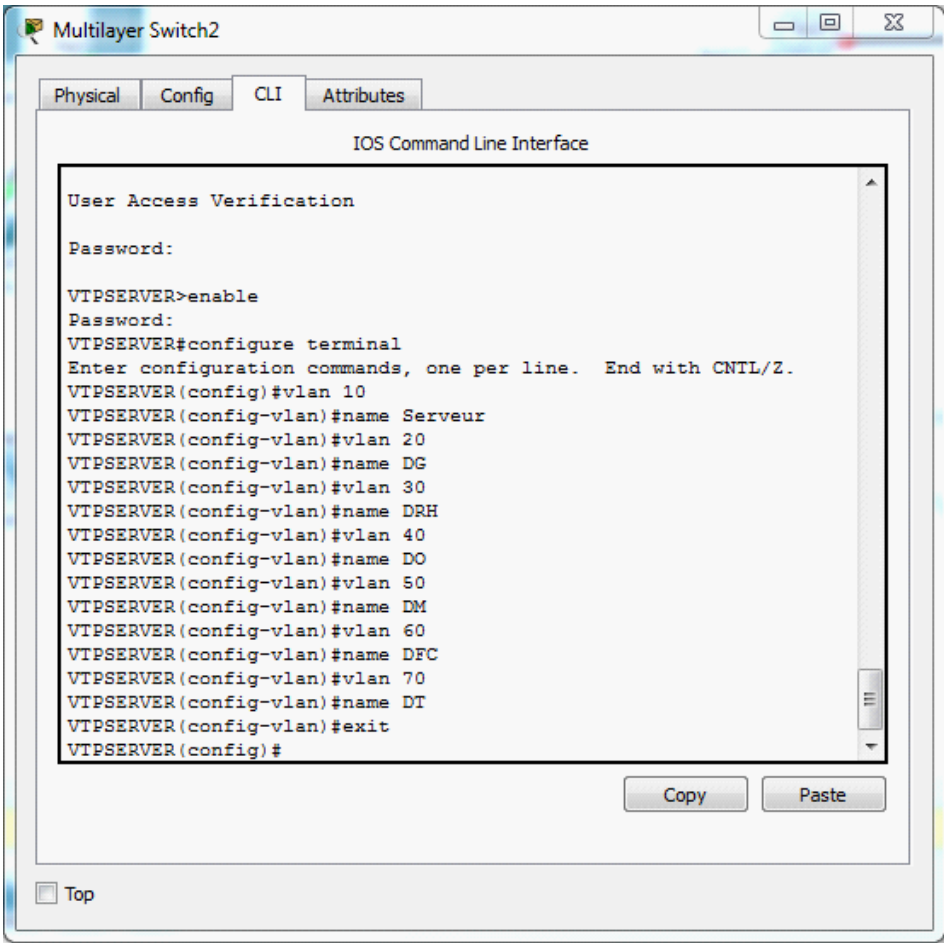


Fig. 5.7 - Création des VLANs.

Il existe deux mode d'association d'un port au VLAN

- **Mode accès**

La commandes suivantes nous permettent d'associer les ports au VLANs en mode accès:

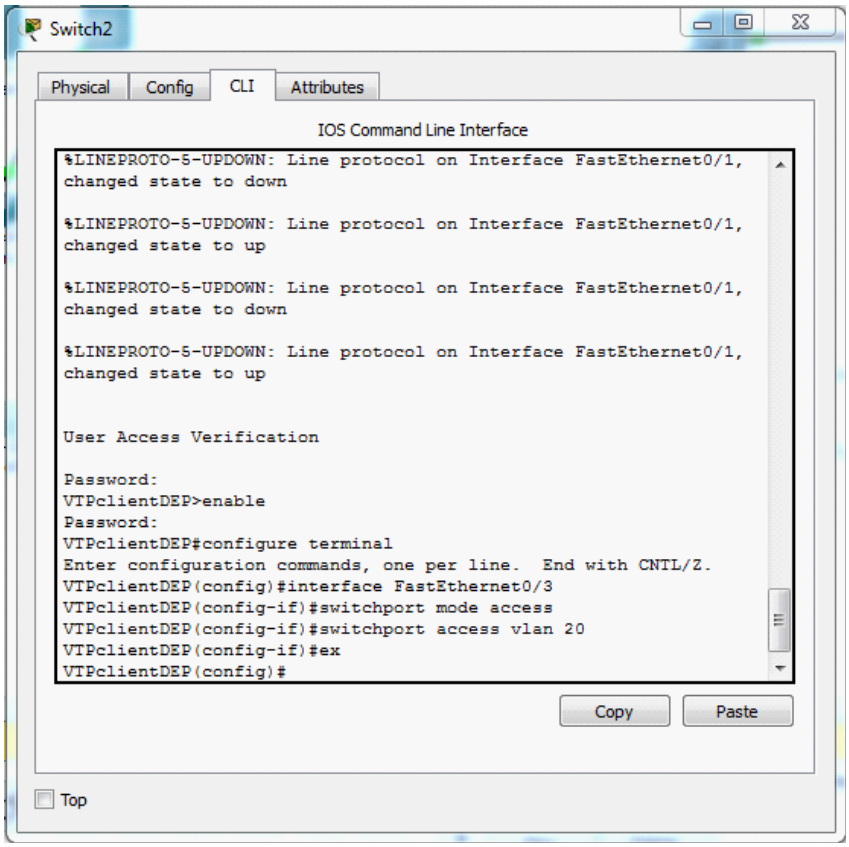


Fig. 5.8 - Attribution des ports aux VLANs.

- **Mode Trunk**

Les interfaces des équipements d'interconnexion à configurer en mode trunk existent toutes entre l'ensemble des commutateurs Accès et le commutateur multi-fonction.

les commandes suivantes nous permettent d'associer les ports au VLANs en mode trunk:

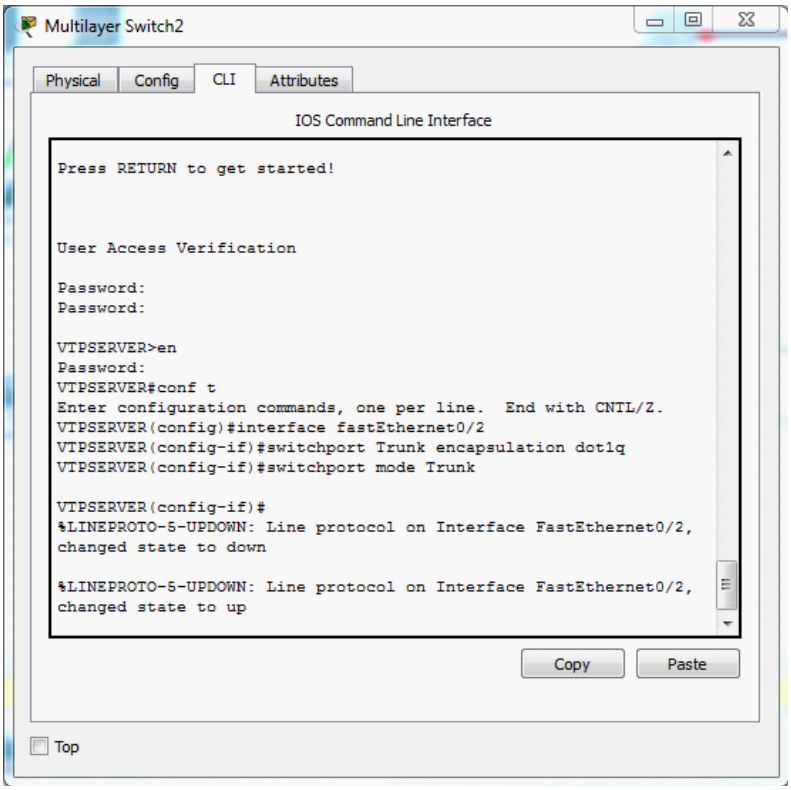


Fig. 5.9 - Configuration des liens Trunk au niveau de la multi-fonction.

### 5.6.4 Configuration DHCP

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

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

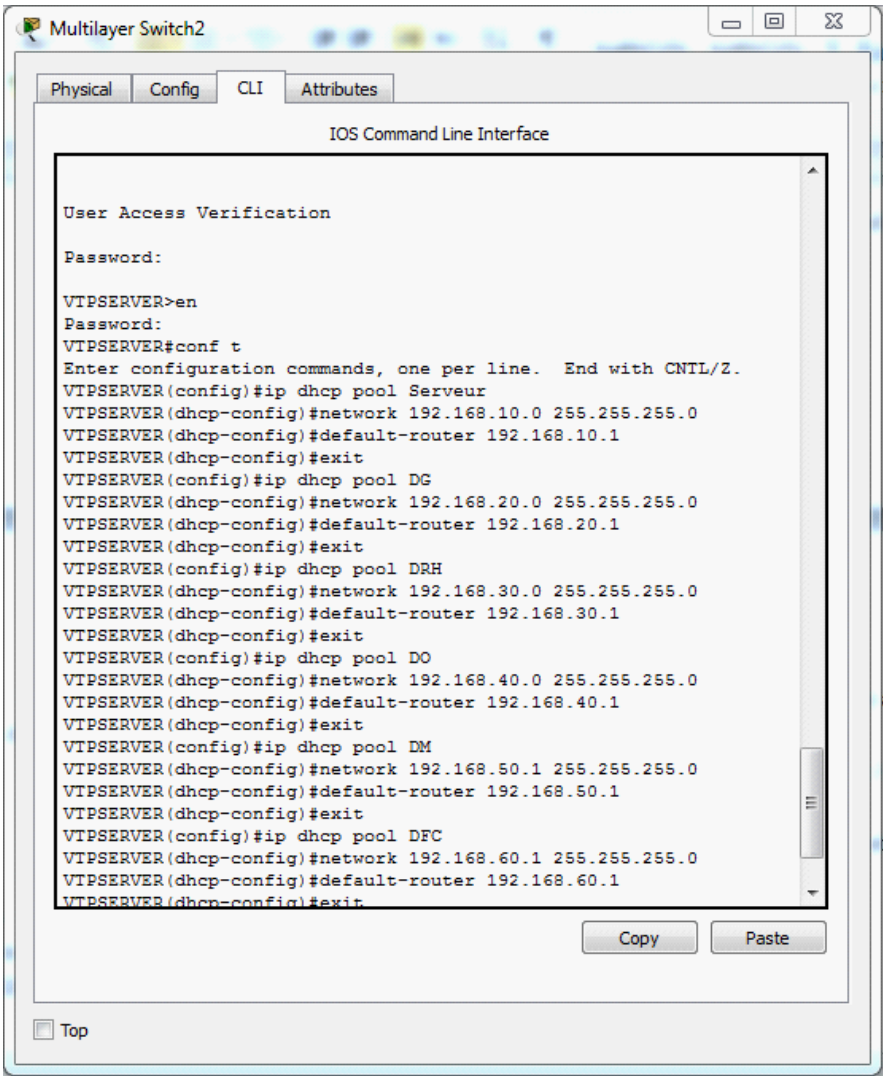


Fig. 5.10 - Configuration DHCP.

### 5.6.5 Routage inter-VLAN

Le routage inter-Vlans permet à plusieurs Vlans différents de communiquer la figure ci-dessous nous montre les commande obligatoire pour réussir le routage:

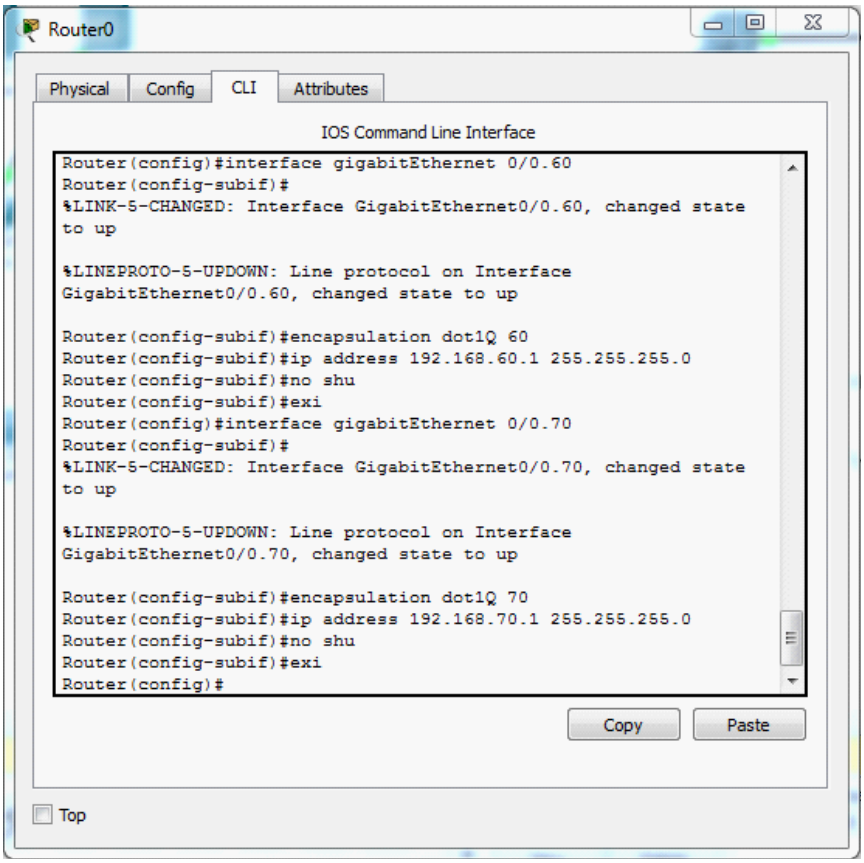


Fig. 5.11 - Le routage inter-VLANs.

### 5.6.6 Configuration du Point d'accès Wifi

Pour la configuration des points d'accès Wifi, nous prendront pour exemple un point d'accès Wifi. Les figures suivantes nous illustrent la configuration du point d'accès et les Laptop (Fig.5.12 et Fig.5.13):

1. **Configuration des points d'accès**

Nous allons commencer par la configuration de point d'accès (Access pointwifi).

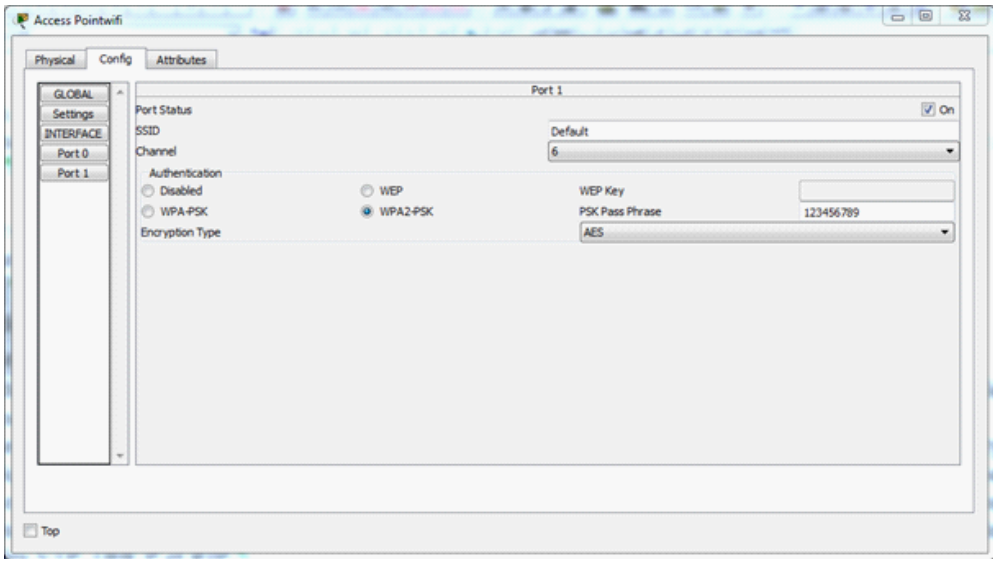


Fig. 5.12 - Configuration du point d'accès (Access Pointwifi).

2. **Configuration des Laptops**

Nous allons maintenant introduire la même clé wifi au niveau du Laptop, afin que ce dernier puisse ce connecter au point d'accès Wifi.

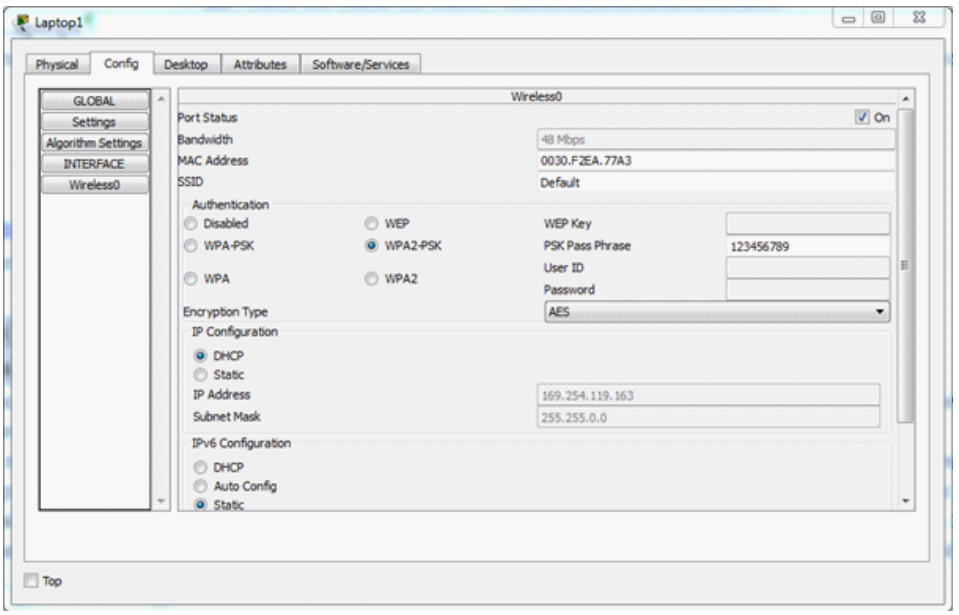


Fig. 5.13 - Configuration du Wifi sur le Laptop.

Aprés l'introduction du mot passe correct, le Laptop est connecté.


Fig. 5.14 - La connexion au point d'accès wifi est établie.

### 5.6.7 Le test de validation

La figure suivante nous illustre le test de validation (Fig.5.15):

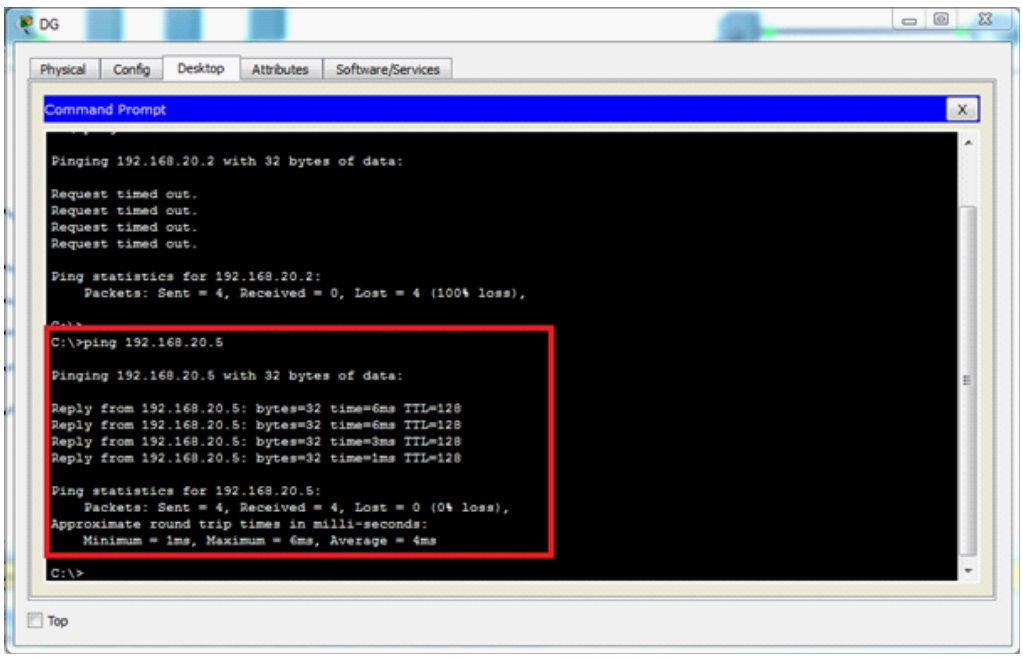


Fig. 5.15 - Ping réussi entre le pc DG et le pc DRH.

## 5.7 Conclusion

Dans ce chapitre, nous avons présenté la nouvelle architecture logique du réseau local de Bejaia Mediteranean Terminal basée sur les VLANs.

Pour cela, nous avons procédé à l'organisation du réseau de l'entreprise au département dans des réseaux virtuels en fonction de leurs fonctionnalités, aussi nous avons choisi la méthode par port pour la création des VLANs car elle procure le niveau de sécurité le plus élevé.

Les réseaux virtuels ainsi implémentés nous ont montré une amélioration au niveau sécurité. En effet de point de vue sécurité, les tests que nous avons fais ont montré que les frontières entre les différents VLANs sont infranchissables. Finalement, nous avons configuré le routeur afin de permettre le routage inter-VLANs.

# Conclusion

L'étude du réseau local de l'entreprise BMT, nous a permis de mettre en place des VLANs dans une nouvelle architecture que nous avons proposé pour son site principal.

Dans notre travail, nous avons abordé les généralités sur les réseaux locaux virtuels notamment, leurs différents types et leurs utilités, ainsi quelques protocoles d'administration VTP et DHCP qu'on a implémenté sur notre architecture réseau.

Notre travail est réalisé selon une définition du contexte du projet et critique de l'architecture existante, puis on a proposé une nouvelle architecture réseau adaptée à la topologie physique actuelle de l'organisme d'accueil, enfin on a créé des VLANs avec des protocoles VTP et DHCP.

En effet, nous avons constaté l'intérêt les VLANs, ainsi les protocoles VTP et DHCP dans l'amélioration de la qualité de transmission d'information et plus de souplesse dans l'amélioration d'un réseau local. Pour un réseau informatique de l'entreprise BMT, qui va lui permettre une augmentation considérable des performances du réseau.

Ce travail nous a fait l'objet d'une expérience intéressante, et a eu énormément d'apport sur nos connaissances et nos compétences en terme de configuration dans un environnement Cisco. De plus, nous avons enrichi nos connaissances déjà acquises dans la segmentation des réseaux locaux d'entreprises en VLANs.

# Bibliographie


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

[2] José DORDOIGNE, *Réseaux informatiques Notions fondamentales (Protocoles, Architectures, Réseaux sans fil, Virtualisation, Sécurité, IP v6,...)*. Editions ENI, Janvier 2013.

[3] GILBERT Held, *les réseaux locaux virtuels, Conception, mise en œuvre et administration.* Août 1998.

[4] Sylvain, *le modèle TCP/IP*, source " http://www.frameip.com/tcpip/ ", 2003.

[5] K.TOUAHRI et J.TIDJET. *Sécurité du réseau intranet de l'Université de Béjaia : Implémentation d'une solution avec VLANs*, 2007/2008.

[6] Claude SERVIN. *Réseaux et Télécoms*. Editions DUNOD, 2003, 2006, 2009.

[7] Clément Michael. *Le protocole TCP/IP*, Octobre 2002. pdf.

[8] Fréderic Jacquenod, *cours réseaux : les matériels d'interconnexion*, source "http://www.netalya.com/fr/reseaux5.asp".

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

[10] Khelalfa, Halim M, *Introduction à la sécurité Informatique*, SECINFO04,2000.

[11] Joelle MUSSET. *Sécurité Informatique : Ethical hacking : Apprendre l'attaque pour mieus se défendre*, 2009.

[12] *Support de cour réseau EISTI* ,"http:// www.elstl.fr", 02.05.2016.

[13] LESCOP Yves V1.6, *Sécurité informatique.pdf*, 2002.

[14] A. Mokhetari, *La sécurité dans les Echanges et la Sauvegarde des Données*, Université de Versailles.2000-2001.

[15] M.Badra, *Le transport et la sécurisation des échanges sur les réseaux sans fil*, thèse de doctorat, l'Ecole Nationnale Supérieure des Télécommunications, 2004.

[16] BELHADI Hakima, *La sécurité des données informatique cryptographier*, mémoire de fin d'études master 2, université de Béjaia .2010/2011.

[17] Mattheui Herrb Jean- Luc Archimaud, *Certificats électroniques.pdf* ,Février 2002.

[18] Sreven André, Brian Kenyon, and Erik Pack Birkholz, *Security Sage's guide to hardening the network infrastructure*. Syngress, 2000.

[19] TOM Thomas,*La sécurité des réseaux first-step*, ISBN : 2-7440-8,2005.

[20] Guillaude Desgeorge, *La sécurité des réseaux*, 2000. "http://www.guill.net/reseaux/La sécurité des réseaux.html".

[21] Marc BOGET, *étude des vulnérabilités d'un grand réseau d'entreprise et solutions de sécurité* ,2003.

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

[23] Adrien Miller and Pilippe Jean Dit Pannel, *Sécurité avec ip : Les solutions*. 2003.

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

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

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

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

[28] Rogner SANCHEZ, *Les réseaux locaux virtuels (VLAN) CERTA*, Janvier.

[29] François Santy. *La virtualisation*, 2013.

[30] David Passmore John Feeman,*The Virtual LAN Technology Report*. May 1998.

[31] *Etude et optimisation du réseau local de inova* si - Toussaint KOUASSI.html.

[32] Philippe NOLL, *les_ VLAN.pdf.*

[33] *Le grand livre de securitéinfo*, "http://www.securiteinfo.com", février 2004.

[34] *Analysing the InterSwitch Link protocol, CISCO network ACADEMY*, "http://www.firemalle.cx/vlan.php".

[35] F.NOLOT, *cours les virtual LAN, Université de Reims Champagne – Ardenne*, "http://www.nolot.eu/Downlaod/Cours/rezo/AdminRS-Cours2-VLAN.pdf".

[36] E.NOBIET, *Procédure VLAN Trunking Protocol*, "http://nobileteric.weebly.com/uploads/2/9/6/6/29668301/proc%C3%A9dure-vtp.pdf".

[37] Florent Nolot, *Des protocoles de Spanning Tree*, Master2 informatique, Université de Reims, 2008.

[38] Collectif, *Dictionnaire Hachette encyclopédie illustré* , Paris, Ed. Hachette livre, 1998.

[39] A.AUBERT, *Apprentissage et suppression de boucle*, Télécom Saint-Etienne.

[40] S.BOUBALOU et M.YOUSFI, *Proposition d'une configuration sécurisée d'un réseau local Cas d'étude : Entreprise NAFTAL*, 2015/2016.

[41] I.REDOUANE et Y.AMAOUCHE, *Proposition d'une nouvelle architecture LAN et implémentation d'une solution VLAN cas : SARL ifri , 2015/2016* .

[42] "www.Bejaiamed.com".

[43] BOUFALIOUNE Kahina, *La mise en place d'un serveur DES sous windows server 2012 R2*, 2014/2015.

[44.] *Simulation du fonctionnement d'un réseau informatique*, Académie de LYON, source "http://sen.arbrezcarme.free.fr/_atelier/3.3-rotation-3-ToutEnBois/3.3.6-Simulation-du-fonctionnement-d-un-reseau-informatique.pdf".

# Liste des figures

# Liste des Abréviations

| | |
|---|---|
| **AAA** | **A**uthentication **A**uthorization **A**ccounting. |
| **ACL** | **A**ccess **C**ontrol **L**ists. |
| **BMT** | **B**ejaia **M**editerranean **T**erminal. |
| **BOOTP** | **B**oot **s**trap **P**rotocol. |
| **CFI** | **C**anonical **F**ormat **I**dentifier. |
| **CAU** | **C**ontrolled **A**ccess **U**nit. |
| **CPE** | **C**onseil de la **P**articipation de l'**E**tat. |
| **CRC** | **C**ontrol **R**edundancy **C**heck. |
| **CTMS** | **C**ontainer **T**erminal **M**anagement **S**ystem. |
| **DFC** | **D**irection des **F**inances et de **C**omptabilité. |
| **DG** | **D**irection **G**énérale. |
| **DHCP** | **D**ynamic **H**ost **C**onfiguration **P**rotocol. |
| **DM** | **D**irection **M**arketing. |
| **DMZ** | **D**e **M**ilitarized **Z**one. |
| **DO** | **D**irection des **O**pérations. |
| **DRH** | **D**irections des **R**essources **H**umaines. |
| **DT** | **D**irection **T**echnique. |
| **EPB** | **E**ntreprise **P**ortuaire **B**ejaia. |
| **ETCD** | **E**quipement **T**erminal de **C**ircuit de **D**onnée. |
| **FTP** | **F**ile **T**ransfer **P**rotocol. |
| **H-IDS** | **H**ost based **I**ntrusion **D**etection **S**ystem. |
| **HTTP** | **H**ypertext **T**ransfer **P**rotocol. |

**IDS** **I**nstruction **D**etection **S**ystem.

**IMAP** **I**nternet **M**essage **A**ccess **P**rotocol.

**IP** **I**nternet **P**rotocol.

**IPSec** **I**nternet **P**rotocol **S**ecurity.

**IPV4** **I**nternet **P**rotocol **V**ersion **4**.

**IPV6** **I**nternet **P**rotocol **V**ersion **6**.

**ISL** **I**nter **S**witch **L**ink Protocol.

**ISO** **I**nternational **S**tandards **O**rganization.

**LAN** **L**ocal **A**rea **N**etwork.

**PPTP** **P**oint to **P**oint **T**unneling **P**rotocol.

**MAC** **M**edia **A**ccess **C**ontrol.

**MAN** **M**etropolitan **A**rea **N**etwork.

**MAU** **M**ultistation **A**ccess **U**nit.

**MD5** **M**essage **D**igest **5**.

**N-IDS** **N**etwork based **I**ntrusion **D**etection **S**ystem.

**OSI** **O**pen **S**ystem **I**nterconnction.

**PAN** **P**ersonal **A**rea **N**etwork.

**POS** **P**ersonal **O**perating **S**pa.

**PPP** **P**oint to **P**oint **P**rotocol.

**PPTP** **P**oint to **P**oint **T**unneling **P**rotocol.

**L2F** **L**ayer **T**ow **F**orwarding.

**L2TP** **L**ayer **T**wo **T**unneling **P**rotocol.

**RLE** **R**éseau **L**ocal d'**E**ntreprise.

**SHA** **S**ecure **H**ash **A**lgorithm.

**SI** **S**écurité **I**nformatique.

**SMTP** **S**imple **M**ail **T**ransfer **P**rotocol.

**STP** **S**panning **T**ree **P**rotocol.

**SSL** **S**ecure **S**ocket **L**ayer.

| | |
|---|---|
| **TCI** | **T**ag **C**ontrol **I**nformation. |
| **TPID** | **P**rotocol **I**dentifier. |
| **TCP** | **T**ransmission **C**ontrol Protocol. |
| **TFTP** | **T**rivial **F**ile **T**ransfer **P**rotocol. |
| **UDP** | **U**ser **D**atagram **P**rotocol. |
| **URL** | **U**niform **R**esource **L**ocator. |
| **VLAN** | **V**irtual **L**ocal **A**rea **N**etwork. |
| **VPN** | **V**irtual **P**rivate **N**etwork. |
| **VTP** | **V**LAN **T**runking **P**rotocol. |
| **WAN** | **W**ide **A**rea **N**etwork. |
| **WIMAX** | **W**orldwide **I**nteroperabilite **f**or **M**icroware **A**ccess. |

# Résumé

De nos jours, la sécurité informatique est quasi-indispensable pour le bon fonctionnement de n'importe quel réseau informatique. Pour cela, les administrateurs réseau doivent mettre des mécanismes de gestion et de sécurité plus robuste de leur réseau. Notre travail consiste en une proposition d'une configuration sécurisé pour le réseau informatique de L'entreprise Bejaia Mediterranean Terminal (BMT). Les concepts fondamentaux des réseaux locaux sont bien explicités, les différents mécanismes de sécurité y sont étudiés. Nous avons présenté et étudié l'architecture du réseau, ensuite, nous avons implémenté une solution sécurisé comprenant la configuration des VTP et le DHCP et les listes de contrôle et des mots de passe au niveau du routeur avec le logiciel Cisco Packet Tracer basé sur les VLANs.



**Mots clés :** Réseau Local, Sécurité Informatique, VLAN, BMT, DHCP, VTP.



# Abstract

Nowadays, computer security is almost indispensable for the proper functioning of any computer network. To do this, network administrators must put more robust management and security mechanisms in their network. Our work consists of a proposal for a secure configuration for the computer network of the company Bejaia Mediterranean Terminal (BMT). The basic concepts of local networks are well explained, the different security mechanisms are studied there. We introduced and studied the architecture of the network and then implemented a secure solution including VTP configuration and DHCP and router-level checklists and passwords with Cisco Packet Tracer software based on VLANs.



**Keywords:** Security, VLAN, BMT, DHCP, VTP.