RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ IBN-KHALDOUN DE TIARET

FACULTÉ DES SCIENCES APPLIQUEES

DÉPARTEMENT DE GENIE ELECTRIQUE

MEMOIRE DE FIN D'ETUDES

Pour l'obtention du diplôme de Master

Domaine : Sciences et Technologie
Filière : Génie Electrique

Spécialité : informatique industrielle

THÈME

Création d'une application E-Commerce

Préparé par : MINT MOHAMED SALEM HINDOU

Devant le Jury :

Nom et prénoms	**Grade**	**Qualité**
Mr .ADDA BENATIA	MAA	Président
Mr .MAASKRI MUSTAPHA	MAA	Examinateur
Mr .GOUASMI MED	MAA	Examinateur 1
Mr .BENABID HOUARI	MAA	Encadreur

PROMOTION : 2016_2017

Remerciement

Je veux exprimer par ces quelques lignes de remerciements mes gratitudes envers tout d'abord à mon encadreur, Monsieur BENABID HOUARI pour ses conseils, son encadrement présence, son soutien, et sa disponibilité j'ai trouvé le courage d'accomplir ce projet enfin.

Je remercie tous ceux qui m'ont aidé à mener les réflexions pour réaliser ce projet pour leurs nombreuses sollicitudes et leur disponibilité, et qui méritent d'être particulièrement saluées

Dédicace

Je dédie ce travail
A

Mon père et Ma mère
Pour les sacrifices déployés à mes égards pour leur
Patience, amour et leur confiance qu'on me donner
Le long de ma vie et au cours de ma cursus scolaire.
A
Mon grand frère ; mon père et mon amie Mr. Mohamed lemin Bedy pour son confiance et son soutient tous le long de ma cursus scolaire.
A

Mes sœurs qui ont attendez ce moment depuis longtemps
Que dieu nous garde toujours unis.

A
Mes chères amis et collègues de promo de l'informatique industrielle 2016/2017.
A
Tous ce qui ont été présent dans ma vie ; ceux qui ont étaient la force derrière chaque succès le long de ma vie.

Sommaire

Chapitre I : Généralité sur le réseau informatique

Listes des figures et des tableaux

Listes des figures

Chapitre I : Généralité sur le réseau informatique

Chapitre II : Sécurité d'informatique

Chapitre III : E-Commerce

Chapitre IV : Conception et réalisation d'application

Liste des tableaux

Chapitre I : Généralité sur le réseau informatique

Chapitre II : Sécurité d'informatique

Chapitre IV : Conception et réalisation d'application

Liste abreviations

A

AES : Avanced Encryption Standard.

ARM : AsynchronousReponse Mode.

ABM : AsynchronousBalanced Mode.

B

B2B : Business to Business.

B2C : Business to Business

B2E : Business to Employer.

C

C2B : Consumer to Business.

C2C : Consumer to Consumer.

CSS : Cascading StyleSheets.

C-SET : Chic Secure ElectronicTransaction .

CRC : Cyclic Redundancy Check.

CSMA : CarrierSense Multiple Access.

D

DCTE : Data Circuit Terminating Equipement.

DOS : Disc Operating System.

DES : Data Encryption Standard.

DMZ : DeMilitarized Zone.

E

ETTD : Equipement Terminal de Traitement de Données.

F

FCS : Frame Control Sequence.

FTP : File Transfert Protocol.

FDDI : FiberDistributed Data Interface.

G

H

HDLC : High-level Data Link Control.

HTTP : Hypertext Transfer Protocol.

HTML : HypertextMarkupLanguage.

I

IEEE : Institue of Electrical and Electronics Engineers.

IDEA : International Data Encryption Algorithm .

ISO : International Organization for Standardzation.

IP : Internet Protocol.

J

K

L

LRC : LongitidinalRedundancy Check.

LAN : Local Area Network.

M

Mysql : Michael Monty StructedQueryLanguage.

MAU : Multi-station Access Unit.

MAC : Media Access Control.

MAN : Metrolipian Area Network

N

NRM : NormalReponse Mode.

NBS : National Bureau of Standards.

NIST : National Institue of Standards and Technology.

NSA : National Security Agency**.**

O

OSI : Open Système Interconnexion.

OUI : Organizational Unique Identifer**.**

P

PGP : Pretty Good Privacy.

PHP : Personal Home Pages

PKI : Public Key Infrastructure.

PAN : Personal Area Network.

Q

R

RSA : Rivest; Shamir, Adleman

S

SSL : Secure Socket Layer.

SET : Secure Electronic Transaction.

STT : Secure Transaction Technology.

SEPP : Secure Electronic Pyement Protocol.

SQL : Structed Query Language .

SMIME : Secure Multiprocess Internet Mail Extension.

SMTP : Simple Mail Transfer Protocol.

T

TCP : Transmission Control Protocol**.**

U

UML : Unified Modeling Language.

URL : Uniform Ressource Localer.

UDP : User Datagramme Protocol.

V

VRC : Vertical Redundancy Check.

W

WWW : World Wide Web .

WAN : Wide Area Network.

X

Y

Introduction générale

Introduction générale

Bien qu'il paraisse aujourd'hui comme une nouvelle innovation technologique, le terme e-commerce n'est pas entièrement nouveau. En effet les échanges existaient depuis les années 60 grâce principalement aux standards de l'EDI (échange de données informatisées).

Apres l'apparition de l'Internet ce dernière est imposé alors comme le marché potentiel le plus prometteur du commerce électronique avec en 1995, plus de 50 millions de personnes connectées dans le monde. Les autoroutes de l'information sont alors nées, à savoir des liaisons à débit important dont le World Wilde Web (www) ; ce qui a permet de nos jours d'échanger non seulement des informations textuelles mais également des données multimédias (photos-sons-vidéo..) de manière simple et rapide. Désormais, le Net est un outil universel au profit du public ; sa popularité a incité de nombreuses entreprises à établir leurs présences sur le web. Il est devenu une zone planétaire de libre échange très favorable aux transactions commerciales.

Aujourd'hui l'expansion de l'Internet provoque des changements profonds au niveau commercial, de la publicité jusqu'à la livraison, tous les détails d'une relation commerciale entre le vendeur et le client passe aujourd'hui par l'Internet, ce dernier met à la disposition de tous les partenaires, tous les outils pour finaliser l'achat et la vente en succès et en toute sécurité, ce qu'on l'appelle aujourd'hui le E-Commerce

Ce mémoire consiste à la mise en place d'un site web dynamique qui gère la commercialisation de matériels informatiques. Ceci est possible à travers des catalogues en ligne proposant ces matériels aux meilleurs prix par rapport aux concurrents. La société n'aura donc qu'à agencer ses produits et bien sûr de mettre sa base de données à jour. Les clients peuvent consulter le site après une inscription, et commander les produits, qui sont par la suite livrés à domicile .on vous présente ce projet sur quatre chapitres :

Chapitre1 : **Généralité sur le réseau informatique** ; dans ce chapitre on a fait une présentation brève sur le réseau informatique en mentionnant tous les facteurs et outils intervenant dans un réseau informatique débutant du partie physique jusqu'à la partie logique.

Chapitre2 : **sécurité informatique,** vous présente les différents attaques et risques que peut votre système informatique aura durant votre utilisation quel que soit par les matériaux logiques ; les matériaux physiques ou par l'humain lui-même ; bien sûr en terminant avec les outils disponible pour résoudre ses problèmes ou le minimiser de maximum possible.

Chapitre3 **:E-Commerce** ; premièrement vous trouvez une introduction sur chacun des facteurs intervenant dans la création d'un site web e-commerce ; pour vous donner une idée sur ce projet ; les différents types des sites web ; des client/serveur …etc. ensuite une introduction sur le e-commerce ; et enfin un cahier de charge montre la problématique étudié.

Chapitre4 : **Conception et Réalisation de l'application**: c'est le chapitre qui fait la mise en œuvre de l'application souhaitait, en présentant les outils utilisées; en détaillant les procédures pris durant le développement de l'application.

Chapitre I :

Généralité sur le réseau informatique

I. *Introduction :*

Dans de nombreux cas, un réseau d'ordinateurs est vu par les utilisateurs comme un grand ordinateur dont les disques durs, les bases de données et les autres ressources sont mis à disposition sur des ordinateurs très puissants (les Serveurs), alors que les postes de travail plus petits (Workstation) utilisent ces services. Les performances des réseaux sont devenues si grandes qu'un utilisateur d'un poste de travail ne se rend pas compte du fait qu'il utilise effectivement les ressources d'un ordinateur central, à travers le réseau.

La conception d'un réseau informatique peut constituer un défi de taille de Performances et de sécurités, en effet, cette tache dépasse largement le simple branchement d'ordinateurs entre eux .un réseau doit comporter des nombreuses caractéristiques peut être évolutif, sécurisé et facile à gérer, pour que le réseau soit fiable et évolutif nous devons être conscients que chacun de ses composants comporte des exigences particulières en termes de performances et de sécurité.

Ce chapitre vous donne un vue sur le réseau informatique, leur utilité et leur notion de base.

II. *Le Réseau Informatique :*

Les réseaux ont pour fonction de transporter des données d'une machine terminale vers une autre machine terminale. Pour ce faire, une série d'équipements et de processus sont nécessaires, allant de l'environnement matériel utilisant des câbles terrestres ou des ondes radio jusqu'à l'environnement logiciel, constitué de protocoles, c'est-à-dire de règles permettant de décider de la façon de traiter les données transportées. [1]

Le réseau informatique est la science des méthodes, des techniques, des équipements permettant l'échange d'information numériques à distance entre un ensemble d'ordinateurs connectés entre eux par des liaisons physiques.

II.1. *L'intérêt d'un réseau :*

Un réseau permet :

- Le partage de fichiers, d'applications, d'informations au sens large, le stockage et la sauvegarde centralisée des données
- La communication entre personnes (grâce au courrier électronique, la discussion en direct, ...)
- La communication entre processus (entre des machines industrielles)
- La garantie de l'unicité de l'information (bases de données)
- Tolérance en panne : continuation des services, et duplication des données.[2]

II.2. *Les éléments du base d'un réseau :*

- Les éléments physiques : tels que les interfaces d'interconnexions, les câbles de liaisons, les équipements de connexion, ordinateur...etc.

- Les éléments logiques (logiciels) : les navigateurs, les protocoles, les services (web, mail, FTP) ...etc.[3]

II.3. *Les Topologies d'un réseau* :

Une topologie d'un réseau informatique correspond à l'architecture physique ou logique de celui-ci, définissant les liaisons entre les équipements du réseau et une hiérarchie éventuelle.

II.3.a. *Topologie physique :*

Elle s'apporte à la disposition des équipements et des supports .Il existe 5 topologies :

1. Topologie en BUS : cette topologie est représentée par un câblage unique des unités réseaux ; les machines sont reliées par un câble coaxial et chaque ordinateur est connecté en série sur le bus. Les informations envoyées à partir d'une station sont transmises sur l'ensemble du bus à toutes les stations, l'information circulant sur le réseau (trame) contient son adresse de destination et c'est aux stations de reconnaitre les informations qui leur sont destinées. Cette topologie à été très répandu car son cout d'installation est fiable ; et une station en panne ne perturbe pas le reste du réseau. En cas de la rupture du câble ; le réseau est inutilisable.[4]

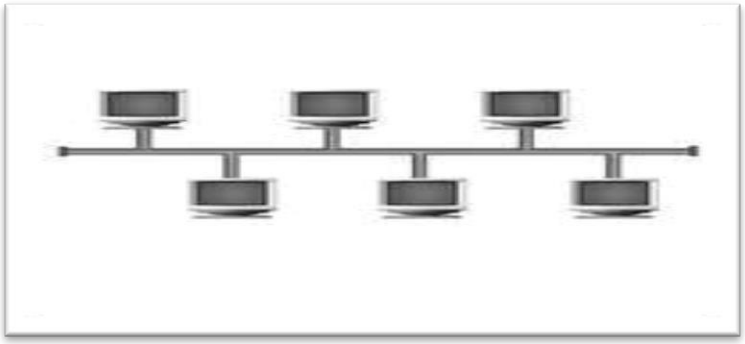


Fig. I. 1 : Topologie en BUS

2. Topologie en Etoile : toutes les stations sont connectées à une commutation ; les stations émettent vers ce concentrateur qui renvoie les données vers tous les autres ports du réseau (hub) ou uniquement aux destinateurs(Switch) ; les câbles entre les différents nœuds est désigné sous le nom de pair torsadées et se termine par des connecteurs RJ45. Cette topologie facilite une évolution hiérarchisée du matériel ; on peut facilement déplacer un appareil sur le réseau ; la panne d'une station ne perturbe pas le fonctionnement global du réseau.[5]

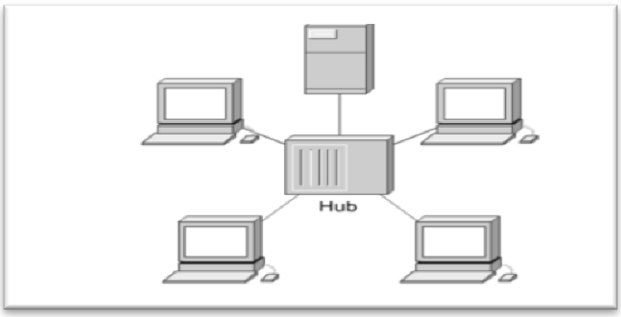


Fig. I. 2: Topologie en Etoile

3. <u>Topologie en étoile étendu :</u> lorsqu'un réseau en étoile est développé afin d'accueillir un équipement supplémentaire ; comme un hub ou un commutateur connecté à l'équipement de réseau principale, on parle de topologie en étoile étendue. Cette topologie permet de réduire de manière significative le trafic sur les câbles .Les paquets sont envoyés uniquement vers les câbles de l'hôte de destination.[4]

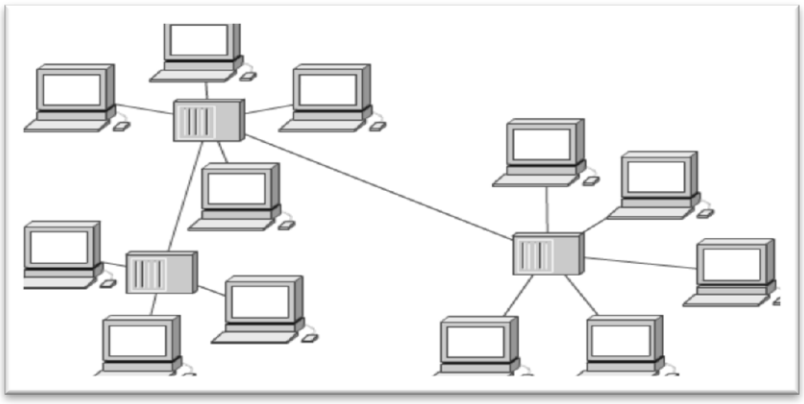


Fig. I. 3 : Topologie en Etoile Etendu

4. <u>Topologie en Anneau</u> : Dans un réseau possédant une topologie en anneau ; les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour ; cela ressemble à un bus mais qui serait refermé sur lui-même, le dernière nœud est relié au première. En réalité, les ordinateurs ne sont pas reliés en boucle, mais sont reliée à un répartiteur qui va gérer la communication entre les ordinateurs qui lui sont reliés en répartissant à chacun d'entre-deux un temps de parole.IL est nécessaire d'interrompre le fonctionnement du réseau lors de l'ajout d'un nouveau poste, la panne d'une station bloque toute la communication du réseau.[4]

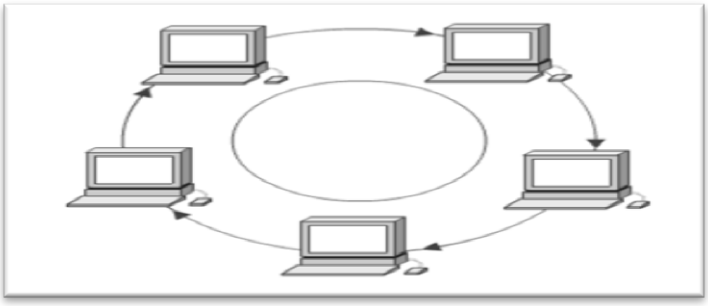


Fig.I. 4 : Topologie en Anneau

5. Topologie Maillée : les réseaux maillés utilisent plusieurs chemins de transfert entre les différents nœuds, c'est une structure réseau hybride reprenant un câblage en étoile regroupant différents nœuds de réseaux, cette méthode garantit le transfert des données en cas de panne d'un nœud. [5]

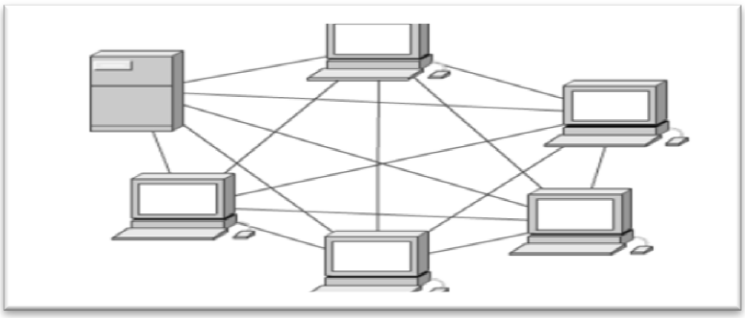


Fig. I. 5: Topologie en Maillée

II.3.b. ***Topologies Logiques :*** Il convient de distinguer trois normes de réseaux locaux

1. Topologie Token Ring : un ordinateur doit capturer une trame spéciale, appelée jeton, pour pouvoir envoyer des données. Cette méthode évite les collisions.

Fig.I. 6: Topologie Token Ring

Un jeton libre circule dans l'anneau. En passant, il demande aux unités du réseau si elles veulent transmettre des données. Dans un réseau Token ring, chaque nœud du réseau comprend un MAU (Multi Station Access Unit) qui peut recevoir les connexions des postes. Le signal qui circule est régénéré par chaque MAU.

2. *Topologie FDDI :*La technologie FDDI (FiberDistributed Data Interface) est une technologie d'accès réseau utilisant des câbles fibre optiques. Le FDDI est constitué de deux anneaux : un anneau primaire et anneau secondaire. L'anneau secondaire sert à rattraper les erreurs de l'anneau primaire ; le FDDI utilise un anneau à jeton qui sert à détecter et à corriger les erreurs. Ce qui fait que si une station MAU tombe en panne, le réseau continuera de fonctionner.[6]

3. *Topologie Ethernet :* Ethernet est aujourd'hui l'un des réseaux les plus utilisées en local. Il repose sur une topologie physique en étoile. Dans un réseau Ethernet, la communication se fait à l'aide d'un protocole appelé CSMA/CD, ce qui fait qu'il aura une très grande surveillance des données à transmettre pour éviter toute sorte de collision. Par conséquent un poste qui veut émettre doit vérifier si le canal est libre avant d'y émettre[2]

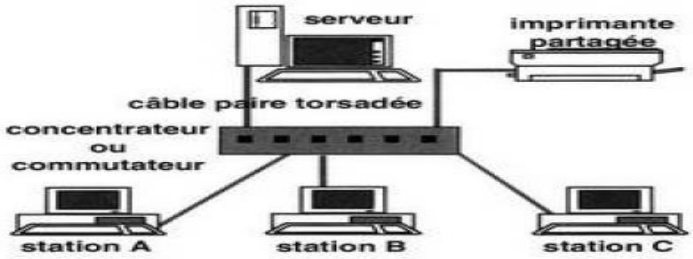


Fig.I. 7 : Exemple de topologie Ethernet

II.4. *Les Types de Réseau :*

On distingue les différents types de réseau selon leur distance (qui sépare les ordinateurs) :

II.4.a. *Réseau LAN (Local Area Network)* : C'est un réseau informatique à une échelle géographique relativement restreinte par exemple dans une entreprise, une salle ou d'un bâtiment ; il est constitué d'ordinateur et de périphérique reliées entre eux et implantés dans une même entreprise et à caractère privé ; il a les caractéristiques suivants :Il ne dépasse pas généralement la centaine des machines et ne dessert jamais au-delà du kilomètre. Le partage des ressources est ici fréquent et les vitesses de transmission vont de 10 à 100 Mb/s.[7]

II.4.b. *Réseau MAN (Métropolitan Area Network)* :C'est un réseau métropolitain qui désigne un réseau composé d'ordinateur habituellement utilisés dans les campus ou dans les villes, Ainsi, un MAN permet à deux nœud (ordinateurs) distants de se communiquer comme s'ils faisaient partie d'un même réseau local.

IL correspond à la réunion de plusieurs réseaux locaux(LAN) à l'intérieur d'un même périmètre d'une très grande entreprise ou d'une ville par exemple pouvant relier des points distants de 10 à 25 km. Il à les caractéristiques suivants :

- En général le câble coaxial est le support physique le plus utilisé dans ce type de réseau.
- Peuvent –être privé ou public.

- Utilise un ou deux câbles de transmission.
- Pas d'éléments de commutation (routage).
- Norme spéciale IEEE-802-6.

II.4.c. *Le réseau WAN (Wide Area Network)* :est un réseau multiservices couvrant un pays ou un groupe de pays, qui est en fait constitué d'un ensemble de réseau locaux interconnectés.

II.4.d. *Le réseau PAN (Personal Area Network)* : un réseau personnel désigne un type de réseau informatique restreint en terme d'équipements ; généralement mis en œuvre dans un espace d'une dizaine de mètres, d'autre appellation pour ce type de réseau sont le réseau cosmétique ou réseau individuelle ; ce type de réseau utilise généralement l'USB ; les technologies sans fil telles que Bluetooth et l'infrarouge.[8]

II.5. *Les supports de communications :*

Les supports de communications sont des câbles métalliques ou bien des ondes qui assurent l'interconnexion entre les équipements d'un réseau :

1. Câble coaxial : formé d'une âme en cuivre pour transmettre les signaux, le retour du signal se fait par une gaine conductrice qui entoure l'âme ; les deux étant séparées par un isolant.

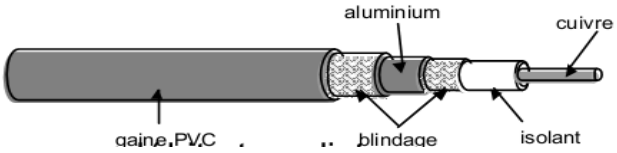


Fig.I. 8: Câble coaxial

2. Le pair torsadé : Formée de pair de fil conducteur, contenues dans une gaine isolante, les paires sont torsadées pour éviter les interférences électriques.

Fig.I. 9 : Le pair torsadé

3. Les fibres optiques : sont formés d'une fibre très fine en verre ou en plastique, entourée par une gaine protectrice ; les signaux sont transmis sous forme lumineuse. On distingue des

fibres multi modes (plusieurs signaux, moins rapides et moins chers) et des fibres monomodes (un seul signal lumineux, plus rapide et très cher).

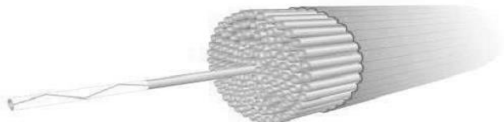


Fig.I. 10: Les fibres optiques

4. ***Faisceau hertzien et onde radio :***Un faisceau hertzien est un système de transmission de signaux permanent entre deux points fixes. Il utilise comme support les ondes radioélectriques, très fortement concentrées à l'aide d'antennes directives. [8]

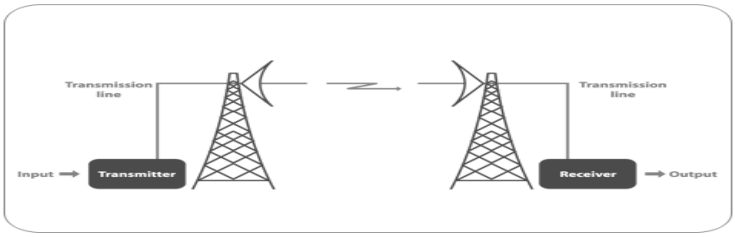


Fig.I. 11 : Faisceau hertzien

II.6. *Les équipements d'interconnexion :*

Les équipements d'interconnexions sont les briques constitutives d'un réseau :

1. Répéteur : c'est un équipement électronique simple permettant d'amplifier un signal et d'augmenter la taille d'un réseau ; ce n'est pas un organe intelligent capable d'apporter des fonctionnalités supplémentaires, il ne fait qu'augmenter la longueur du support physique.

Fig.I. 12 : Répéteur

2. Le concentrateur (Hub) : il permet de concentrer le trafic réseau provenant de plusieurs hôtes ; il possède 4 ports, 8 ports ,16 ports ou 32 ports et le choix de port dépend du nombre de réseau.

Fig.I. 13 : Hub

3. Ponts (Bridge) : les ponts sont des équipements permettant de relier des réseaux travaillant avec le même protocole, ils travaillent au niveau logique (couche 2 modèle OSI) sa fonction est d'interconnecter deux segments de réseau distincts, mais physiquement séparés.

4. Commutateur (Switch) : il est également appelé pont multiport ; sa fonction est d'interconnecter plusieurs carte d'interface ensemble, cependant, lorsqu'il réceptionne une trame il compare l'adresse MAC de destination avec sa table de correspondance. Ainsi il ne diffuse cette trame uniquement sur le port physique concerné.

Fig.I. 14: Commutateur (Switch)

5. Routeur : c'est un dispositif d'interconnexion de réseau informatique permettant d'examiner les paquets entrant ; choisir le meilleur chemin pour le transporter sur le réseau et le commuter ensuite au port approprié, ils sont utilisé dans les grands réseaux[8]

Fig.I. 15: Routeur

III. *Le Modèle OSI (Open System Interconexion) :*

Les systèmes de communication en réseau sont souvent décrits grâce au modèle de référence Open System Interconnexion (OSI). Ce modèle a été développé par l'ISO (International Organization for standardization) ; le modèle OSI est constitué de 7 couches remplissant chacune une fonctionnalité particulière de la couche application à la couche de transmission chacune des différents couches ne représente pas nécessairement un protocole spécifique l'illustration ci-après présente la structure de ce modèle :

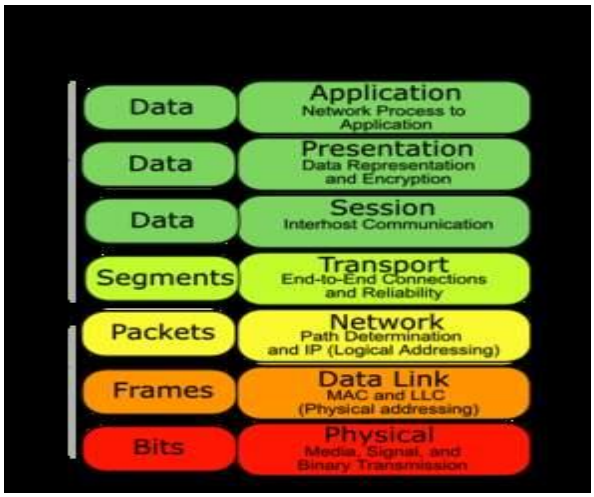


Fig.I. 16 : Structure du Modèle OSI

III.1. *La couche physique :*

La couche physique assure l'interface avec le matériel, prend en charge la conversion des signaux numériques en signaux analogiques (la modulation) l'émission physique sur la ligne de communication.

III.1.a.*Circuit de données :*Un circuit de donné est constitué d'une ligne de transmission et deux équipements de terminaison de circuit de données DCTE (Data Circuit –Terminating Equipement) :

- *ETCD (Equipement Terminal de Circuit de Données) :*à pour rôle d'établir la communication et de transmettre les données.

- *ETTD (Equipement Terminal de Traitement de Données) :* est un équipement informatique quelconque.

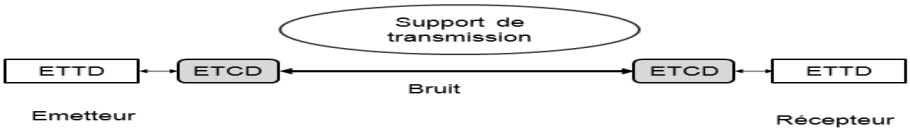


Fig.I. 17 :L'ETTD et ETTC

III.1.b. ***Les Modes de liaisons*** : Selon le sens de communication un circuit de donnée peut-être :

- ***Simplexe :*** la transmission dans un seul sens.

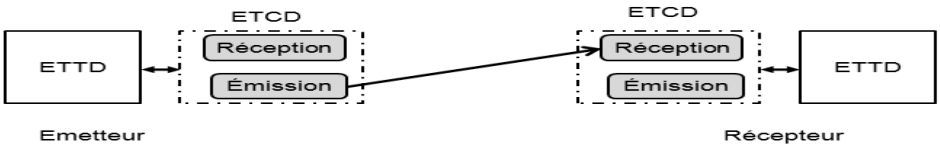


Fig.I. 18: Transmission simplexe

- ***Semi-duplex (Half-duplex) :*** la transmission est dans les deux sens.

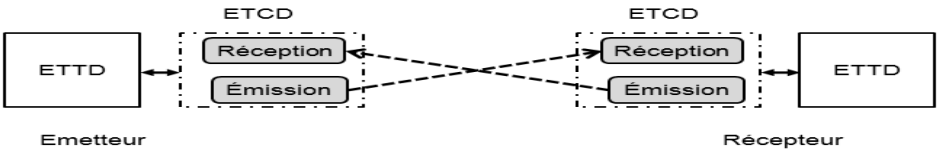


Fig.I. 19: Transmission Half-duplex

- ***Duplex (full-duplex) :*** la transmission dans les deux sens simultanément.

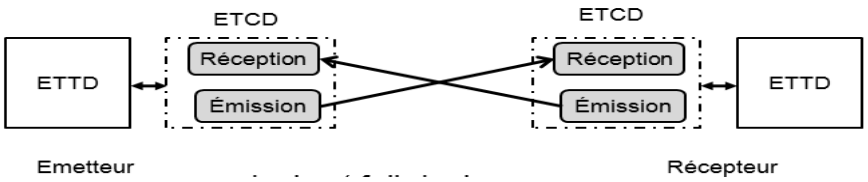


Fig.I. 20: Transmission Full-duplex

III.2. ***La couche liaison :***la couche liaison assure la fiabilité de la transmission des données par la couche 1(couche physique) sur le support réseau, elle réalise cette fonction par la synchronisation de la transmission des données et par différents procédés d'identification et de correction d'erreurs. Cette couche a pour rôle découpage en trame ; délimite les données issus de la couche réseau, contrôle d'accès au média de transmission ; adressage ; contrôle d'erreurs et contrôle de flux. La couche liaison se décompose en 2 sous couches :

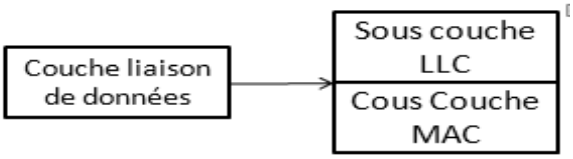


Fig.I. 21: la couche liaison

III.2.a.*La sous couche MAC (Media Access Control) :*à pour rôle de gérer l'accès au support physique, structurer les bits d'information en trame et gérer les adresses physiques des interfaces de communication.

1. ***Notion d'une trame :*** est une suite délimitée des bits.

Délimiteur du début de la trame	Entête de la trame	Données	Délimiteur du fin de la trame

Tableau.I. 1 :Notion d'une trame

- Délimiteur du début et la fin de la trame : ensemble de bits utilisé pour détecter le début et la fin d'une trame
- Entête de la trame : ensemble d'informations rajoutées par la couche liaison de données aux données issues de la couche réseaux.
- Les données : les données reçus de la couche réseaux.

2. ***Mode de connexion :***

- Connexion point à point : deux station seulement partage le support de communication.

Fig.I. 22 : Connexion point à point

- Connexion multipoints : plusieurs stations utilise le même support de transmission.

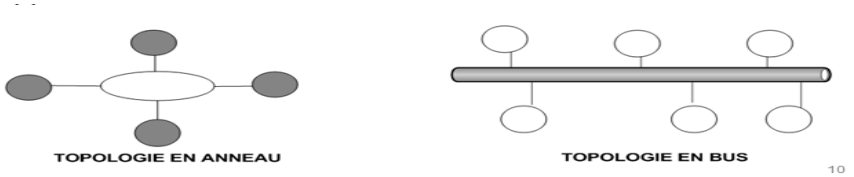


Fig.I. 23: Connexion multipoint

3. ***Les protocoles de la sous couche MAC :*** a pour rôle de définir des protocoles qui déterminent les stations autorisés à transmettre des données sur le média partagé et de régler les problèmes des collisions. Il existe deux grandes catégories de protocoles MAC :
   - Les protocoles déterministes : JETON.
   - Les protocoles aléatoires: ALOHA, CSMA.

4. ***Adresse MAC :*** chaque ordinateur à une façon unique de s'identifier, qu'il soit relié à un réseau ou non ; possède une adresse physique qui se trouve sur la carte réseau ; il comporte 6 octets et sont exprimés en 12 chiffres en Hexadécimal ; les 6 premières chiffres qui sont administrés par l'IEEE, identifiant le fabricant ou le fournisseur et constituent donc l'identifiant unique d'organisation OUI (Organizational Unique Identifier) et les 6 autres sont le numéro de série d''interface. EX :

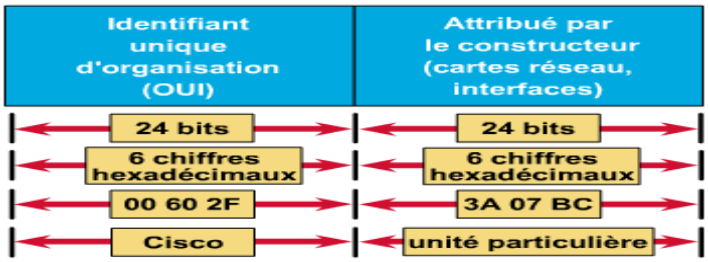


Fig.I. 24:Adresse MAC

III.2.b. ***La sous couche LLC :***c'est l'interface avec la couche réseau il lui offre une couche logique plutôt que physique ; elle assure la protection contre les erreurs de transmission ; assure le transfert des trames et le contrôle de flux entre les stations du réseau, elle est indépendante de la méthode d'accès utilisé par la sous couche MAC.

1. ***Détection des erreurs :*** les techniques les plus utilisées pour la détection des erreurs sont :
   - VRC (Vertical Redundancy Check) : Calculer la parité est rajouté un bit à l'information envoyé.
   - Parité paire : si le nombre de 1 dans l'information est pair alors le bit de parité est égal à 1, sinon 0.
   - Parité impaire : si le nombre de 1 dans l'information est impair alors le bit de parité est égal à 1, sinon 0.
   - LRC (Longitudinal Redundancy Check) : Appliquer le principe de la parité (paire ou impaire) aux colonnes d'un bloc de données.
   - CRC (Cyclic Redundancy Check) : vérification polynômiale.

2. ***Correction d'erreurs :*** la méthode la plus simple pour corriger une erreur c'est de demander une retransmission c.-à-d. que le récepteur qui détecte une erreur demande

une retransmission jusqu'au qu'il n'y est plus d'erreurs ou bien utilisé le code correcteur. Le principe des codes correcteurs est le même que celui de code détecteurs lors de l'émission on rajoute des bits de contrôle supplémentaire ; a la réception les bits de contrôle seront détecter et corrigé. Le code de Hamming est parmi ces codes, il permet de détecter une seul erreur ; il est basé sur le calcule de parité.

3. ***Le contrôle de flux :*** Dans une liaison de données on doit disposer d'un protocole pour Réguler le flux de données entre l'émetteur et le récepteur et assurer ainsi un bon transfert des trames ; Lorsque les tampons (espace de stockage des trames) du récepteur sont pleins, un message est envoyé à l'émetteur afin d' arrêter la transmission jusqu'à ce que les données dans les tampons soit traitées. On distingue deux types de trames échangés entre les stations:

- Trame d'information.
- Trame de contrôle : acquittement, chaque trame est acquittée soit d'une façon positive ou négative (ACK, N-ACK).[9]

4. ***Le Protocol HDLC :*** est un protocole orienté bits ; Il utilise un format de trame spécial.

Fanion	1 octet	1 octet	>= 0	2 Oct	Fanion
01111110	Adresse	Commande	Donnée	FCS	01111110

Tableau. I. 2: Le Protocol HDLC

- Fanion (Flag) : séquence de délimitation de trame;
- Adresse : champ d'adresse de la station secondaire ;
- commande : champ de commande;
- données : champ d'information;
- FCS (Frame Control Séquence): (contrôle d'erreur).[10]

5. ***Les modes de fonctionnement du HDLC :***

- Primaire / secondaire (ARM - AsynchronousResponse Mode) la station primaire à l'initiative de l'initialisation de la liaison de données.

- Mode NRM: Mode de réponse normal, Mode déséquilibré asymétrique dans lequel une station maître et l'autre esclave. La station secondaire ne peut émettre que sur l'ordre de la station primaire.
- Primaire / primaire (le plus courant) (ABM – AsynchronousBalanced Mode) tous les équipements agissent de la même façon mode équilibré (Balanced).

6. *Les Types de Trames:*

- **Trames d'information:** le premier bit est à 0, les autres bits contiennent les compteurs N(S) et N(R) ainsi que le bit P/F.
- **Trame de supervision :** les deux premiers bits ont pour valeurs 10, les deux suivants définissent quatre commandes (ou réponse) possibles pour le contrôle d'erreur et le contrôle de flux, les autres contiennent le compteur N(R) et le bit P/F.
- **Trame de supervision non séquentielles (non numérotées) :** les deux premiers bits ont pour valeurs 11, les autres bits (sauf le bit de P/F) définissent un ensemble de commandes et de réponses pour l'Initialisation et la fermeture d'une connexion.[5]

III.3. *La Couche Réseau :*

La couche réseau prend en charge l'optimisation des chemins de transmission entre les ordinateurs distants. Les données circulent vers le bas du modèle OSI, elles sont encapsulées au niveau de chaque couche, les données sont encapsulées dans les paquets (datagramme).La couche réseau offre deux fonctionnalités de base :

- L'adressage : chaque machine doit être dotée d'une adresse logique unique dans un réseau.
- Le routage : la couche réseau permet de retrouver une machine dans un réseau grâce à une route précisant comment la machine peut être atteinte.

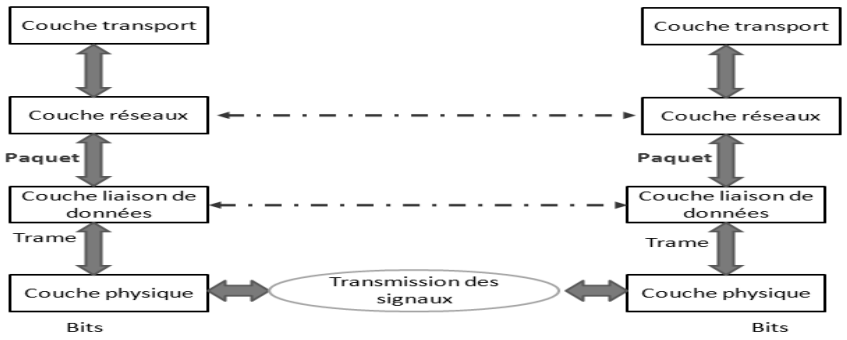


Fig.I. 25: La Couche Réseau

III.3.a.*L'adressage IPV4 :*

Un adresse est codé sur 32 bits (4octets) dite " adresse IP " il comprend deux parties :

- Un **numéro de réseau**(NET-ID): une adresse globale pour identifier un réseau, cette adresse et commun a toutes les machines de ce réseau.
- Un **numéro de machine** (hôte) : identifier une machine dans un réseau.

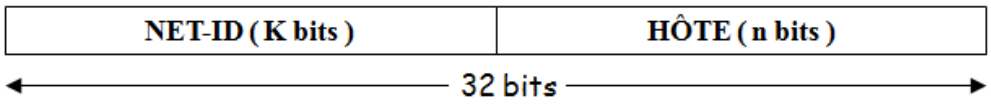


Tableau.I. 3*:Adressage IPV4*

III.3.b. ***Les Classes :***La taille d'une partie réseau (NET-ID) détermine la classe ; ce dernière se divise en 3 :

- Classe A : la plage d'adresse possible est de 0.0.0.0 à 126.255.255.255

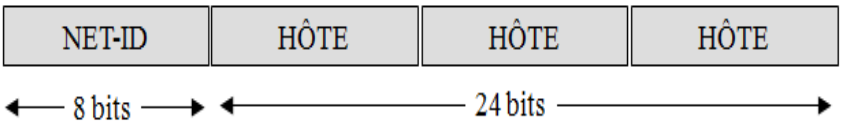


Tableau.I. 4: Classe A

- Classe B : la plage d'adresse possible est de 125.0.0.0 à 191.255.255.255

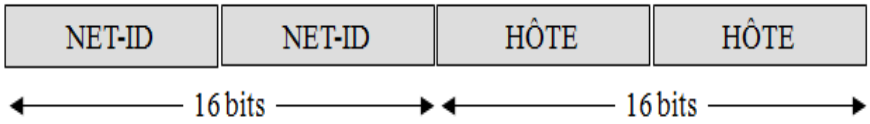


Tableau.I. 5: Classe B

- Classe C : la plage d'adresse possible est de 192.0.0.0 à 223.255.255.255

Tableau.I. 6:Classe C

1. ***Adresse Particulière*** :
   - Classe D : pour le multicast (communication en groupe) ; la plage d'adresse possible est de 224.0.0.0 à 239.255.255.
   - Classe E : sont réservés pour les tests ; la plage d'adresse possible est de 240.0.0.0 à 247.255.255.255.
   - L'adresse réseau : c'est l'adresse d'où la partie hôte n'est composé que de 0 ex :90.25.32.11 @ réseau est : 90.0.0.0.
   - L'adresse 0.0.0.0 désigne tous les réseaux.
   - L'adresse 255.255.255.255 est l'adresse de diffusion de masse toutes les machines vont recevoir le paquet.

2. ***Adresse de diffusion (brodcast) :*** on parle de diffusion lorsqu'une source envoie des données à toutes les unités d'un réseau ; quand une adresse ne contient que des 1 dans la partie hôte ; c'est l'adresse de brodcast.

EX : 90.25.38.11 @brodcast est 90.255.255.255.

3. ***Adresse privé :*** si les machines d'un réseau ne sont pas connectés à d'autres réseaux ou on pas besoin d'être visible de l'extérieur :

- 1 réseau de classe A : 10.0.0.0.
- 16 réseaux de classe B : du 172.16.0.0 à 176.31.0.0.
- 235 réseaux de classe C : du 192.168.0.0 à 192.31.0.0.

4. ***Les sous-réseaux (segmentation)*** : Au sein d'un réseau IP, toutes les stations communiquent entres elles, afin de masquer certaines stations il est nécessaire de segmenter le réseau initial.

Cette segmentation d'un réseau en sous réseau va permettre de réunir un certain nombre de réseau locaux sous la forme d'un seul et unique inter-réseau ; cela permettre également de subdiviser un grand réseau en sous réseau plus petit reliés par des routeurs.

Le principe est de prendre n bits de la partie hôte ; le nombre de bits à empruntés dépend du nombre de sous réseau qu'on veut avoir et le nombre de machines dans chaque sous réseau.

EX : si on veut avoir 7 sous réseaux :

Donc on a 2^3=8 sous réseaux et alors 3 bits à empruntés.

Net-id (K bits)	Hôte (m bits)	
Net-ID (k bits)	Sous réseau (n bits)	Hôte (m-n bits)

Tableau.I. 7:Les sous-réseaux (segmentation)

5. ***Le masque des sous-réseaux :*** lorsqu'on utilise les sous réseaux, le masque réseau par défaut n'est plus valable, puisque nous avons rajouté des bits supplémentaires au NET-ID. La nouvelle valeur du masque pour les sous réseaux est calculée comme suit :

- Prendre les masques par défaut du réseau initial.
- Compléter les bits empruntés de la partie hôte par des 1 ; et laisser les bits restant de la partie hôte à zéro.

6. ***Adresse de broadcast pour les sous réseaux*** : Dans le cas des sous réseaux l'adresse du broadcast n'est pas la même pour tous les sous réseaux. Pour calculer l'adresse de broadcast d'un sous réseaux :

- Ecrire l'adresse de ce sous réseaux en binaire.
- Remplir la partie hôte uniquement avec des 1 ; Et traduire par la suite en décimal.

III.4. *La couche Transport :*

L'objectif de la couche transport est le transport et contrôle du flux de données entre la source et la destination de manière fiable. La couche de transport offre à la couche application les fonctionnalités suivants :

- Le multiplexage /démultiplexage à la notion de port.
- Le transport des données grâce à TCP et UDP.
- Le contrôle de flux grâce à TCP.
- Le contrôle de congestion grâce à TCP.

III.4.a.*Les protocoles TCP /UDP :*

- **Le protocole TCP (Transmission Contrôle Protocol)** :

fournit un service sécurisé de remise des paquets, orienté connexion, encapsulé dans le protocole IP.

- **Le protocole UDP (User Datagramme Protocol)** : orienté non connexion, peu fiable, n'utilise pas d'accusés de réception et n'assure aucun contrôle de flux mais il est rapides.

III.4.b. *Le Multiplexage :*Les protocoles TCP et UDP peuvent servir simultanément à plusieurs application (processus) sur la même machine c'est le multiplexage ; ces processus communiquent par la même interface réseau et partagent le même adresse IP.

III.4.c.*Notion De port :*Un port est un concept abstrait (pas physique), c'est un numéro qui permet d'identifier une application sur une machine, on dit qu'une application est attaché à un port, et chaque machine attache des numéros de port à ses applications indépendamment des autres machines deux applications sur la même machine ne peuvent pas avoir le même port. [8]

III.5. *La couche Session :*

Cette couche organise et synchronise les échanges entre tâches distantes. Elle réalise le lien entre les adresses logiques et les adresses physiques des tâches réparties. Elle établit également une liaison entre deux programmes d'application devant coopérer et commande leur dialogue (qui doit parler, qui parle...). Dans ce dernier cas, ce service d'organisation s'appelle la gestion du jeton. La couche session permet aussi d'insérer des points de reprise dans le flot de données de manière à pouvoir reprendre le dialogue après une panne.[8]

III.6. *La couche présentation :*

Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises : c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information. Typiquement, cette couche peut convertir les données, les reformater, les crypter et les compresser.[2]

III.7. *La couche Application :*

C'est dans ce couche que vous trouvez la plupart des **protocoles** utilisés par les utilisateurs. On peut citer notamment le protocole HTTP lors de l'accès à une page web, le protocole SMTP pour les mails, le FTP pour le transfert de fichiers.

- FTP File Transfer Protocol port 21 Transfert de fichiers - Utilise 2 sockets.
- SMTP Simple Mail Transfer Protocol port 25 Messagerie électronique.
- HTTP Hyper Text Transfer Protocol port 80 Protocole d'échange d'hyper textes et de plus généralement d'objets informatiques.

IV. *Le Modèle TCP/IP :*

Le modèle TCP/**IP** est nommé ainsi car les protocoles de communications TCP et IP y sont les éléments dominants. Il faut noter que les protocoles TCP et IP ont été inventés bien avant le modèle qui porte leur nom et également bien avant le modèle OSI. Le modèle TCP/IP a

été construit suite aux travaux du département de la défense américaine (Dod) sur le réseau ARPANET, l'ancêtre d'internet, et sur le mode de communication numérique via des datagrammes. C'est suite à cette réalité technique qu'est venu se greffer la normalisation du modèle TCP/IP qui dans le principe et sur certaines couches s'inspire du modèle OSI.[9]

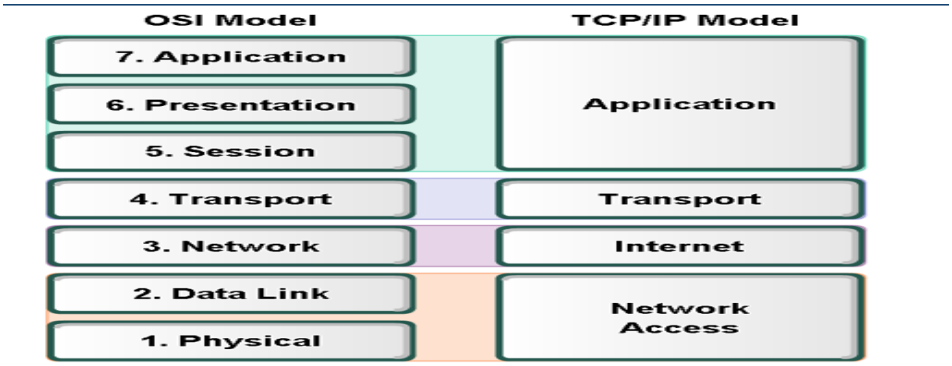


Fig.I. 26: Le Modèle TCP/IP

IV.1. *La couche Accès réseau :*

Dans le **modèle TCP/IP,** les couches 1 et 2 du modèle OSI sont regroupées et forment la couche **d'**accès au réseau qui permet aux paquets de transiter d'une machine à une autre tant au niveau physique qu'au niveau des trames.

IV.2. *La couche Internet :*

Les principaux protocoles de la couche 3 du modèle TCP/IP sont les protocoles **TCP** (Transmission Control Protocol) et **UDP** (*User Datagram Protocol*) qui ont chacun un mode de fonctionnement distinct mais dont le rôle est bien de proposer une méthode pour transporter une information d'une machine à une autre (couche **Transport**).

IV.3. *La couche Transport :*

Dans le modèle TCP/IP il n'existe ni couche session ni couche présentation. Les applications sont implémentées « au-dessus » du transport, en utilisant typiquement les « sockets ». Le modèle client-serveur gère de manière implicite l'organisation du dialogue entre les applications (analogue à la session). Après une phase préalable de connexion/négociation, le client émet une requête et attend la réponse du serveur. Une application est identifiée par le port TCP ou UDP (analogue à un TSAP OSI) qui permet de la joindre. L'adresse Internet d'une application est donc constituée par l'adresse IP de la machine qui l'abrite et un port de connexion (ex 129.182.45.67:21).[4]

IV.4. *La couche Application :*

Les couches 5, 6 et 7 du modèle OSI sont également regroupées en une seule couche dite **"Application"** qui comporte tous les protocoles de "haut niveau" comme le SSH, l'HTTP, le SMTP...

V. ***Conclusion :***

On a essayé dans ce chapitre de vous donner une présentation brève en ce qui concerne le réseau informatique, tous ses information collecter ne forment pas qu'une partie de ce domaine qui est un domaine très vaste et en cours d'évolution.

Enfin, On peut dire que l'ensemble des réseaux jouent un rôle croissant dans notre société de l'information. La nécessité de donner accès aux informations et aux ressources à de nombreux utilisateurs sur de nombreux ordinateurs rend une mise en réseau pratiquement indispensable dans la plupart des environnements professionnels.

Chapitre II :

La Sécurité Informatique

I. Introduction :

Les exigences de la sécurité de l'information au sein des organisations ont conduit à deux changements majeurs au cours des dernières décennies. Avant l'usage généralisé d'équipements informatiques, la sécurité de l'information était assurée par des moyens physiques (classeurs fermés par un cadenas) ou administratifs (examen systématique des candidats au cours de leur recrutement). Avec l'introduction de l'ordinateur, le besoin d'outils automatisés pour protéger fichiers et autres informations stockées est devenu évident. Ce besoin est accentué pour un système accessible via un téléphone public ou un réseau de données. On donne à cette collection d'outils conçus pour protéger des données et contrecarrer les pirates le nom de sécurité informatique.

La sécurité informatique est de nos jours devenue un problème majeur dans la gestion des réseaux d'entreprise ainsi que pour les particuliers toujours plus nombreux à se connecter à Internet. La transmission d'informations sensibles et le désir d'assurer la confidentialité de celles-ci est devenu un point primordial dans la mise en place de réseaux informatiques.

Ce Chapitre présente les différents méthodes et services pour assurer la sécurité d'un système informatique.

II. La Sécurité Informatique :

La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système informatique contre les menaces accidentelles ou intentionnelles auxquelles il peut être confronté. En d'autres mots, c'est l'ensemble des techniques qui assurent que les ressources du système d'information (matérielles ou logicielles) d'une organisation sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient. [11]

II.1 *Les services de la sécurité informatique :*

Les exigences fondamentales de la sécurité Informatiques se résument dans :

- **La disponibilité** : L'information sur le système doit être toujours disponible aux personnes autorisées.
- **La confidentialité** : L'information sur le système ne doit être diffusée qu'aux personnes autorisées.
- **L'Intégrité** : L'information sur le système ne doit pouvoir être modifiée que par les personnes autorisées.
- Le **non répudiation**, permettant de garantir qu'une transaction ne peut être niée.
- L'**authentification**, consistant à assurer que seules les personnes autorisées aient accès aux ressources.

Dans le concept de la sécurité informatique on prendre en compte les espaces suivants :

- **La sécurité logique**, c'est-à-dire la sécurité au niveau des données, notamment les données de l'entreprise, les applications ou encore les systèmes d'exploitation.
- **La sécurité des télécommunications :** technologies réseau, serveurs de l'entreprise, réseaux d'accès, etc.
- **La sécurité physique**, soit la sécurité au niveau des infrastructures matérielles : salles sécurisées, lieux ouverts au public, espaces communs de l'entreprise, postes de travail des personnels, etc.[12]

II.2 *Les Attaques de sécurité :*

Les attaques portées à la sécurité d'un ordinateur ou d'un réseau sont mieux caractérisées en considérant le système en tant que fournisseur d'information. En général, il existe un flot d'information issu d'une source - un fichier ou une zone de la mémoire centrale, vers une destination à un autre fichier ou utilisateur. Il existe quatre catégories d'attaques : interruption, interception, modification, fabrication.

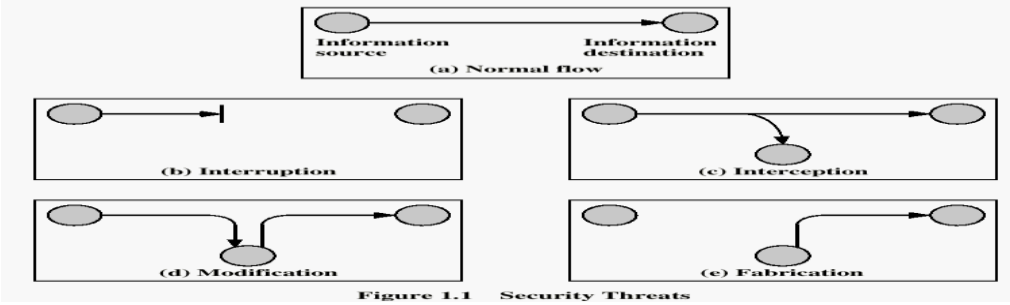


Fig.II. 1: Les Attaques de sécurité

- ***Interruption*** : C'est une attaque portée à **la disponibilité**. La destruction d'une pièce matérielle (tel un disque dur), la coupure d'une ligne de communication, ou la mise hors service d'un système de gestion de fichiers en sont des exemples.
- ***Interception :*** Une tierce partie non autorisée obtient un accès à un atout. C'est une attaque portée à la **confidentialité**. Il peut s'agir d'une personne, d'un programme ou d'un ordinateur. Une écoute téléphonique dans le but de capturer des données sur un réseau, ou la copie non autorisée de fichiers ou de programmes en sont des exemples.
- ***Modification :*** Une tierce partie non autorisée obtient accès à un atout et le modifie de façon (presque) indétectable. Il s'agit d'une attaque portée à **l'intégrité**. Changer des valeurs dans un fichier de données, altérer un programme de façon à bouleverser son comportement ou modifier le contenu de messages transmis sur un réseau sont des exemples de telles attaques.
- ***Fabrication :*** Une tierce partie non autorisée insère des contrefaçons dans le système. C'est une attaque portée à **l'authenticité**. Il peut s'agir de l'insertion de faux messages dans un réseau ou l'ajout d'enregistrements à un fichier.[13]

Il peut être utile de distinguer deux catégories d'attaques : les attaques passives et les attaques actives.

II.2.a ***Les Attaques passives*** **:** Écoutes indiscrètes ou surveillance de transmissions sont des attaques de nature **passive**. Le but de l'adversaire est d'obtenir une information qui a été transmise.

1. ***La capture du contenu de messages*** :

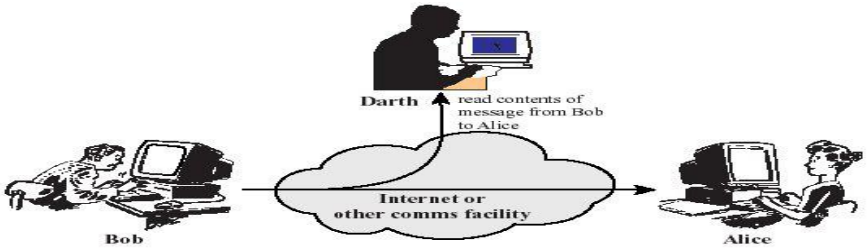


Fig.II. 2 : La capture du contenu de messages

1. ***Analyse de Trafic :***

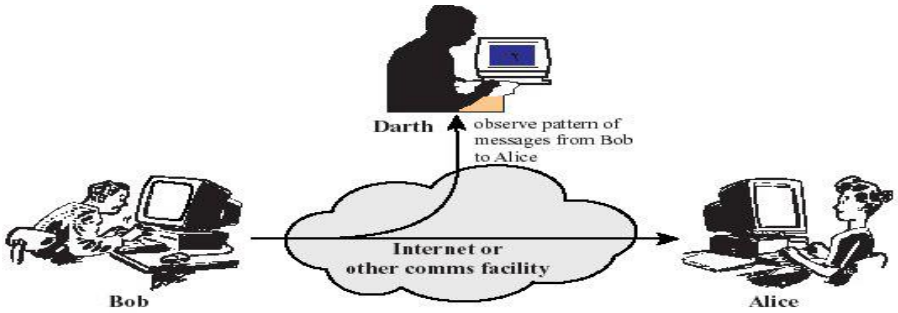


Fig.II. 3: Analyse de Trafic

I.1.b ***Les Attaques Actives :***Ces attaques impliquent certaines modifications du flot de données ou la création d'un flot frauduleux ; elles peuvent être subdivisées en quatre catégories **[14]**

1. ***Une mascarade :***

Fig.II. 4: Mascarade

2. ***Le rejeu :***

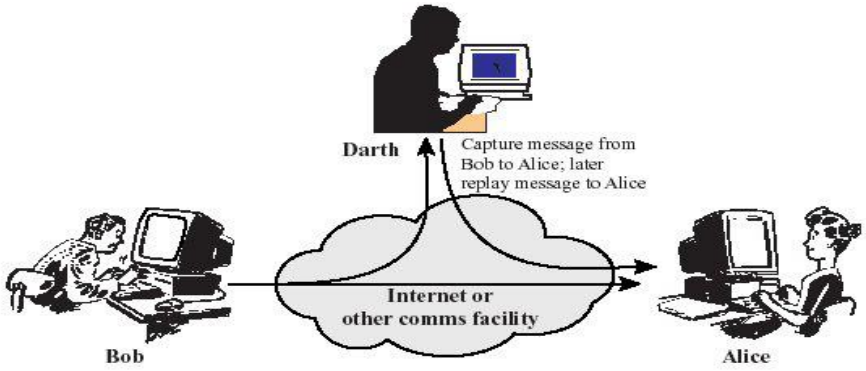


Fig.II. 5: Le rejeu

3. ***La modification des messages :***

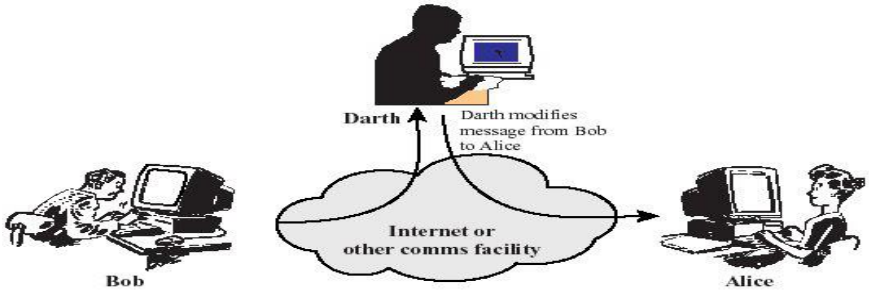


Fig.II. 6 : La modification des messages

4. ***Le déni de service(DOS) :***

Fig.II. 7: Le déni de service(DOS)

II. Risques Informatiques :

II.1 ***Risques*** : Les problèmes de sécurité informatique peuvent de façon très générale être classés en deux grandes catégories :

II.1.a *Risques physiques :* Il s'agit de toutes les atteintes physiques directes dont peut être victime un système d'informations au cours de son cycle de vie. On les appelle également risques matériels, parce qu'ils ont trait à l'intégrité du matériel. Il s'agit entre autres d'événements tels que:

- Incendies, explosion, effondrement
- Dommages électriques, foudre
- Tempêtes, inondations, événements naturels
- Bris de machines, vol, actes de vandalisme
- Défaillance matérielle

Les risques physiques constituent dans la conception traditionnelle de la sécurité, les premières sources d'inquiétude des responsables d'entreprise en termes de sécurité, même si en pratique, ils ne représentent qu'un faible pourcentage des sinistres informatiques enregistrés en entreprise.[15]

II.1.b ***Risques Logiques :*** Ces risques se résument dans les notions suivantes :

- ***L'accident :*** Il s'agit là d'un événement perturbant les données ou les flux de données, en l'absence de dommages physiques aux équipements (altération physique du matériel).
- ***L'erreur :*** Il peut s'agir d'une erreur de conception, de programmation, de paramétrage ou de manipulation des données et de leurs supports. L'erreur désigne des préjudices consécutifs à l'intervention humaine dans le processus de traitement automatisé des données.
- ***La malveillance :*** Il s'agit de tous actes traduisant la volonté manifeste de son auteur de faire usage, sans autorisation d'un système d'information, avec des intentions préjudiciables. Le virus informatique et l'acte de malveillance le plus médiatisé, il en existe une très grande diversité (Botnet, Chevaux de Troie, etc.).[15]

II.1.c ***Vulnérabilité :***

C'est une faille dans les actifs, les contrôles de sécurité technique ou les procédures d'exploitation ou d'administration utilisées dans l'entreprise. Elle consiste en général ; en une faiblesse dans la protection du système ; sous la forme d'une menace qui peut être exploité pour intervenir sur l'ensemble du système ; sous la forme d'une menace qui peut être exploité pour intervenir sur l'ensemble du système ou d'un intrus qui s'attaque aux actifs.

II.1.d *Vulnérabilités liées aux domaines physiques :*

- Manque de redondance et de ressource au niveau équipement,
- Accès aux salles informatiques non sécurisé,
- Absence ou mauvaise stratégie de sauvegarde des données.

II.1.e *Vulnérabilités liées aux domaines organisationnels :*

- Manque de : Ressource humain
- Absence de : contrôles périodiques, documents de procédures adaptés à l'entreprise ; moyens adaptés aux risques encours.

II.1.f *Vulnérabilités liées aux domaines technologiques :*

- failles nombreuses dans les services et applicatifs Web et les bases de données,
- pas de mises à jour des systèmes d'exploitation et des correctifs,
- pas de contrôle suffisant sur les logiciels malveillants,
- récurrence des failles et absence de supervision des évènements,
- réseaux complexes, non protégés,
- mauvaise utilisation de la messagerie.[16]

II.2 *Les Menaces :*

Les systèmes d'informations sont vulnérables par rapport à plusieurs menaces susceptibles de leur infliger différents types de dommage et des pertes significatives. L'importance des dégâts peut s'échelonner de la simple altération de données à la destruction complétée de centres de données informatique. Les effets de différentes menaces varient considérablement suivant les conséquences affectant l'entreprise ; certaines affectent la confidentialité ou l'intégralité des données, d'autres agissent sur la disponibilité des systèmes. Les menaces les plus connues sont représenté ci-dessous :

- ***Erreurs d'émissions*** :

Ce sont des menaces importantes pour l'intégralité des données et des systèmes. Ces erreurs ont souvent une origine humaine. En effet ; même les programmes les plus sophistiquées ne peuvent pas tout détecter .n'importe quelle personne intervenant sur le système d'information (utilisateur , administrateur ,système , développeur…) contribue directement ou indirectement à ces dangers mettant en péril la sécurité des systèmes .souvent l'erreur concerne une menace(erreur d'entrée de données, erreur de programmation..)Ou encore créer elle-même la vulnérabilité.

- ***Les Hackers :***

Le terme hacker ou encore cracker fait référence à la personne qui s'introduit dans les systèmes d'information sans autorisation pour, dans le pire des cas provoquer des dégradations dans les données ou les applications. Ses actions peuvent s'effectuer à partir de l'intérieur (dans le cas où il a pu obtenir un accès sur le réseau) ou de l'extérieur de

l'entreprise. il n'est pas facile de détecter sa présence sur les systèmes ni de connaitre ce qu'il a provoqué comme dégâts.

- ***Programmes malveillants :***

Ils font référence aux virus, chevaux de Troie, bombes logiques et autres logiciels indésirables souvent, leur point d'entrée se situe au niveau des ordinateurs personnels mal protégés lors de leur connexion sur Internet.Leurs effes peuvent s'étendre à tout le réseau de l'entreprise en co ntaminant d'autres matériels.[15]

III. Mécanisme de la Sécurité Informatiques :

Un mécanisme qui est conçu pour détecter, prévenir et lutter contre une attaque de sécurité ; Un seul mécanisme ne peut fournir tous les services de sécurité. On peut noter qu'un élément particulier sous-tend la plupart des mécanismes de sécurité en usage : les techniques cryptographiques. Le chiffrement - ou des transformations similaires - de l'information est le moyen le plus courant pour fournir une sécurité.

III.1 ***Mécanisme pour la sécurité d'échanges :*** ce mécanisme repose sur le cryptage (chiffrement) ; deux mots crèques: crypto=caché et graphie =écrire. La cryptographie est la science du chiffrement qui consiste à transformer tout ou une partie d'un texte dit clair en message chiffrer ou protégé :

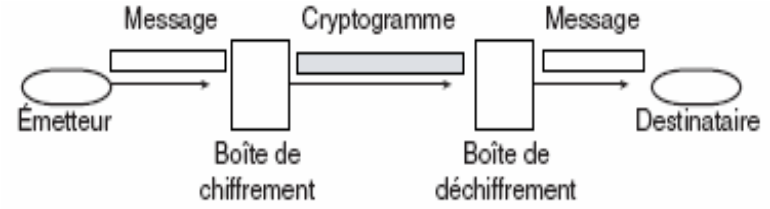


Fig.II. 8:Mécanisme pour la sécurité d'échanges

Le mécanisme de chiffrement émet un message X sous une forme secrète au moyen d'une clé K :

- L'émetteur dispose d'une fonction algorithmique E, qui, à X et K, associe E (K, X)
- Le récepteur reçoit E (K, X) et le déchiffre au moyen de sa clé K' avec sa fonction algorithmique de déchiffrement D, qui à E (K, X) et K' associe X. On a alors :

D (K', E (K, X)) = X

III.1.a ***Cryptage Symétrique :*** Historiquement, les premiers algorithmes de chiffrement étaient tels que K = K' et D = E–1.La clé K, unique, était secrète et l'algorithme du récepteur consistait à faire l'inverse de l'algorithme de l'émetteur Il suffisait de connaître la clé K. On parle alors de chiffrement symétrique car il n'y a qu'une clé.**[17]**

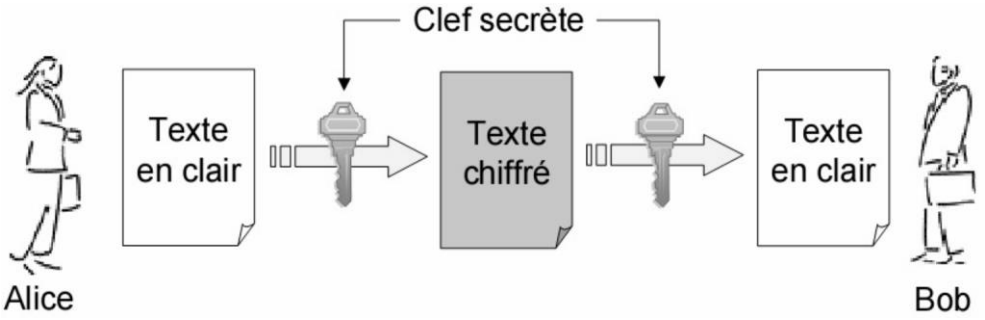


Fig.II. 9: Cryptage Symétrique

1. ***Algorithme DES (Data Encryption Standard) :***

1.1. ***Historique :***

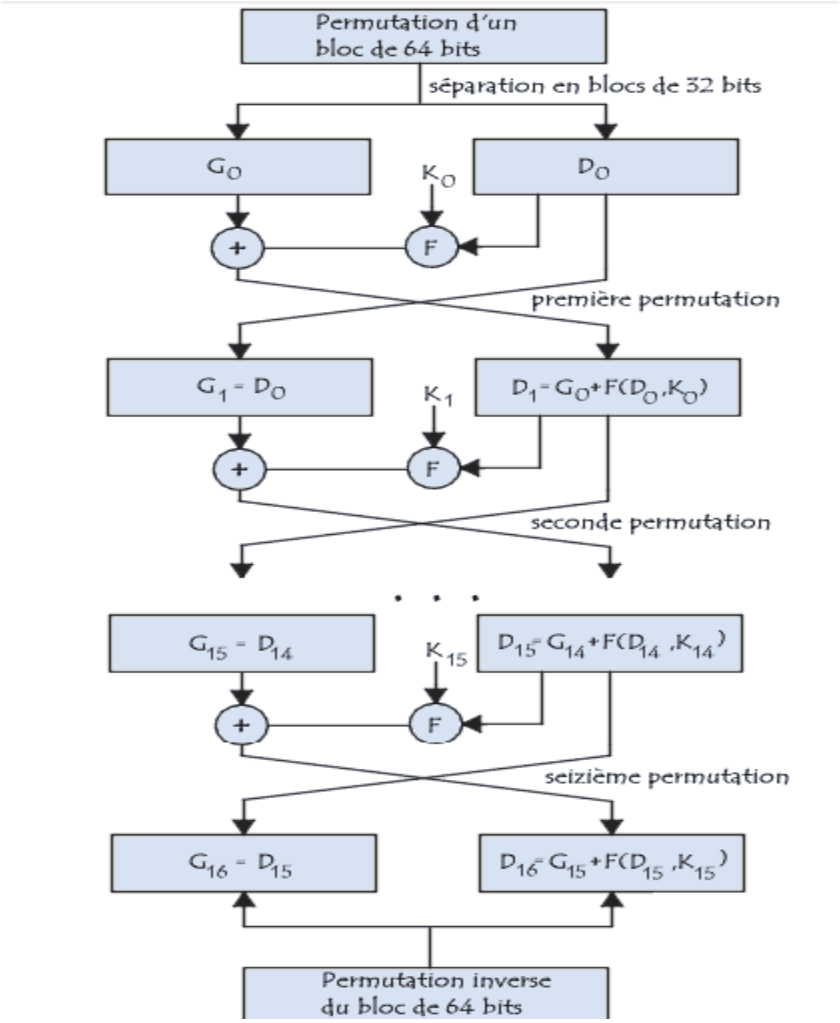
Le 15 mai 1973 le **NBS** (National Bureau of Standards, aujourd'hui appelé NIST - National Institute of Standards and Technology) a lancé un appel dans le Fédéral Registre (l'équivalent aux Etats-Unis du Journal Officiel en France) pour la création d'un algorithme de chiffrement répondant aux critères suivants :

- posséder un haut niveau de sécurité lié à une clé de petite taille servant au chiffrement et au déchiffrement.
- être compréhensible ; adaptable ; économique ; efficace et exportable
- ne pas dépendre de la confidentialité de l'algorithme.

Fin 1974, IBM propose « Lucifer », qui, grâce à la NSA (National Security Agency), est modifié le 23 novembre 1976 pour donner le **DES** (Data Encryption Standard). Le DES a finalement été approuvé en 1978 par le NBS.[18]

1.2. Le principe :

Il s'agit d'un système de chiffrement symétrique par blocs de 64 bits, dont 8 bits (un octet) servent de test de parité (pour vérifier l'intégrité de la clé). Chaque bit de parité de la clé (1 tous les 8 bits) sert à tester un des octets de la clé par parité impaire, c'est-à-dire que chacun des bits de parité est ajusté de façon à avoir un nombre impair de '1' dans l'octet à qui il appartient. La clé possède donc une longueur « utile » de 56bits, ce qui signifie que seuls 56 bits servent réellement dans l'algorithme. L'algorithme consiste à effectuer des combinaisons, des substitutions et des permutations entre le texte à chiffrer et la clé, en faisant en sorte que les opérations puissent se faire dans les deux sens (pour le déchiffrement). La combinaison entre substitutions et permutations est appelée code produit**.** La clé est codée sur 64 bits et formée de 16 blocs de 4 bits, généralement notés k à k. Etant donné que« seuls » 56 bits servent effectivement à chiffrer, il peut exister 2 (soit 7.2*10) clés différentes.[19]



1.3. Fonctionnement :

- ***Permutation initial:*** Dans un premier temps, chaque bit d'un bloc est soumis à la permutation initiale, pouvant être représentée par la matrice de permutation initiale (notée PI) suivante :

PI								
	58	50	42	34	26	18	10	2
	60	52	44	36	28	20	12	4
	62	54	46	38	30	22	14	6
	64	56	48	40	32	24	16	8
	57	49	41	33	25	17	9	1
	59	51	43	35	27	19	11	3
	61	53	45	37	29	21	13	5
	63	55	47	39	31	23	15	7

Tableau.II. 1:Permutation initial:

Cette matrice de permutation indique, en parcourant la matrice de gauche à droite puis de haut en bas, que le 58^{émé} bit du bloc de texte de 64 bits se retrouve en première position, le 50 en seconde position et ainsi de suite.

- ***Division en 2 blocs :*** Une fois la permutation initiale réalisée, le bloc de 64 bits est scindé en deux blocs de 32 bits, notés respectivement **G** et **D**

On note $\mathbf{G_0}$et $\mathbf{D_0}$l'état initial de ces deux blocs :

G_0							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8

D_0							
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Tableau.II. 2: Division en 2 blocs

- ***Fonction d'expansion*** : Les 32 bits du bloc **D** sont étendus à 48 bits grâce à une table (matrice) appelé table d'expansion (notée **E**), dans laquelle les 48 bits sont mélangés et 16 d'entre eux sont dupliqués :

E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Tableau.II. 3 : Fonction d'expansion

Ainsi, le dernier bit de **D** (c'est-à-dire le 7 bit du bloc d'origine) devient le premier, le premier devient le second, ...

De plus, les bits 1,4,5,8,9,12,13,16,17,20,21,24,25,28 et 29 de **D** (respectivement 57, 33, 25, l, 59, 35, 27,3, 6l, 37, 29, 5, 63, 39, 31 et 7 du bloc d'origine) sont dupliqués et disséminés dans la matrice.

- ***Ou Exclusif avec la clé :*** La matrice résultante de 48 bits est appelée **D'** où bien **E** [**D]**. L'algorithme DES procède ensuite à un OU exclusif entre la première clé **K** et **E** [**D]**. Le résultat de ce OU exclusif est une matrice de 48 bits que nous appellerons **D** par commodité (il ne s'agit pas du **D** de départ!).
- ***Fonction de substitution :*** Dest ensuite scindé en 8 blocs de 6 bits, noté D . Chacun de ces blocs passe par des fonctions de sélection (appelées parfois boîtes de substitution ou fonctions de compression), notées généralement S. Les premiers et derniers bits de chaque D détermine (en binaire) la ligne de la fonction de sélection, les autres bits

(respectivement 2, 3, 4 et 5) déterminent la colonne. La sélection de la ligne se faisant sur deux bits, il y a 4 possibilités (0, 1, 2,3). La sélection de la colonne se faisant sur 4 bits, il y a 16 possibilités (0 à15). Grâce à cette information, la fonction de sélection "sélectionne" une valeur codée sur 4 bits.

S_1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Tableau.II. 4:Fonction de substitution

Soit **D'**égal à 101110. Les premiers et derniers bits donnent 10, c'est-à-dire 2 en binaire. Les bits 2, 3,4 et 5 donnent 0111, soit 7 en binaire. Le résultat de la fonction de sélection est donc la valeur situé à la ligne n°2, dans la colonne n°7. Il s'agit de la valeur 11, soit en binaire 111.

- ***La 2éme permutation :*** Le bloc de 32 bits obtenu est enfin soumis à une permutation **P** dont voici la table :

P

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Tableau. II. 5 : La 2éme permutation

- ***Ou Exclusif :*** L'ensemble de ces résultats en sortie de **P** est soumis à un OU Exclusif avec le **G** de départ (comme indiqué sur le premier schéma) pour donner D1, tandis que le **D** initial donne **G.**
- ***Itération :*** L'ensemble des étapes précédentes (rondes) est réitéré 16 fois.
- ***Permutation Inverse :*** A la fin des itérations, les deux blocs **G** et **D** sont "recollés, puis soumis à la permutation initiale inverse :

PI-1

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Tableau.II. 6:Permutation Inverse

Le résultat en sortie est un texte codé de 64 bits ![18]

2. ***Algorithme IDEA (International Data Encryption Algorithm) :*** *Mis* au point par des chercheurs suisse mais, Breveté a propriété ASCOM, usage non commercial libre ; proposé comme remplacement ADES ; et il a des Bloc de 64 bits et Clé de 128 bits avec 8 rondes.
3. ***Algorithme AES (Advanced Encryption Standard) :*** Issu d'une compétition de cryptographie organisée par NIST (National Institute of Standards and Technology). C'est un Algorithme public, autorisation d'utilisation non discriminatoire ;a Chiffre symétrique par blocs (128 bits ou 192 bits ou 256 bits) ; Clés de 128, 192 et 256 bits ; avec des rondes identiques de 10 à 14 rondes. Chaque ronde utilise une clé de ronde : générée à partir de la clé principale (Applique 10 rondes avec une clé de 128 bits, 12 rondes avec une clé de 192 bits et 14 rondes avec une clé de 256 bits).

III.1.b ***Cryptage Asymétrique :*** il utilise deux clefs :

- **Clé publique :** sert à chiffrée un message.
- **Clé privée :** sert à déchiffré un message.

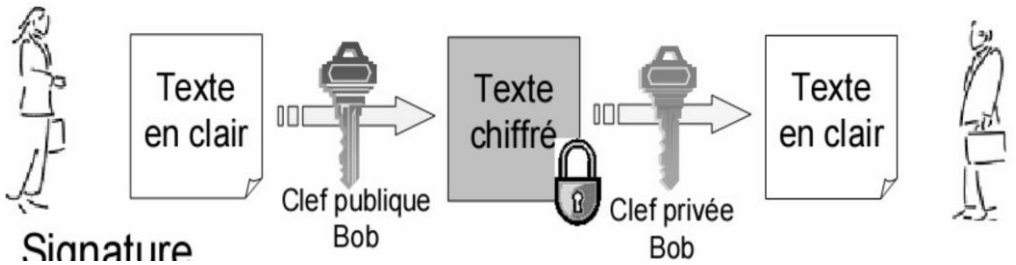


Fig.II. 10: Cryptage Asymétrique

1. ***Algorithme RSA (Rivest, Shamir, Adleman) :*** cet algorithme est utilisé pour assurer :

- la confidentialité : seul le propriétaire de la clé privée pourra lire le message chiffré avec la clé publique correspondante.
- la non-altération et la non-répudiation : seul le propriétaire de la clé privée peut signer un message (avec la clé privée). Une signature déchiffrée avec la clé publique prouvera donc l'authenticité du message.

1.1. Le concept : par exemple Bob possède un message confidentiel qu'il souhaite transmettre à Alice. Cette dernière doit construit deux clés ; une de chiffrement publique qu'elle transmet à Bob et une autre clé de déchiffrement privée qu'elle conserve soigneusement. Bob utilise la clé publique pour chiffrer le message, et le transmets à Alice. Alice utilise la clé privée pour déchiffrer le message reçu.

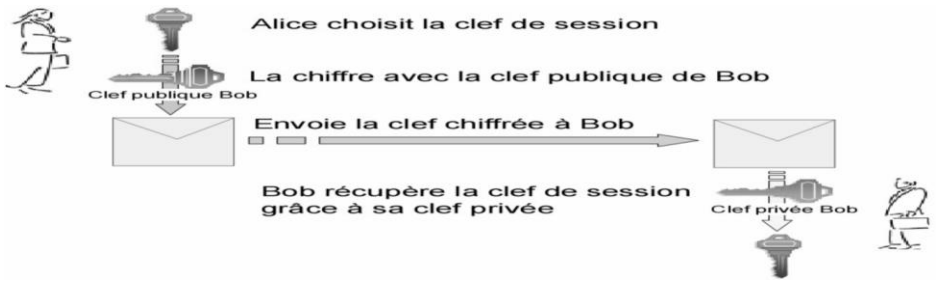


Fig.II. 11:Le RSA

1.2. Génération des clés : Soient deux grands nombres premiers « aléatoirement » choisis : **p** et **q**.

- Notons : **n = p*q et φ = (p-1)*(q-1)**
- Soient **d** un grand entier « aléatoirement » choisi, premier avec φ. Et e l'inverse de d modulo φ.
- La clé publique de chiffrement est le couple (**n**, **e**), la clé privée de déchiffrement le couple (**n**, **d**).

1.3. Chiffrement :

- Avant d'être chiffré, le message original doit être décomposé en une série d'entiers M de valeurs comprises entre 0 et n-1.
- Pour chaque entier M il faut calculer **C≡ M^e [n].**
- Le message chiffré est constitué de la succession des entiers C.

1.4. Déchiffrement :

- Conformément à la manière dont il a été chiffré, le message reçu doit être composé d'une succession d'entiers C de valeurs comprises entre 0 et n-1.
- Pour chaque entier C il faut calculer **M≡ C^d [n].**
- Le message original peut alors être reconstitué à partir de la série d'entiers M.

1.5. La fiabilité : La sécurité de l'algorithme RSA repose sur la difficulté à factoriser n. Pour décrypter le message, il est nécessaire de trouver d connaissant e, ce qui nécessite de recalculer φ, et donc de connaître p et q, les deux facteurs premiers de n. Or, la factorisation d'un entier (de très grande taille) en facteurs premiers est extrêmement difficile, cette opération nécessitant une capacité de calcul très importante.

Par exemple : en 2010, l'INRIA et ses partenaires ont réussi à factoriser une clé de 768 bits. Il leur a fallu deux ans et demi de recherche, et plus de 10^20 calculs. C'est à ce jour le meilleur résultat connu de factorisation.[20]

2. *Algorithme Elgamal (Taher Elgamal) :*

Le crypto système de Elgamal, ou chiffrement El Gamal (ou encore système d'El Gamal ...) est un algorithme de cryptographie asymétrique fondé sur le problème du logarithme discret. Il a été créé par Taher Elgamal.. Il peut être utilisé pour le chiffrement, mais aussi la signature électronique, par exemple l'algorithme DSA du NIST.

L'algorithme est décrit pour un groupe multiplicatif $\mathbb{Z}p^*$, p premier, mais n'importe quel groupe cyclique fini pour lequel le problème du logarithme discret est difficile convient. On suppose que Bob veut envoyer un message à Alice (le chiffrement est asymétrique).

- Alice calcule deux clés, une clé publique et une clé privée : elle choisit d'abord p suffisamment grand pour que le calcul du logarithme discret soit infaisable pratiquement dans le groupe multiplicatif $\mathbb{Z}p^*$, g un générateur de ce groupe et un entier naturel s, $s < p$, puis calcule $h = g^s \bmod p$. L'entier s est la *clé secrète*, le triplet (p, g, h) la *clé publique*. Cette dernière seule est connue de Bob.
- Le message clair de Bob est supposé être un m dans $\mathbb{Z}p^*$, Bob choisit aléatoirement un nombre entier k puis calcule (dans $\mathbb{Z}p^*$, $c_1 = g^k$ et $c_2 = mh^k$. Le message chiffré est le couple (c_1, c_2) que Bob envoie à Alice.
- Alice peut déchiffrer le message reçu en calculant $m = c_2 / c_1^s$. En effet :

$$\frac{c_2}{{c_1}^s} = \frac{m \cdot h^k}{g^{ks}} = \frac{m \cdot h^k}{h^k} = m$$

Casser l'algorithme Elgamal est dans la plupart des cas au moins aussi difficile que de calculer le logarithme discret. Cependant, il est possible qu'il existe des moyens de casser l'algorithme sans résoudre le problème du logarithme discret.

III.1.c *Cryptage Hybride :*

La cryptographie asymétrique est intrinsèquement lente à cause des calculs complexes qui y sont associés, alors que la cryptographie symétrique brille par sa rapidité. Toutefois, cette dernière souffre d'une grave lacune, on doit transmettre les clés de manière sécurisée (sur un canal authentifié). Pour pallier ce défaut, on recourt à la cryptographie asymétrique qui travaille avec une paire de clés : la clé privée et la clé publique. La cryptographie hybride combine les deux systèmes afin de bénéficier des avantages (rapidité de la cryptographie symétrique pour le contenu du message) et utilisation de la cryptographie "lente" uniquement pour la clé.[16]

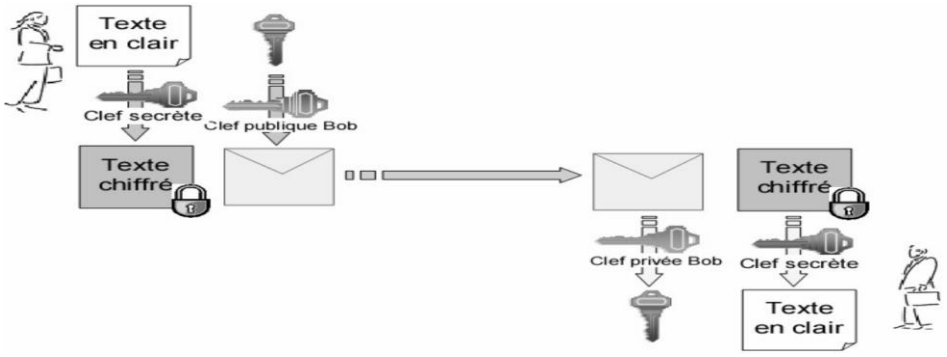


Fig.II. 12: Cryptage Hybrides

III.1.d ***Signature électronique:*** est basée sur l'utilisation conjointe d'une fonction de hachage et de la cryptographie asymétrique

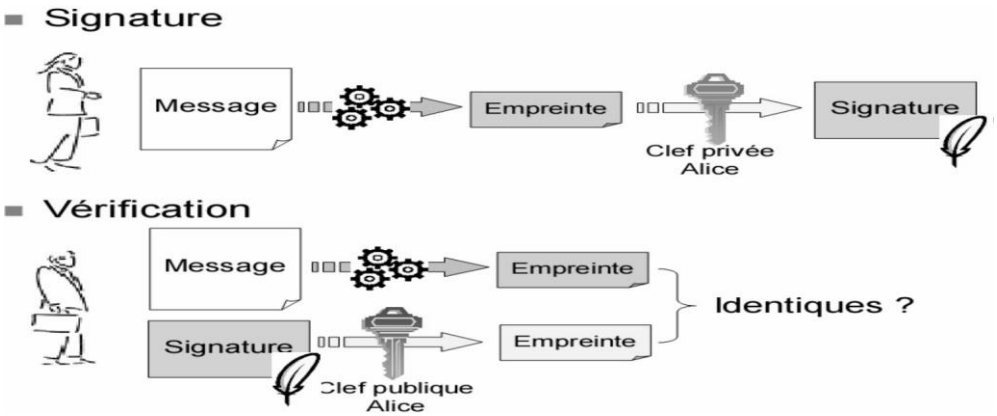


Fig.II. 13: Signature électronique

III.2 ***Mécanisme pour la sécurité de ressources :***

III.2.a ***Firewalls :***Un Firewall, ou pare-feu ou encore coupe-feu est un logiciel, un équipement réseau, ou les deux, qui analyse le trafic qu'il reçoit et prend une décision

- en fonction des adresses de couche 2, 3 et 4 filtrage sans état
- en fonction de l'état d'une connexion et/ou des drapeaux TCP filtrage dynamique ou « à états »
- en fonction du contenu de couche 7 filtrage applicatif
- en fonction de tout ce qui précède et de l'identité présumée de l'utilisateur pare-feu authentifiant
- Un pare-feu protège tout un réseau

1. ***Un Firewall sans état :*** il ne sait pas si un paquet appartient à une connexion déjà établie ; il ne tient compte que de la source ; la destination et les ports cibles. Il regarde chaque paquet indépendamment des autres et le compare à une liste de règles pré configurées.
2. ***Un Firewall à état :*** connaît l'état de chaque connexion ; conserve une table répertoriant les connexions et leurs états ; il fait l'analyse de chaque paquet provoque une mémorisation.

3. ***Un Firewall applicatif (proxy de sécurité)*** **:** réalisé au niveau de la couche Application ; Il analyse du trafic échangé au niveau application (niveau 7) pour appliquer une politique de sécurité spécifique de chaque application ; vérifie la conformité totale du paquet à un protocole donné un Proxy pour chaque protocole d'application SMTP, FTP, HTTP,...

III.2.b ***DMZ :*** est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet (ou d'un autre réseau) par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet.[21]

III.3 ***D'autre mécanisme de sécurité :***

III.3.a ***PKI (Public Key Infrastructure) :*** L'infrastructure PKI repose sur la notion de chiffrement asymétrique. Pour s'authentifier, en revanche, le détenteur des clés utilise un certificat, sorte de document électronique faisant office de carte d'identité électronique. Inséré dans un message, lors d'un paiement sur Internet par exemple, ce certificat joue le rôle de signature numérique. Il contient des informations relatives à l'identité du détenteur, son champ d'application (date de validité, types d'applications, etc.) et la clé publique. Un tier de confiance garantit l'association ente un individu et les données contenues dans le certificat.

III.3.b ***Antivirus :*** logiciel censé protéger ordinateur contre les logiciels (ou fichiers potentiellement exécutables) néfastes. Ne protège pas contre un intrus qui emploie un logiciel légitime, ou contre un utilisateur légitime qui accède à une ressource alors qu'il n'est pas autorisé à le faire.

III.3.c **Analyse des vulnérabilités ("Security audit")** : identification des points de vulnérabilité du système. Ne détecte pas les attaques ayant déjà eu lieu, ou lorsqu'elles auront lieu.

III.3.d ***Quelques protocoles de sécurités :***

1. ***SSL (Secure Socket Layer)***de Netscape est le protocole le plus répandu pour établir une connexion sécurisée entre client et serveur. Il est situé entre les couches TCP et HTTP. Ce protocole public utilise une clé de 40 bits (version d'exportation) avec l'algorithme RSA pour chiffrer toute la transaction. Ce protocole ne peut garantir l'identité de l'interlocuteur !

2. ***SET (Secure Electronic Transaction) :*** est la convergence des deux procédures de sécurisation STT *(Secure Transaction Technology)* de Visa et Microsoft et SEPP *(Secure*

ElectronicPayment Protocol) de Mastercard, IBM et Netscape. Il permet de sécuriser les transactions par cartes bancaires (chiffrement par clés publiques/privées et authentification des parties).

3. ***C-SET (Chip Secure Electronic Transaction) :*** est l'adaptation du protocole SET à la carte à puce française.

4. ***S/MIME (Secure Multipurpose Internet Mail Extension)***est le protocole le mieux accepté pour la sécurisation des courriers électroniques.

5. ***PGP (Pretty Good Privacy) :.*** Le cryptage de toute l'information par une clé publique nécessitant un temps de calcul élevé, PGP utilise une technique plus rapide : Le document est compressé (pour éviter les redondances) puis crypté avec une clé de session aléatoire (cryptage rapide), seule la clé de session est cryptée par la clé publique du destinataire et ajoutée au document. Le destinataire utilise sa clé privée pour décrypter la clé de session et peut ainsi décrypter le document et le décompresser.[22]

IV. Conclusion :

La sécurité d'un système informatique devient plus difficile avec le progrès de la technologie de la communication ; on a vu précédemment que la défection d'un système n'est pas aux niveaux logiques seulement mais aussi en niveau physique.

Chapitre III

E-Commerce

I. Introduction :

L'expansion de l'Internet provoque des changements profonds au niveau commercial, de la publicité jusqu'à la livraison, tous les détails d'une relation commerciale entre le vendeur et le client passe aujourd'hui par l'Internet, ce dernier met à la disposition de tous les partenaires, tous les outils pour finaliser l'achat et la vente en succès et en toute sécurité, ce qu'on l'appelle aujourd'hui le E-Commerce.

Dans ce chapitre on va parler de l'importance de l'e-commerce à nos jours-là ; mais premièrement on va présenter le grand facteur intervenir dans ce genre des services qui est l'internet, en détaillant ensuit le rôle d'un système serveur/client et enfin on vous présente le cahier de charge de ce projet.

II. Internet :

II.1 Définition : L'Internet est un système de communication qui permet aux ordinateurs autour du monde de communiquer et de d'échanger de l'information entre eux. Cette communication entre ordinateurs permet plusieurs possibilités et offre une masse d'informations chaque jour plus important dans des domaines comme la médecine, la science et la technologie, les jeux. Lorsque deux ordinateurs communiquent pour s'échanger des informations, il faut qu'ils utilisent une méthode commune de conversation. On parle alors d'un protocole informatique.

En informatique, un protocole est un ensemble de règles suivies par deux ordinateurs lors de L'échange de l'information. Il existe de nombreux protocoles différents. Nous n'évoquerons que TCP/IP. [23]

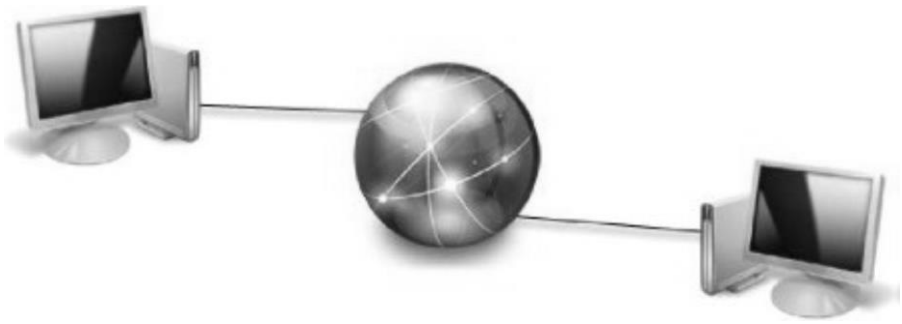


Fig.III. 1 : Internet

II.2 **Le Serveur :** l'ordinateur qui fournit l'information est appelée un serveur : lorsque les informations (un texte, une image, un courrier,...) doivent être envoyées sur Internet, l'ordinateur qui fournit l'information :

- découpe le document à transmettre en petits paquets à l'aide d'un programme spécialisé;
- chaque paquet est muni de l'adresse de l'expéditeur et de l'ordinateur de destination ;
- chaque paquet est envoyé indépendamment des autres: il passe peut-être par un autre chemin.

II.3 ***Un Client :*** C'est l'ordinateur qui reçoit des informations ; ces dernières parviennent à l'ordinateur de destination

- sous la forme de petits paquets ;
- qui peuvent arriver dans le désordre (selon le chemin suivi) ;
- ces informations sont recombinées et remises en ordre par un programme spécialisé dans l'ordinateur d'arrivée.

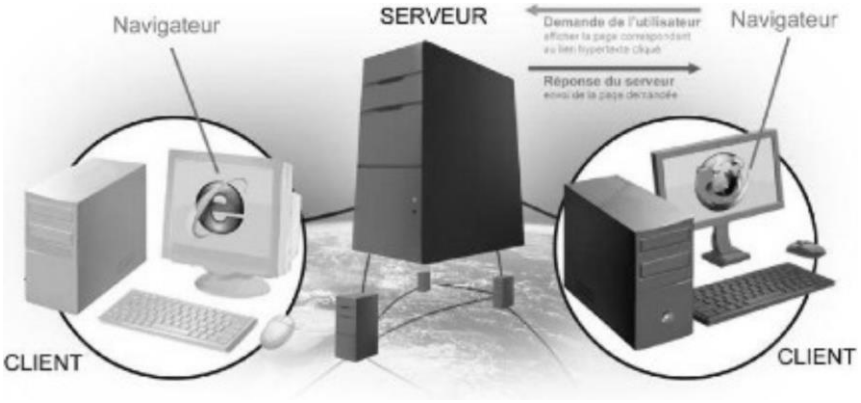


Fig.III. 2:Le Client

II.4 ***Architectures client/serveur :***

Il en existe 3 architectures client/serveur :

II.4.1 ***Client-serveur de pair à pair*** : place la logique de présentation sur le poste client, mais laisse les traitements sur le serveur.[24]

II.4.2 ***Client-serveur à deux niveaux (fat client-thin server) :*** est actuellement le plus répandu et le mieux maîtrisé. Il laisse au client la charge de la couche de présentation et de la logique d'application, le serveur abritant la gestion des données. Ce modèle d'architecture comporte des limitations majeures à savoir :

- il génère un trafic sur le réseau élevé. L'utilisation de réseaux à haut débit peut dans certains cas régler ce problème,
- il est difficile de se connecter à plusieurs applications ou plusieurs bases de données en même temps.
- une mauvaise extensibilité qui a pour conséquence de limiter le nombre d'utilisateurs à une centaine ; des temps de réponse qui peuvent se révéler désastreux.
- la création de clients «trop gros» qui disposent de toute la logique applicative et dont la maintenance coûte cher (à chaque modification, il faut mettre à jour tous les postes clients.[25]

II.4.3 ***Client-serveur à trois niveaux :*** ôte la logique et le traitement de l'application du poste client pour les mettre sur un serveur spécialisé. Le client conserve néanmoins la présentation incluant le dialogue avec l'utilisateur et plus généralement l'interface homme-machine. La communication entre le client et le serveur d'applications et entre le serveur d'applications et le serveur de données s'établissent par l'intermédiaire d'une

couche médiateur. Cette couche gère les requêtes émises par les clients, répartit la charge entre les serveurs, gère la sécurité, etc. Cette architecture logicielle à trois niveaux se combine du coup avec une architecture matérielle elle aussi à trois niveaux où :

- le poste client de type PC-Windows gère la présentation ;
- un serveur d'application de taille intermédiaire (comme Windows NT ou OS2 Warp Server) gère la logique d'application ;
- un serveur de données de type gros système ou serveur départemental offrant des performances élevées gère les requêtes multiples aux bases de données.

L'avantage du modèle à trois niveaux (aussi appelé trois tiers) est d'enlever l'application du poste client, là où elle est le plus difficilement maintenable et sécurisa blé. Par contre, l'ajout de serveurs intermédiaires complique l'architecture finale déployée et les règles de gestion associées. Ainsi, au niveau de l'architecture de l'application, il est difficile de partitionner simplement les services offerts et rendus, de placer les programmes sur l'architecture matérielle et de gérer les accès hétérogènes aux données.[26]

III. Le web :

III.1 Introduction au World Wide Web(WWW) :

On appelle «**Web**» (nom anglais signifiant «**toile**»), contraction de «World Wide Web» (d'où l'acronyme www), une des possibilités offertes par le réseau Internet de naviguer entre des documents reliés par des liens hypertextes.

Le principe de web repose sur l'utilisation d'hyperliens pour naviguer entre des documents (appelés «**pages web**») grâce à un logiciel appelé **navigateur** (parfois également appelé fureteur ou butineur ou en anglais browser). Au-delà des liens reliant des documents formatés, le web prend tout son sens avec le protocole HTTP permettant de lier des documents hébergés par des ordinateurs distants (appelés serveurs web, par opposition au client que représente le navigateur). Sur Internet les documents sont ainsi repérés par une adresse unique, appelée URL, permettant de localiser une ressource sur n'importe quel serveur du réseau internet.[27]

III.2 Une page Web : Une page web est ainsi un simple fichier texte écrit dans un langage de description (appelé HTML), permettant de décrire la mise en page du document et d'inclure des éléments graphiques ou bien des liens vers d'autres documents à l'aide de balises.

III.3 Un Site Web : Est un ensemble cohérent de pages, qui peuvent toutes être consultées en suivant des hyperliens à l'intérieur du site. L'adresse Web d'un site correspond en fait à l'URL d'une page Web, prévue pour être la première consultée : la page d'entrée ou page d'accueil du site. La consultation des pages d'un site s'appelle une visite, car les hyperliens entre les pages permettent de consulter toutes les pages du site sans le quitter (sans devoir consulter une page Web hors du site). Il faut toutefois noter qu'une visite peut commencer par n'importe quelle page, particulièrement lorsque son URL est donnée par un moteur de recherche. Techniquement, rien ne distingue la page d'entrée d'une autre page.

Il en existe deux types des sites web :

III.3.1 ***Un site web Statique :*** les pages du site ne sont pas modifiables par des utilisateurs. Le site est donc rempli et mis à jour par l'administrateur qui le fait depuis son poste de travail. Une fois le site mis à jour sur l'ordinateur de l'administrateur, celui-ci devra être envoyé sur le site via FTP. Le site est dit statique car les pages HTML qui le compose sont toujours identiques entre deux visites sans mise à jour. Le serveur donc n'a pas besoin d'éléments de Scripting.

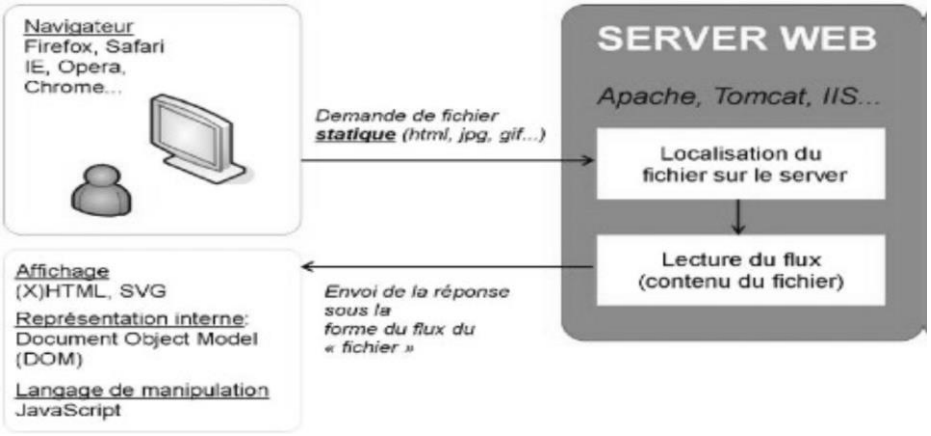


Fig.III. 3:Un site web Statique

III.3.2 ***Un site web Dynamique :*** les pages du site qui le compose peuvent être modifiables par les visiteurs. De plus, entre deux visites sur un même site, le contenu de la page peut être différent sans action de l'administrateur du site Internet. Les grandes applications de ce type de site sont : les forums, les Wiki (Wikipédia étant le plus grand représentant du genre) et tous les sites communautaires (Facebook, Twitter, hi5, etc.).

Le serveur qui fait fonctionner le site utilise une technologie de scripting (comme PHP, Ruby, Python ou Perl) ainsi qu'une base de données comme MySQL.

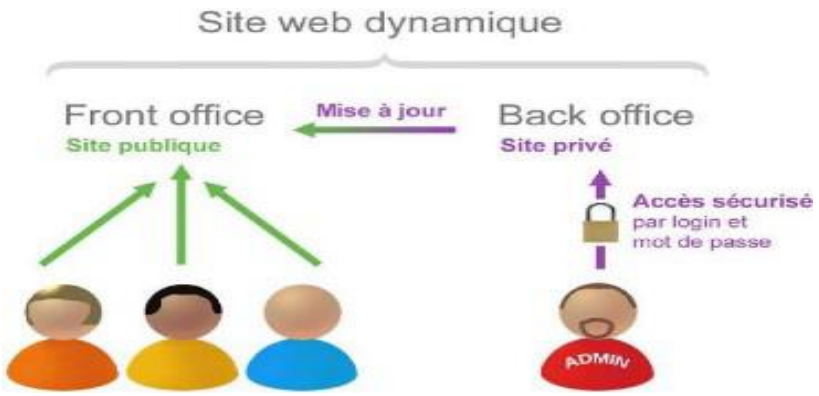


Fig.III. 4:Un site web Dynamique

III.4 Quel type d'utilisation pour quel site ?

On utilisera un site web statique pour une utilisation bien particulière. On utilisera ce fonctionnement pour un site web nécessitant peu de maintenance, peu de mise à jour et contenant peu de pages.
En effet, comme la mise à jour d'un site Internet statique peut être fastidieuse, on utilisera ce type de site uniquement si les mises à jour sont exceptionnelles. Car, à chaque mise à jour il faudra modifier la page HTML du site et la mettre en ligne en effectuant une copie par FTP.

On utilisera plutôt un site dynamique si on souhaite créer une interaction avec ses lecteurs. Le site dynamique permet de se connecter en ligne sur son site pour réaliser sa mise à jour en direct. Une fois la mise à jour du site dynamique effectuée, le résultat apparaît directement aux lecteurs. On privilégiera donc les sites web dynamiques pour les sites permettant aux visiteurs de laisser des commentaires (blogs) ou de converser avec d'autres lecteurs (forums). De même si le site doit être mis à jour très fréquemment (plusieurs fois par semaine) on pourra choisir de créer un site dynamique même si aucune interaction n'est prévue avec les visiteurs. Par exemple pour réaliser un site vitrine présentant les 10 produits vendus par une entreprise on pourra choisir :

- ***Un site statique*** si les produits ne sont modifiés qu'une ou deux fois par mois et qu'un ou deux nouveaux produits sont ajoutés au catalogue chaque année.
- ***Un site dynamique*** si on souhaite que les visiteurs ajoutent des commentaires sur les fiches produits et/ou qu'il faut modifier très souvent (ajout, suppression, modification) les fiches produits.[28]

IV. E-Commerce :

IV.1 Définition : Historiquement .le « commerce électronique « a fait son apparition des que l'internet s'est ouverte aux entreprises, ainsi avec l'avènement des serveurs Web qui permettent de présenter l'entreprise et les produits qu'elle voudrait mettre en vente, le commerce électronique a multiplié ses fonctionnalités et a évolué.

L'expression « commerce électronique est souvent associée à la vente de produit ou de service sur internet. Les transactions peuvent s'effectuer entre l'entreprise et un nouveau client, mais nous pouvons aussi faire des affaires avec des particuliers comme nous ou même avec d'autre entreprise. D'après les prévisions, le commerce entre entreprises pourrait même augmenter dix fois plus vite que le commerce grand public.

IV.2 Les types d'E-Commerce :

IV.2.1 B2B (Business to Business) :

Ceux sont les entreprises qui font affaire avec d'autres, comme les fabricants qui vendent a des distributeurs et grossistes, qui a leur tour vendent aux détaillants. La tarification est basée sur la quantité de l'ordre et est souvent négociable

IV.2.2 B2C (Business to consumer) :

Ceux sont les entreprises vendant au grand public en général grâce à des catalogues en utilisant des logiciels panier. En volume en dollars, B2B à la palme, cependant B2C est

vraiment ce que l'utilisateur, a en tête en ce qui concerne l'e-commerce électronique, dans son ensemble.

IV.2.3 C2B (consumer-to-Business) :

Le consumer to business (C2B) est un modèle d'entreprise (business model) dans lequel les consommateurs (les particuliers) sont au service de l'entreprise en apportant un produit ou une prestation, et non le contraire comme c'est le cas traditionnellement. Ce type de système économique est qualité de modèle d'entreprise inversé. Deux événements ont rendu possible l'émergence de ce nouveau type de relation commerciale.

IV.2.4 C2C (Consumer-to-Consumer) :

Il existe de nombreux sites offrants de petites annonces gratuites, enchères, et des forums ou les particuliers peuvent acheter et vendre en ligne grâce au système de paiements tels que Papal, ou les gens peuvent envoyer et recevoir de l'argent en ligne en toute simplicité. Le service d'enchère d'eBay est un bon exemple de commerce de personne, des transactions ont lieu tous les jours depuis 1995. Les entreprises utilisant les réseaux internes, pour offrir a leurs employés des produits et services en ligne -- pas nécessairement en ligne sur le web – se sont livrées à B2E (Business—to-Employée) e-commerce.[23]

IV.3 Les Avantages du E-Commerce :

Dans un premier temps, nous allons donc analyser les avantages que l'e-commerce procure à l'entreprise ainsi qu'à ses clients

IV.3.1 Pour l'entreprise :

- Il ouvre un nouveau canal de distribution, un circuit complémentaire pour certain produit et services de l'entreprise.
- Il permet de couvrir des niches de marcher dont l'atteinte serait jugée trop onéreuse par les moyens classiques de commercialisation.
- Il favorise l'interactivité en développant une relation personnelle avec le consommateur ou le client, facilitant la vente « one to one » (personnalisée) et le sur-mesure.
- Il facilite les transactions en évitant à l'acheteur de se déplacer (donc de lui faire gagner du temps) tout en lui offrant un service identique et confortable.
- Il donne la possibilité de réduire les prix publics des produits en éliminant la marge laissée habituellement aux intermédiaires, comme certains couts de structure.
- L'enregistrement des données via internet est quasiment automatique et demande peu d'effort.

IV.3.2 Pour le client :

- Un accès facile à un plus large éventail de produits et de services.
- Pas d'horaire d'ouverture (24 H /24H).
- La recherche du meilleur prix ;
- Pas de pression de la part des vendeurs ;
- Un marché aux puces à l'échelle mondiale ;

- Un gain de temps ;
- Une offre actualisée (on trouve les derniers modèles).
- Possibilité d'acheter à n'importe quand et n' importe où dans le monde.

IV.4 Inconvénients :

IV.4.1 Pour l'entreprise :

- L'incertitude et le manque de confiance autour de la sécurisation des moyens de paiement, malgré le fait que dorénavant les méthodes de cryptage de données assurent une confidentialité quasi parfaite lors de la transaction.
- La résistance des intermédiaires (grossistes, distributeurs) qui craignent une destruction d'emplois assortie d'une perte de chiffre d'affaires.

IV.4.2 Pour le client :

- L'insécurité des paiements et la peur de tomber sur un cybermarchand malhonnête qui ne livre pas.
- Le manque de relations humaines et le sentiment d'isolement devant sa machine (cas des internautes peu expérimentés).
- Le manque de contact avec le produit.
- Les difficultés de recours en cas d'ennuis.

V. Mode de paiement :

Le contrat électronique en ligne passe par le paiement des services et des biens. Le paiement est l'aspect le plus controversé du commerce électronique car il demeure, l'obstacle à son développement face au risque encore assez important de fraude et de piratage. En effet, seules les méthodes sur le paiement sur le réseau pourront favoriser la confiance des opérateurs : banques, commerçants, utilisateurs …

Portant, les risques de détournement d'un numéro de carte bancaire sur le réseau ne sont pas plus grands que ceux l'empreinte laissée après un paiement dans un restaurant, d'autant que le risque, pour le consommateur est en générale supporté par le banquier. La recherche de moyens de paiement plus surs assurera sans doute le développement du commerce électronique, notamment par la cryptographie. Le problème de la signature électronique va de pair avec celle des moyens cryptographiques. Plusieurs types de moyens de paiement peuvent être distingués :

- la carte bleue : est le moyen le plus utilisé sur internet l'utilisateur communique son numéro avec sa date d'expiration. Les risques d'interception du numéro de la carte bleue sont faibles.
- les jetons électroniques et les porte-monnaie électroniques : certains sociétés proposent des « monnaies virtuelles » visant à aider les sites commerciaux a fidéliser leurs clients. La pratique est bien connue des adeptes du marketing et déjà nombreux sont les sites qui offrent des cadeaux (« coupants virtuels ») à leurs visiteurs fidèles pour les récompenser.

- Mastercard.
- Paypal : géré par l'entreprise américaine Paypal Inc., est un service de paiement électronique qui permet de payer des achats, de recevoir des paiements, ou d'envoyer et de recevoir de l'argent.[29]

VI. Cahier de charge :

Le but de ce projet est de créer un site web e-commerce pour le vente et l'achat des produits électroniques. Cette boutique en ligne permettra d'offrir beaucoup des services à savoir :

- Recherche de produit,
- Consultation de catalogues de produits,
- Lancer une commande en ligne,

Cette application Web permettra de cibler une nouvelle catégorie de clientèles (locale et internationale), et d'offrir une meilleure qualité de service en communication et en commerce. Ce site devra contenir deux interfaces séparées :

VI.1 Partie administrateur du site :

Cette partie permettra le stockage des documents et leur publication sur internet. Ce mécanisme est accompli par l'administrateur du site qui doit s'authentifier avec son login et son mot de passe à partir de la page d'accueil. Après son authentification comme administrateur, il pourra accéder à la page qui lui permettra de gérer les outils d'administration. Le site affichera toutes les tâches qui peuvent être effectuées par l'administrateur qui pourra :

- Ajouter un produit : chaque produit est caractérisé par son nom et sa catégorie.
- Gérer des comptes : ajout ou suppression d'un compte. Chaque compte est caractérisé parle login, le mot de passe, le nom et le prénom de l'administrateur.
- Déconnexion : cela permet la sécurité de l'interface.

VI.2 Partie client :

Cette interface doit être accessible à n'importe quel internaute cherchant des produits et effectuant des commandes.

VII. Etude des besoins :

Dans cette section du chapitre, nous nous intéressons aux besoins des utilisateurs traités :

VII.1 Besoins fonctionnels :

Les besoins fonctionnels se présentent en :

1. ***Caractéristique d'un produit :*** Notre site doit disposer d'une vitrine virtuelle à travers laquelle le client peut consulter une grande variété des produits, il sera donc indispensable d'y présenter les prix et les caractéristiques techniques de chaque produit pour faciliter la sélection du produit à acheter.

2. ***L'inscription du Client :*** Jusqu'à ce stade, le client est toujours anonyme mais pour pouvoir passer à un stade plus rigoureux, il faut qu'il s'inscrive, cela se fait uniquement pour la première commande mais après, notre client peut s'authentifier avec son E-mail et son mot de passe pour passer d'autres commandes.
3. ***Ajout de produit au panier :*** Après le choix d'un produit le client doit mentionner la quantité qui s'ajoute automatiquement à son panier avec le prix unitaire et le prix total.
4. ***Mode de livraison :***
   Un client qui a déjà confirmé sa commande il est libre de choisir le mode de livraison de sa marchandise soit à domicile ou postal.
5. ***La livraison à domicile :*** En choisissant cette option comme mode de livraison, le client devrait remplir soigneusement un formulaire contenant les informations nécessaires telles que :
   - Le nom du destinataire.
   - L'adresse précise de livraison.

6. ***La livraison postal :*** en plus de l'information précis dans la livraison domicile ; le client doit rentrer sont code postale.
7. ***La confirmation de la demande :*** Jusqu'à cette phase on a un client, une commande et une adresse de livraison le chemin maintenant est plus clair, la commande ne passera qu'après la validation de toutes les informations qui sont affichées dans une seule interface avant de passer à la phase de payement.
8. ***Le mode de paiement :*** le client doit choisir le mode de paiement qu'il arrange :
   - ***Paiement à main :*** en livrant la commande au client ; il paye à main.
   - ***Paiement par carte bancaire :*** le client doit choisir un des cartes qu'il doit effectuer son paiement parmi une liste des cartes proposés ; indiquer le numéro de la carte et sa valeur de vérification.

9. En fin un petit message de remerciement à nos clients avec une idée sur l'adresse, et la date de livraison.

VII.2 Les besoins non fonctionnelles :

Les besoins non fonctionnels sont importants car ils agissent de façon indirecte sur le résultat et sur le rendement de l'utilisateur, ce qui fait qu'ils ne doivent pas être négligés, pour cela il faut répondre aux exigences suivantes :

1. ***Fiabilité :*** L'application doit fonctionner de façon cohérente sans erreurs et doit être satisfaisante.
2. ***Les erreurs :*** Les ambigüités doivent être signalées par des messages d'erreurs bien organisés pour bien guider l'utilisateur et le familiariser avec notre site web.
3. ***Ergonomie et bonne Interface :*** L'application doit être adaptée à l'utilisateur sans qu'il ne fournisse aucun effort (utilisation claire et facile) de point de vue navigation entre les différentes pages, couleurs et mise en textes utilisés.

4. ***Sécurité :*** Notre solution doit respecter surtout la confidentialité des données personnelles des clients qui reste l'une des contraintes les plus importantes dans les sites web.
5. ***Compatibilité et portabilité :*** Un site web quel que soit son domaine, son éditeur et son langage de programmation ne peut être fiable qu'avec une compatibilité avec tous les navigateurs web et tous les moyens que ce soit PC, IPAD ou Mobiles.

VIII. Conclusion :

La sécurité informatique ne s'invente pas, et est encore entourée malheureusement d'un certain halo shamanique ce qui compte, en définitive, c'est de se former en permanence pour rester à niveau en la matière. C'est une tâche dont l'informaticien du groupe web devra avoir à cœur de s'acquitter de façon particulièrement consciencieuse l'incurie des administrateurs est en effet pour beaucoup dans l'état actuel de la sécurité informatique de l'Internet Ce projet n'est pas gérer par une société, c'est pour cela qu'on a se limité de faire une présentation d'un cahier de charge qui met au appartenant d'un client certaines services qui lui assure une bonne navigation dans une zone sécurisé et cohérente.

Chapitre IV

Conception ET Réalisation de l'application

I. Introduction :

Avant de débuter ce projet il faut faire un analyse conceptuelle de chacun des acteurs, en plus de données une vue sur les outils utilisées au cours de l'élaboration de ce projet.

II. Les outils :

Lors du développement de cette application, j'ai utilisé, les outils logiciels suivant

II.1 PHP :

Désigne un langage de programmation libre destiné à produire des pages web dynamique ; il est actuellement le langage le plus utilisé pour l'élaboration des sites web, syntaxe est très proche de celles des langages C, Java et Perl .

Fig.IV. 1:PHP

II.2 MYSQL :

Le MySQL est un système de Gestion de base de données(SGBD) parmi les plus répandus dans le monde .il s'agit d'un logiciel existant aussi bien en version open source qu'en version commercial.

Fig.IV. 2:MYSQL

II.3 Apache :

Le logiciel libre *Apache HTTP Server* (Apache) est un serveur HTTP créé et maintenu au sein de la fondation Apache. C'est le serveur HTTP le plus populaire du World Wide Web.

Fig.IV. 3: Apache

II.4 Le logiciel EasyPHP :

Il s'agit d'une plate-forme de développement Web, permettant de faire fonctionner localement (sans se connecter à un serveur externe) des scripts PHP. EasyPHP n'est pas en soi un logiciel, mais un environnement comprenant deux serveurs (un serveur web Apache et un serveur de bases de données MySQL).

Fig.IV. 4: Le logiciel EasyPHP

- ***Partie configuration :***

.

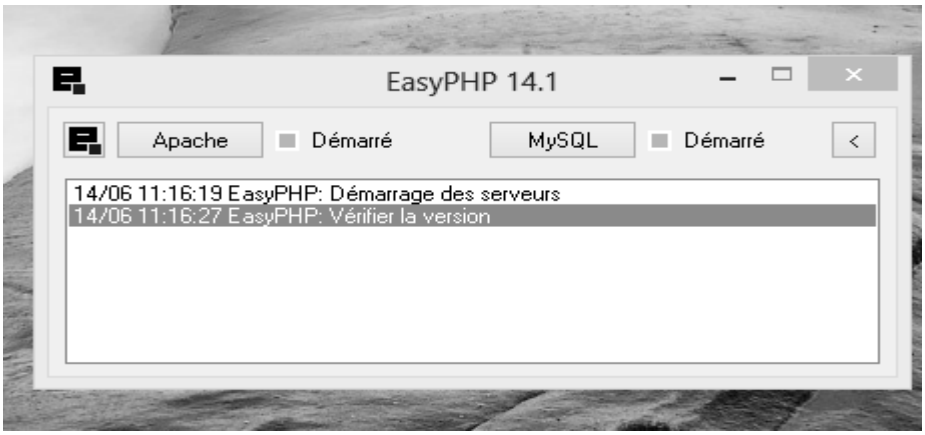


Fig.IV. 5: Partie configuration

II.5 Sublime Text 3 :

Sublime Text est un éditeur de texte générique codé en C++ et Python, disponible sur Windows, Mac et Linux. Sublime intègre la plupart des fonctionnalités de base d'un éditeur de texte, dont la coloration syntaxique personnalisable, l'auto complétion, un système de plugins

Fig.IV. 6: Sublime Text 3

II.6 HTML :

L'***HypertextMarkupLanguage***, généralement abrégé **HTML**, est le format de données conçu pour représenter les pages web. C'est un langage de balisage permettant d'écrire de l'hypertexte, d'où son nom. HTML permet également de structurer sémantiquement et logiquement et de mettre en forme le contenu des pages, d'inclure des ressources multimédias dont des images, des formulaires de saisie, et des programmes informatiques.[28]

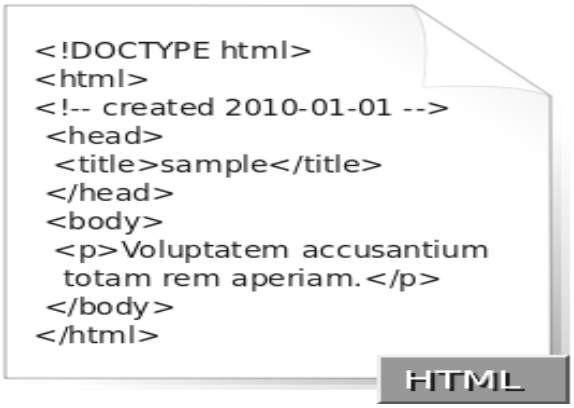


Fig.IV. 7:HTML

II.7 CSS :

CSS appelées en anglais *Cascading Style Sheets*, forment un langage informatique qui décrit la présentation des documents HTML et XML. Les standards définissant CSS sont publiés par le World Wide Web Consortium (W3C).

II.8 Entreprise Architect :

C'est un logiciel de modélisation et de conception UML, édité par la société australienne Sparx Systems. Couvrant, par ses fonctionnalités, l'ensemble des étapes du cycle de conception d'application, il est l'un des logiciels de conception et de modélisation les plus reconnus.

Fig.IV. 8: Entreprise Architect

III. La réalisation du projet :

III.1 L'architecture de notre site :

Ceci représente l'interface générale de notre site web :

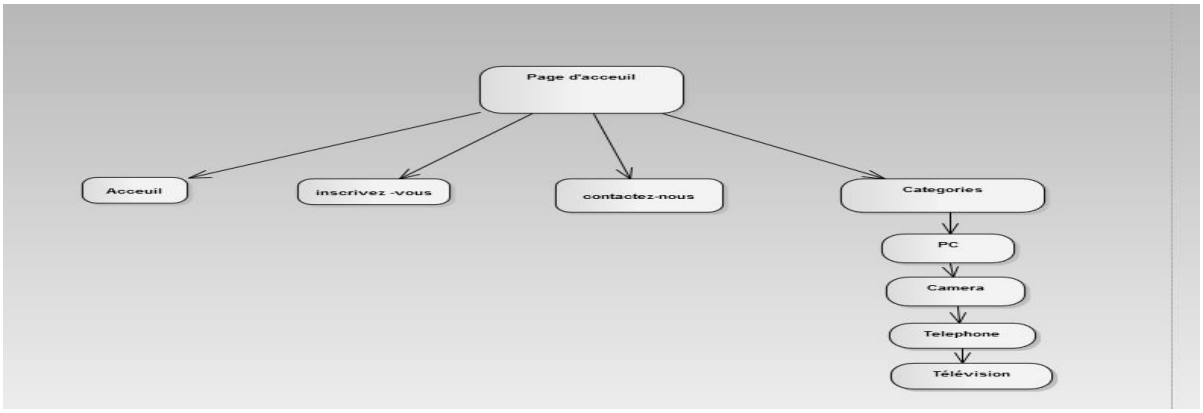


Fig.IV. 9:L'architecture du site

III.2 Le diagramme d'action d'un client :

Ce diagramme vous présente les différentes actions exigées par un acteur client sur notre site web.

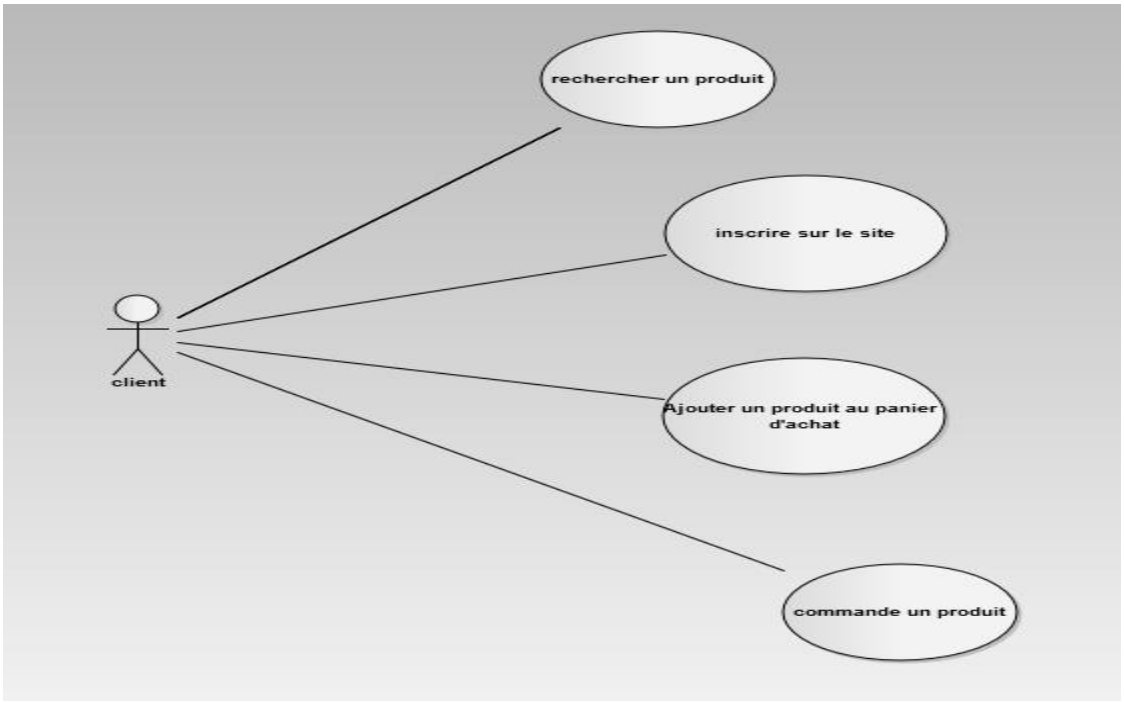


Fig.IV. 10 : Le diagramme d'action d'un client

III.3 Le diagramme d'action d'un client

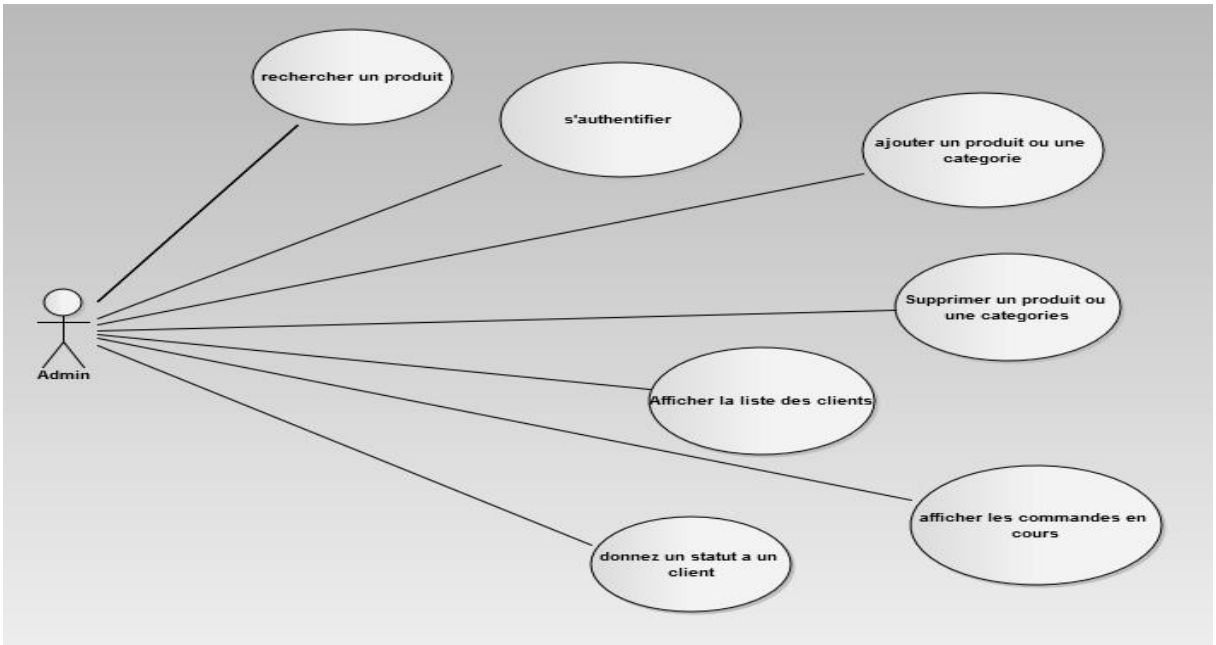


Fig.IV. 11 : Le diagramme d'action d'un Admin

III.4 Création de la base de données :

A partir de l'outil Easyphp on a créé une base de données en utilisant l'interface phpMyadmin. La base de notre site appelée **mabase** est sous la forme suivant :

III.4.1 Tables utilisées :

- Les tables qu'on a besoin au cours de la réalisation du ce projet :

Table	Lignes	Type	Taille
categories	4	InnoDB	16 Kio
client	0	InnoDB	16 Kio
commande	0	InnoDB	16 Kio
panier	0	InnoDB	16 Kio
produit	8	InnoDB	16 Kio
user	0	InnoDB	16 Kio
6 tables	12	--	96 Kio

Tableau.IV. 1: Tables utilisées

- L'affichage de tables par le phpMyadmin :

Fig.IV. 12: Affichage des tables par le phpMyadmin

III.4.2 Attributs :

Pour chacun de tables mentionner ci-dessus on va donner les attributs qui lui correspondants :

1. ***Table Catégories :***

categories

Colonne	Type
id_cat	int(11)
libelle_cat	varchar(100)

Tableau.IV. 2: Table Catégories

2. ***Table Produit :***

produit

Colonne	Type
id	int(11)
libelle	varchar(100)
prix	varchar(100)
description	text
stock	int(11)
id_cat	int(11)
id_marque	int(11)
images	mediumtext
selectionne	int(10)

Tableau.IV. 3 :Table Produit

3. *Table Client:*

client

Colonne	Type
id	int(11)
nom	int(11)
prenom	int(11)
adresse	varchar(100)
email	int(11)
telephone	int(11)
mot_passe	int(11)
code_postal	varchar(200)

Tableau.IV. 4:Table Client

4. *Table User:*

user

Colonne	Type
id_users	int(11)
username	varchar(100)
password	varchar(100)

Tableau.IV. 5 :Table User

5. *Table Commande:*

commande

Colonne	Type
id_commande	int(11)
id_client	int(11)
id_produit	int(11)
quantite	int(11)

Tableau.IV. 6 :Table :Commande

6. *Table Panier:*

panier

Colonne	Type
id_panier	int(11)
Prix_unitaire	int(11)
prix_total	int(11)
Prix final	int(11)

Tableau.IV. 7 :Table Panier

III.4.3 Modèle Conceptuelle de la base de données :

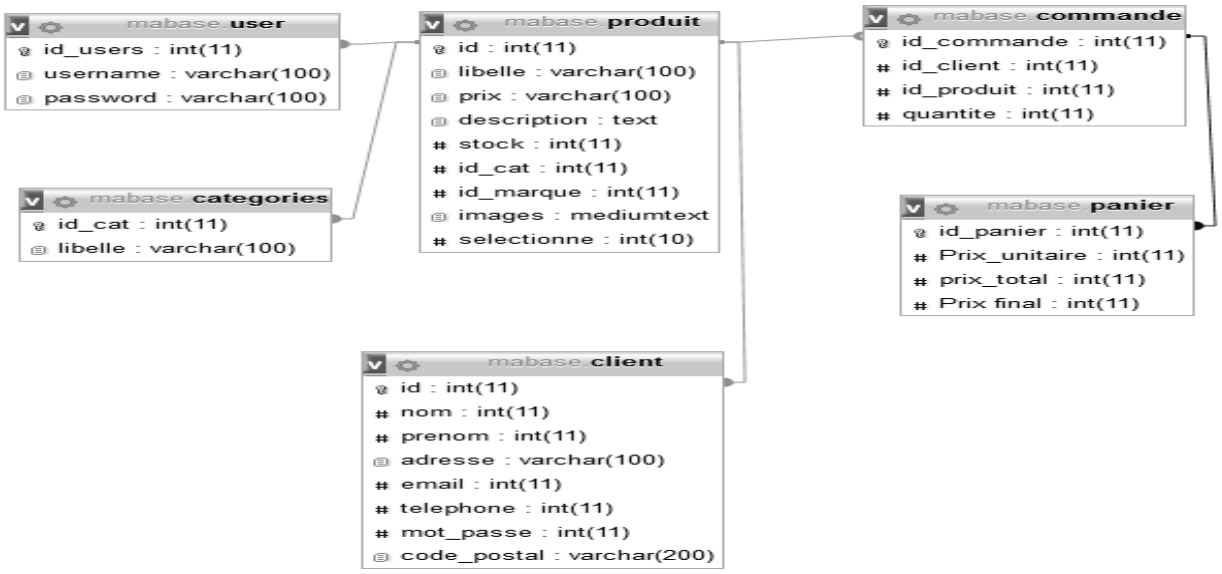


Fig.IV. 13 : Modèle Conceptuelle de la base de données

III.5 Les Scriptes :

Pour une meilleure organisation et documentation du projet, nous avons créé plusieurs répertoires : les scriptes spécifiques aux web site administration dans un répertoire Admin ; et ceux spécifique aux clients dans Client ; les fichiers commun entre les deux dans un répertoire Common et enfin le répertoire include qui contient les scriptes de configuration.

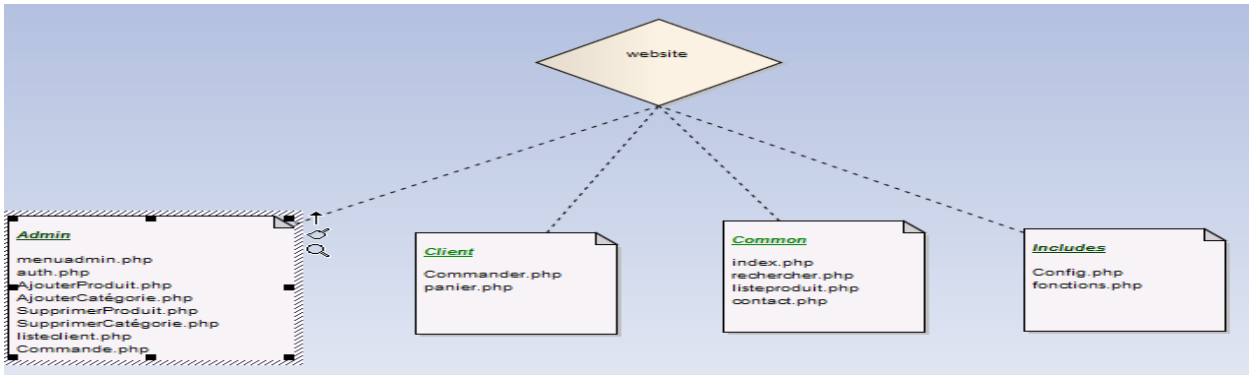


Fig.IV. 14: Organisation des Scriptes

Les Scriptes	Fonctions
menuadmin.php	Affiche le menu d'administrateur
Auth.php	Faire l'authentification de l'admin
AjouterProduit.php	Affiche un formulaire permet d'ajouter des produits dans la base de données.
AjouterCatégorie.php	Affiche un formulaire permet d'ajouter des catégories dans la base de données.
SupprimerProduit.php	Permet de supprimer des produits de la base de données.
SupprimerCatégories.php	Permet de supprimer des catégories de la base de données.
Listeclient.php	Autorise à l'Admin de consulter les clients qui ont effectuées une commande.
List commande.php	Affiche la commande effectuée par un client.
commande.php	Affiche un formulaire au client pour pu entrer ses cordonnées en fin de finalise la commande.
Panier.php	Affiche les produits ajoutés au panier
addp.php	Ajouter au panier.
produit.php	Affiche les produits en stock.
inscription.php	Affiche un formulaire permet au client d'inscrir.
Conexion.php	Assure la connexion avec la base de données.
Index.php	L'interface (1er page s'affiche)

Categories.php	Affiche les catégories.
SuppPan.php	Pour la suppression des produits dans l panier
Entete.php	L'entête du page index
Validation.php	Affiche un message de la validation de la commande
Style.css	Pour le style général du site web

Tableau. IV. 8: Les scriptes

III.6 Les Interfaces graphiques :

III.6.1 Page d'Accueil :

Fig.IV. 15:Page d'Accueil

III.6.2 Menu d'Admin :

Fig.IV. 16: Menu d'Admin

III.6.3 Panier d'achat:

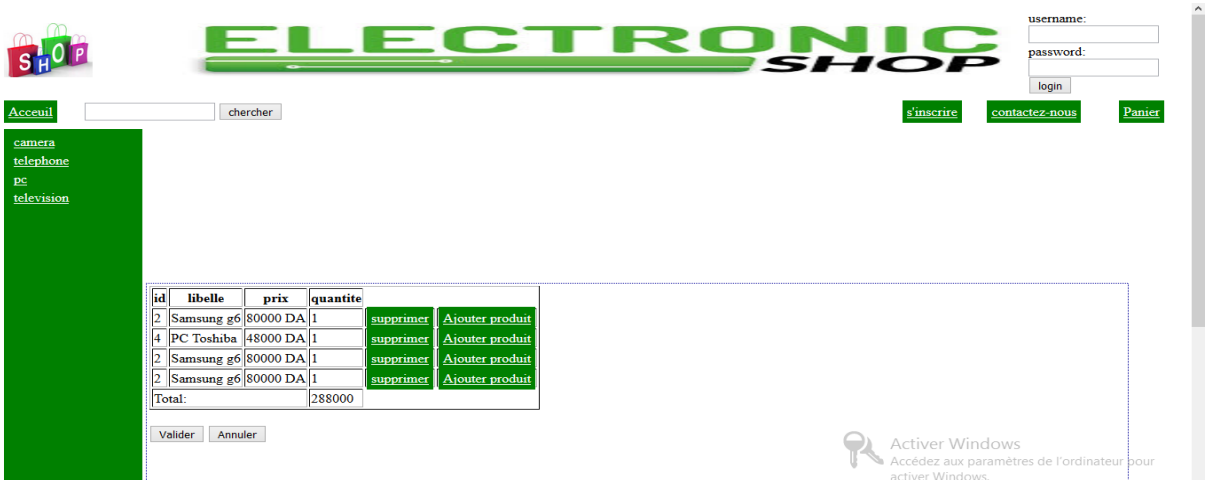


Fig.IV. 17 : Panier d'achat

III.6.4 Formulaire de paiement:

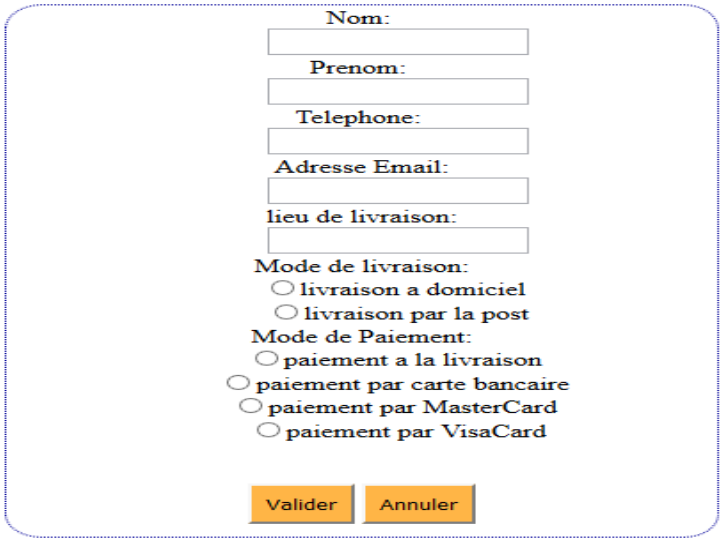


Fig. IV. 18: Formulaire de paiement

III.6.5 Un message de validation de la commande:

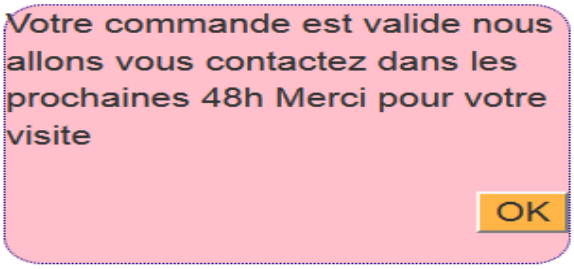


Fig.IV. 19 : message de validation de la commande

III.6.6L'icône contactez-nous:

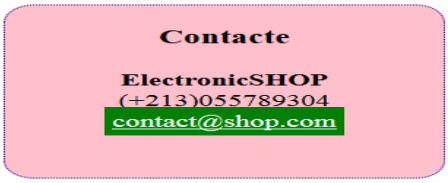


Fig.IV. 20:L'icône contactez-nous

III.6.7 Formulaire d'inscription:

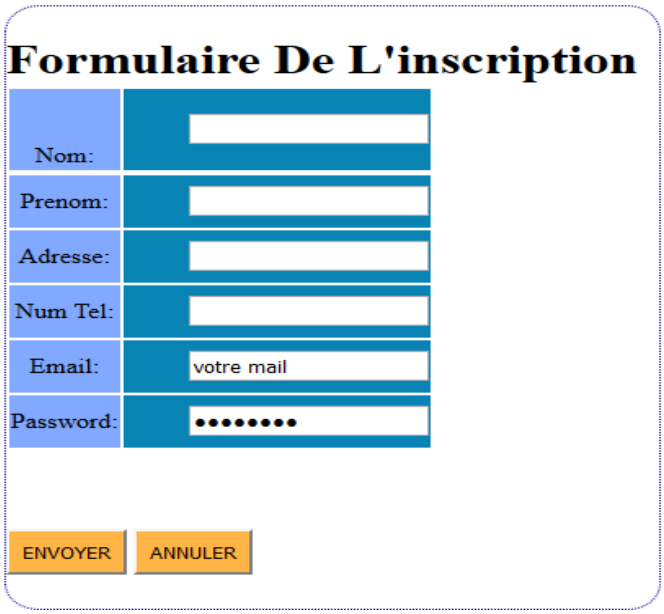


Fig. IV. 21:Formulaire d'inscription

IV. Conclusion :

La partie de réalisation détermine une idée plus claire sur les taches qui sont réalisé dans ce Site web par la présentation des interfaces graphiques. Enfin avec ce chapitre on a terminé la phase de développement de ce site.

Conclusion générale

Conclusion générale

Grâce au e-commerce le consommateur peut aujourd'hui rechercher n'importe quel produit ou service parmi une multitude d'offres, sans se déplacer, et surtout comparer les tarifs sur le plan national ou international. Ce dernier est donc devenu beaucoup plus actif qu'auparavant dans son acte d'achat. Néanmoins, une réticence persiste quant à la sécurité du paiement en ligne et dans l'intangibilité du produit.

Ensuite, on peut dit que ce domaine est un secteur en pleine croissance, depuis de nombreuses années. Même en cas de crises le secteur connaît une croissance, certes faible. Et surtout, pour le futur, on ne voit pas encore venir de saturation du marché, le nombre de sites ne cesse d'augmenter, et la demande ne baisse pas. Pour moi étudiante en informatique industrielle, il représente un marché plein de perspective comme on peut le voir dans les emplois et qui est d'ailleurs à la base de formations spéciales en informatique.

Finalement, on a traité toutes les phases nécessaires à la réalisation de cette application, et dans cette phase on a appris à mieux manipuler les langages PHP, HTML et CSS ; j'ai approfondi mes connaissances sur le langage SQL avec le MySQL

Bibliographie

Bibliographie

[1] Guy Pujolle, *Les reseaux*, Edition 2008. ÉDITIONS EYROLLES,.
[2] Claude SERVIN, *Réseaux & télécoms*, 2ème édition. paris -France, 2009.
[3] « Réseau informatique1 — Wikipédia 4 3 23 39.html ». 3/3/2017 à 22H15.
[4] Danièle Dromard et Dominique SERET, *Architecture des réseaux*. 2009 Pearson Education France.
[5] P. Sicard, « Cours Réseaux ». 21-janv-2004.
[6] Claud Servin, *Réseau et Télécom*. 2009 .
[7] « reseau local, local area network, LAN, JO journal officiel marches publics definition.html ». .
[8] Jean-Luc Dekeyser, « Introduction aux réseaux informatiques ». 27-janv-2009.
[9] CONSERVATOIRE NATIONNAL DES ARTS ET METIERS, *RESEAUX*, vol. 1. .
[10] PUJOLLE (Guy), *Les réseaux (5è édition*, 5éme édition. Groupe Eyrolles, 2006.
[11] Jean-François PILLOU, « Introduction à la sécurité informatique ». sept-2015.
[12] Bernard Cousin, « Sécurité des réseaux informatiques ». Université de Rennes 1.
[13] Laurent Bloch Christophe Wolfhugel, *Sécurité informatique Principes et méthodes*. .
[14] AMAN VLADIMIR GNUAN, « CONCEVOIR LA SECURITE INFORMATIQUE EN ENTREPRISE ». .
[15] « Laurent Bloch, Christophe Wolfhugel. Sécurité Informatiques: principes et méthodes ». .
[16] *Du virus à l'antivirus, guide d'analyse. LUDWIG. Dunod. ISBN 2-10-003467-7 (05/1997), 720 p. (398 FF). .*
[17] *Lagrange X., Godlewski P., Sami Tabbane S. (2000), Réseaux GSM-DCS, 5e édition revue et augmentée, éditions Hermès Sciences Publications*. .
[18] Pierre-Alain Fouque, Equipe de Cryptographie, et Ecole normale supérieure, « Algorithmes de chiffrement symétrique par bloc (DES et AES) ». .
[19] *Basic methods of cryptography. LUBBE. Cambridge UniversityPress. ISBN 0-521-55559-0 (03/1998), 243 p. (230 FF). .*
[20] *William Stallings. Cryptography and Network Security : Principles and Practice, 3rd ed. Prentice Hall, 2003. .*
[21] « Introduction à la sécurité des réseaux - Saadbouh O Cheikh El Mehdi- ISCAE-2012-2013 ». .
[22] *Sécurité opérationnelle: Conseils pratiques pour sécuriser le SI (Solutions d'entreprise) Alexandre Fernandez-Toro (French Edition). .*
[23] Adel RAISSI, « Conception et développement d'un site web de e-commerce pour le compte de LSAT_Nokia ». 2013.
[24] *G. & O. Gardarin, «Le Client-Serveur», Eyrolles Eds., 1996. .*
[25] *D. Garlan, R. Allen & J. Ockerbloom, «Exploiting Style in Architectural Design Environment », Proc. of the ACM SIGSOFT'94, New Orleans, LA, December 1994. .*
[26] *D. Garlan& M. Shaw, «An Introduction to Software Architecture», Advances in Software Engineering and Knowledge Engineering», Vol. 1, V. Ambriola and G. TotoraEds, World Scientific PublishingCompany, New Jersey, 1993, pp. 1-39. .*
[27] « M2 SRIV - Applications Systèmes et Réseaux Olivier GLÜCK Université LYON 1/Département Informatique Olivier.Gluck@univ-lyon1.fr ». .
[28] Alexandre Bacco, *Développez efficacement votre site web avec le framework Symfony2*. .

[29] Mossaab BAGDOURI, « Réalisation d'un site web dynamique E-Commerce » , mémoire master 2 , Université Abou Bakr Belkaid– Tlemcen.2013.

Résumé :

Ce travail est présenté dans le cadre d'une mémoire d'obtenir le diplôme de master est de développer une application e-commerce avec le langage php, afin de s'adapter à la programmation avec les langages HTML, CSS et la base de données MySQL.

Mots clé:

E-commerce ; PHP ; HTML ; MYSQL ; base de données ; site web .

Abstract :

This workis presented as part of a thesis to obtain the masters degree is to develop an e-commerce application with the PHP language, in order to adapt to programming with HTML, CSS and database languages

Keywords:

E-commerce ; PHP ; HTML ; MYSQL ;database, ;website.

خلاصة:

هذا العمل يدخل ضمن مذكرة الماستر لتطوير تطبيق تجاري مع لغة PHP بالتكيف مع البرمجة للغة HTML, CSS وقاعدة البيانات MySQL.

الكلمات المفتاحية:

الموقع التجاري، MYSQL ; HTML ; PHP، قاعدة البيانات، موقع إلكتروني.