الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université Akli Mohand Oulhadj - Bouira -
Tasdawit Akli Muḥend Ulḥag - Tubirett -
Faculté des Sciences et des Sciences Appliquées

وزارة التعليم العالي والبحث العلمي
جامعة أكلي محند أولحاج
-البويرة-
كلية العلوم والعلوم التطبيقية

Référence : ...../MM/2021

المرجع :...../م م/ 2021

Mémoire de Master

Présenté au

Département : Génie Électrique
Domaine : Sciences et Technologies
Filière : Télécommunications
Spécialité : Systèmes des Télécommunications

Réalisé par :

CHABANE CHAOUCHE NADJET

Et

TAMOURT YACINE

Thème

Conception Et Déploiement D'un Réseau Informatique Pour La Transmission Des Données

Soutenu le: **30/10/2021**

Devant la commission composée de :

Mr :	SMAIL Haroun	Prof.	Univ. Bouira	Président
	ROUAM Rania		Univ. Bouira	Rapporteur
	NOURIN Mourad	M.C.B	Univ. Bouira	Examinateur

Année Universitaire: 2020-2021

Dédicaces 1

Je dédie ce modeste travail à :

A mon très cher père ***OULAID*** *et ma très chère mère* ***CHERIFA*** *qui n'ont pas cessé de m'encourager et de se sacrifier pour que je puisse franchir tout obstacle durant toutes mes années d'étude que Dieu me les garde en très bonne santé ; Aucune dédicace ne pourra compenser les sacrifices de mes parents.*

A mon très cher frère ***Hamouche*** *, et mes chères sœurs* ***Faiza*** *et* ***Kahina*** *.*

Tous mes ami(e)s ainsi qu'à tous ce qui me sont chers.

Et à toute personne m'ayant fait part de son savoir.

TAMOURT Yacine

Dédicaces 2

Je dédie ce modeste travail à :

A ma très chère maman **« *Malika* »** *et a mon père* **« *Kamel* »** *qui m'ont soutenu et encouragé durant toute ma vie.*

Qu'elle trouve ici le témoignage de ma profonde reconnaissance. Merci pour tout, mes parents sans je serais pas ici aujourd'hui. Je t'aime

A mes frères et sœurs **: *Asma, Abderrahmane, Abderraouf, Oussama*.**

A mon oncle **« *Nabil* »** *qui m'as toujours soutenu et encouragé.*

A mon binôme ***Yacine*** *ainsi que sa famille* ***TAMOURT****.*

CHABANE CHAOUCHE Nadjet.

Remerciements

Nous remercions Dieu le tout puissant de nous avoir accordé la santé, le courage et la volonté d'arriver au terme de ce travail.

Ce travail a été effectué au sein du Département des Sciences et sciences appliquées de l'Université de Bouira.

Je tiens à remercier, en premier lieu, Mme.ROUAM Rania, Directrice de ce mémoire. pour ses conseils et son aide.

Nous remercions également tous les membres du jury pour l'intérêt qu'ils ont porté à notre travail.

Nous tenons à remercier tous nous collègues d'étude, particulièrement notre promotion Enfin, nous tenons aussi à exprimer notre profonde gratitude à toute personne de près ou de loin, ceux qui nous ont encouragés.

Enfin, on associe à ces remerciements tous ceux qui ont contribué à réaliser ce travail.

Résumé

Le domaine des réseaux informatiques est un domaine trop vaste, qui évolue trop vite. L'administration réseau rassemble les services Internet (Telnet, ftp, mail,...) pour tout le réseau qu'elle protège. Ceci nécessite de créer des comptes dédiés à ces services, ces comptes sont accessibles par un certain nombre de personnes du réseau. Nous avons réalisé un projet de fin d'étude visant ce domaine. On s'est proposé comme objectif ; la sécurité et la cryptographie des données en faisant une implémentation d'un algorithme de chiffrement par bloc <blowfish> dans une architecture client/serveur pour but d'assurer son efficacité, rapidité et fiabilité dans la transmission des données.

Mots clés : : clés, sécurité, cryptographie, blowfish.

Table des Matières

Chapitre 2: Sécurité et cryptographie des données

Liste des Figures

Liste des Tableaux

Listes des Acronymes

Acronymes

BGP	Border Gateway Protocol
EGP	Exterior Gateway Protocol
IS-IS	Système Intermédiaires A System Intermediaries
LAN	Local Area Network En Français Réseau Local
MAN	Metropolitan Area Network
WAN	Wide Area Network (Réseau Étendu)
CSMA	Carrier Sense Multiple Access
CD	Compact Disc
NIC	Network Interface Card
OSI	Open System Interconnexion
WPAN	Wireless Personal Area Network
WLAN	Wireless Local Area Network
ETSI	European Telecommunications Standards Institute
WMAN	Wireless Metropolitan Area Network
BLR	Boucle Locale Radio
WWAN	Wireless Wide Area Network
GSM	Global System For Mobile Communication (Groupe Spécial Mobile)
GPRS	General Packet Radio Service
UMTS	Universal Mobile Telecommunication System
WIFI	Wireless Fidelity
IP	Internet Protocol
TCP	Transmission Control Protocol
FDDI	Fiber Distributed Data Interface
NAT	Network Address Translation
DES	Data Encryption Standard
DNS	Domain Name Server
CCM	Cisco Call Manager
DHCP	Dynamic Host Configuration Protocol

Introduction Générale

La sécurité des réseaux depuis quelques années, a vu son importance s'accroître au point de devenir une priorité dans de nombreuses sociétés. Des outils automatisés de plus en plus complexes, des virus à la réplication foudroyante attaquent les réseaux et menacent en permanence intégrité des systèmes d'information.

Depuis les temps anciens, les êtres humains ont été préoccupés par diverses formes de problèmes de sécurité. L'émergence de l'informatique et des télécommunications a augmenté la complexité des problèmes et des solutions de sécurité, et introduit de nouveaux concepts tels que les virus informatiques, les accès non autorisés, les informations méconnaissables et fausses... Afin de faire face à ces différentes menaces, un système de sécurité suffisant et puissant doit être mis en place pour répondre aux exigences et aux aspirations d'une politique de sécurité.

La construction d'un système de sécurité nécessite presque inévitablement des concepts cryptographiques impliquant la cryptographie et la cryptanalyse.

La cryptographie fournit un ensemble de technologies pour assurer confidentialité, l'authentification, l'intégrité des données et la non-répudiation de la source de données.

Nous distinguons deux grandes catégories de techniques cryptographiques: celles à chiffrement symétrique ou à clé secrète et celles à chiffrement asymétrique ou à clé publique.

Les algorithmes cryptographiques symétriques sont des fonctions de deux paramètres: l'algorithme et la clé; la sécurité de tout le crypto-système (cryptographie) réside dans la clé, l'algorithme peut être public.

Dans notre travail nous avons étudié les vulnérabilités qui mettent en péril la sécurité des réseaux et nous avons proposé des mesures de protection jugées importantes dont la plus essentielle est la cryptographie dans la transmission des données.

Nous avons structuré notre mémoire en trois chapitres comme suit :

Le premier chapitre comporte un ensemble de notions et de généralités sur les réseaux informatique.

Le deuxième chapitre amène un aperçu des techniques de cryptographie classique et moderne et de ses deux types à savoir cryptographies symétrique et asymétrique tout en définissant les algorithmes de chiffrement les plus connus.

Dans le troisième chapitre nous présentons le simulateur Packet Tracer et le réseau crée sur cet outil selon l'architecture client/serveur, ensuite nous décrivons le fonctionnement ainsi que la programmation de l'algorithme de sécurité sous Java, on fini avec l'implémentation de notre

algorithme de sécurité sur l’architecture client/serveur dans le but de la sécurité et la cryptographie de l’information pendant la transmission de données.

Chapitre 1:

Généralités sur les réseaux informatiques

1. Introduction :

Le réseau est devenu une ressource incontournable au profit d'une organisation, d'une entreprise, d'une université,...

Un réseau définit un ensemble d'entités (*objet, personne, etc.)* Interconnectées, il permet donc une circulation physique ou immatérielle entre chacune de ces entités selon des règles bien définies.

Dans le cas d'un réseau informatique, tous ces réseaux sont interconnectés au moyen de lignes physiques qui échangent des informations sous forme de données numériques (*valeurs binaires, c.-à-d. codées sous forment de signaux pouvant prendre deux valeurs 0 et 1*).

Il n'y a pas un seul type de réseau, cela est dû à l'hétérogénéité des supports physiques tant au niveau du transfert des données (*circulation des données sous forme impulsions électriques, de lumières ou d'onde électromagnétiques*) qu'au niveau de type du support (*câble coaxial, paires torsadées, fibres optique, etc.).*

2. les différents types des réseaux informatiques:

On peut distinguer déférent types selon plusieurs critères tel que (*la taille de réseau, sa vitesse de transfert de données et aussi leur entendu*) : [1, 6]

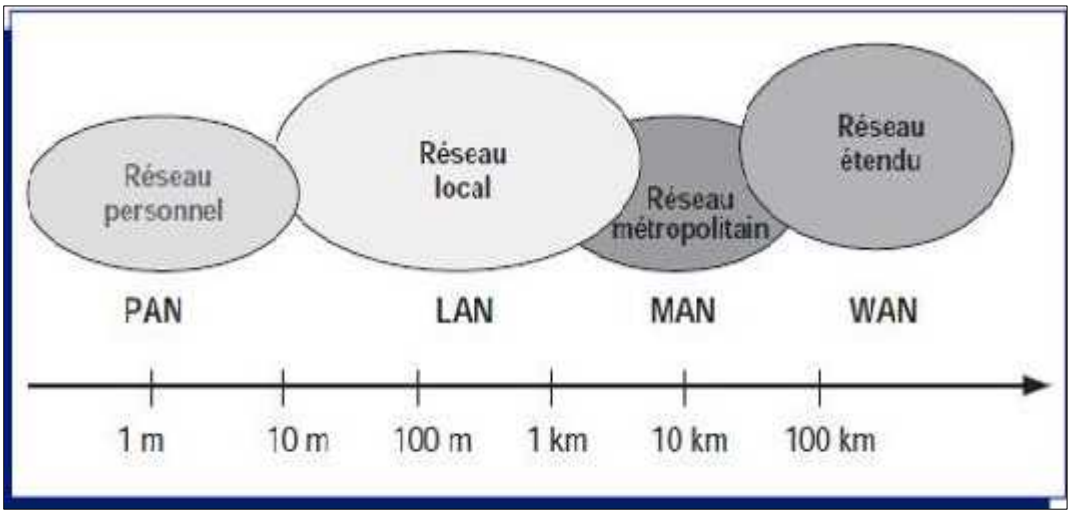


Figure 1.1 : schéma des différents types des réseaux informatiques.[3]

2.1. Les LAN (Local Area Network en français réseau local) :

C'est un ensemble d'ordinateur et équipements informatiques relies les un aux autres dans un même bâtiment, site ou dans des sites déférents ayant une aire géographiquement proche ne dépassant pas 10 km.

Les taux de transfert de données du réseau local vont de 10 Mbit/s (*pour un réseau Ethernet par exemple*) à 1Gbit/s (*en FDDI ou Gigabit Ethernet par exemple).*la taille du réseau peut atteindre jusqu'a 100 voire 1000 utilisateurs [1,6].

2.2. Les MAN (Metropolitan Area Network):

Il s'agit d'une connexion entre les réseaux locaux(*LAN*) géographiquement proches (la distance entre les sites ne dépasse pas 200km) il peut utiliser des chemins de réseau publics (*services de télécommunication, radiocommunication, câble téléphonique etc.)* ou privés pour sécuriser le lien entre deux ou plusieurs sites Internet, lien avec plusieurs utilisateurs de lieux géographiques partageant des ressources via le réseau comme s'ils étaient un réseau local.

2.3. Les WAN (Wide Area Network ou réseau étendu):

C'est la connexion entre plusieurs LAN sur de longues distances, elle connecte un nombre déterminé d'ordinateurs à travers un pays, un continent ou même la planète entière, c'est rendu possible par ses propres réseaux et/ou publics.

Le plus connu des WAN est internet [1,6].

3. Architecteur des réseaux :

Les réseaux sont structure de point de vue fonctionnel en deux catégories :

3.1. Réseaux poste à poste (peer to peer):

Chaque machine du réseau est en même temps un serveur client, et les données ne sont pas centralisées, son principal facteur est le faible coût des matériaux.si le réseau comporter plusieurs machines (*>10 poste*) alors il devient impossible à gérer [2,6,7].

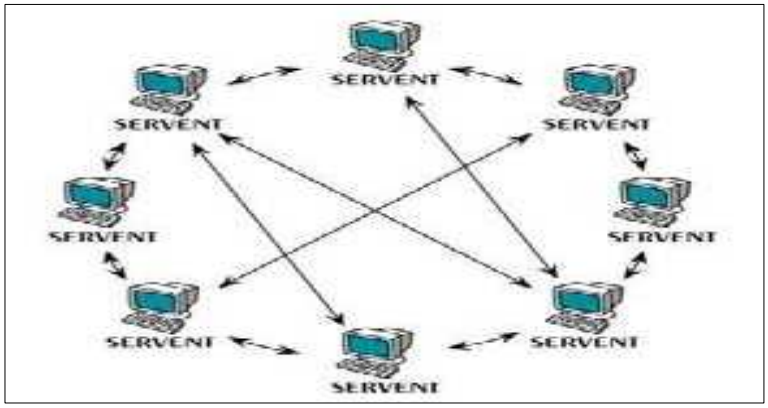


Figure 1.1 : Schéma d'un réseau poste à poste.[2]

3.2. Le réseau server/client:

C'est un réseau peer-to-peer mais cette fois plus forte. Il est plus facile de gérer ce type de réseau car les données sont centralisées par le serveur permettant un fonctionnement précis et une gestion aisée des réseaux constitués de plusieurs stations [2,6,7].

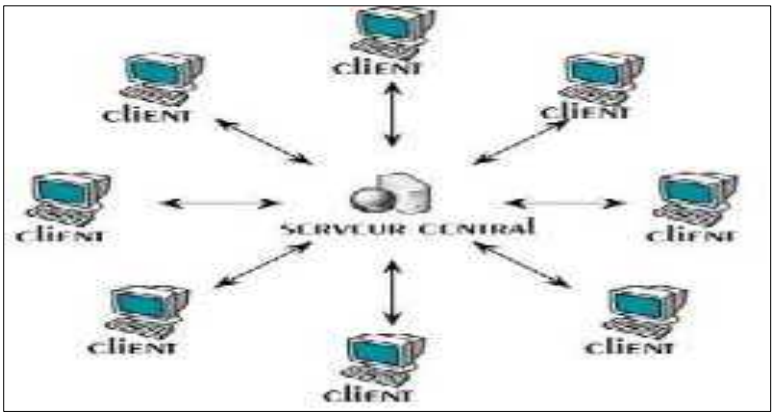


Figure 1. 3 : Schéma d'un réseau serveur/client.[2]

4. Topologie de réseaux :

Il existe 2 catégories de topologie :

4.1. Topologies physiques :

La topologie physique est le dépôt d'un réseau qui ne précise ni le mode de connexion ou le type d'équipement voir même l'adresse [3,4].

Il y'a trois types :

4.1.1. Topologie en bus :

Dans ce type de topologie, tous les périphériques sont rattachés à un segment central où circulent les informations sur l'ensemble du bus, un "bouchon" qui permet d'effacer définitivement les suivants à l'arrivée pour que l'autre station puisse transmettre.

Les signaux d'un réseau de bus sans imitateurs circulent sans fin, ce qu'on appelle le robant de signal.

Cette topologie se caractérise par un certain nombre d'avantages dont: faible coût, facilité d'installation la panne d'une station n'affecte pas le reste du réseau, d'autre part la panne du bus provoque une inutilisation.

Notons aussi que le signal n'est jamais régénéré, ce qui va limiter la longueur des câbles, c'est la technologie Ethernet 10 base 2 [3,4].

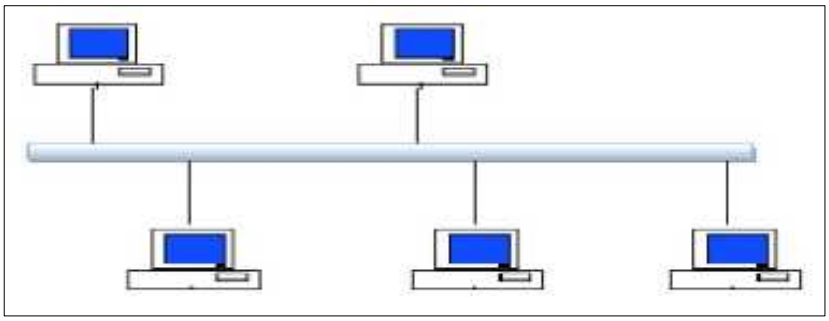


Figure 1.4: topologie en bus.[3]

4.1.2. Topologie en étoile :

C'est la topologie la plus courante, chaque appareil dans une unité centrale, comme un hub, le même câble réseau ne peut connecter les deux qu'en cas de problème, il ne touchera jamais plus de deux appareils, donc ce n'est pas pertinents pour l'ensemble du réseau.

Ce type de réseau est facile à configurer et à surveiller, les appareils transmettent des données qui à leur tour transmettent les informations au segment de réseau où l'appareil cible peut les recevoir [3,4].

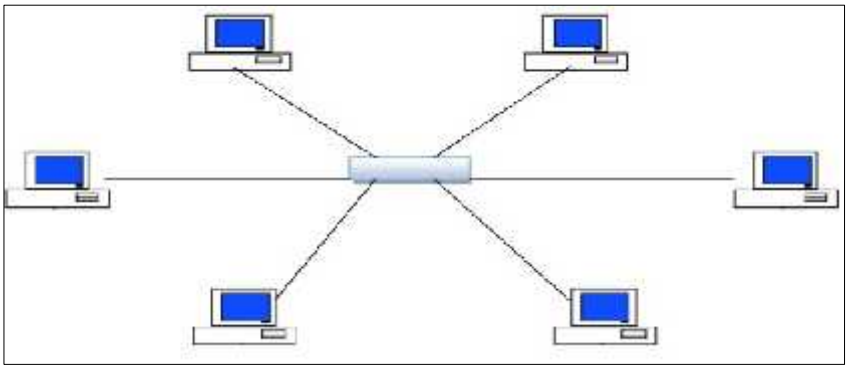


Figure 1. 5: topologie en étoile.[3]

4.1.3. Topologie en anneau :

Dans cette topologie chaque périphérique est relié aux deux périphériques les proches, et l'ensemble du réseau forme un cercle dont les données sont transmises auteur de l'anneau, dans une seul direction chaque station de travail accepté et répond aux paquets qui lui sont adressés, puis les fait suivre a la prochaine station de l'anneau [3,4].

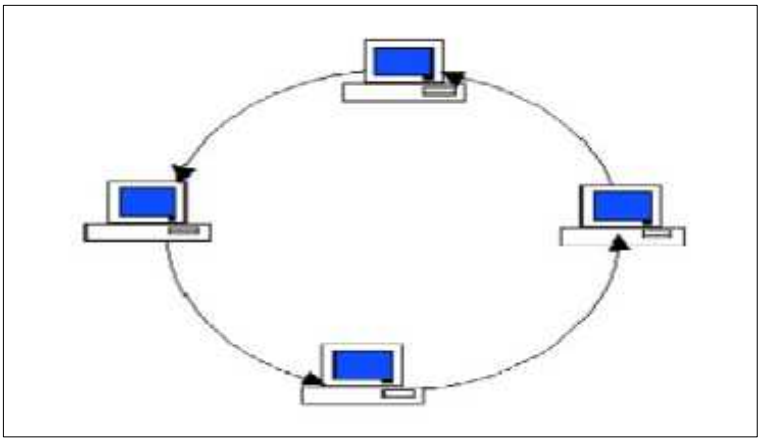


Figure 1.6 : topologie en anneau.[3]

4.2. Topologies logiques :

La topologie logique d'un réseau décrit la manière par laquelle les données sont mises en trames et comment les impulsions électrique sont envoyées sur le support physique du réseau [3,4].

Ethernet et Token Ring sont les deux systèmes de transport réseau (topologie logique) les plus courants :

4.2.1. Topologie Ethernet :

Dans ce réseau, la communication se fait en utilisant un protocole appelé CSMA/CD, cela permet de surveiller très bien les données transmises pour éviter toute collision.

4.2.2. Topologie Token ring :

Il est basé sur une topologie physique dans l'anneau (ring), en utilisant la méthode d'accès au jeton (*token*). Dans cette technologie, la station avec le jeton a le droit de transmettre.

4.2.3. Topologie FDDI :

Se compose de deux tours : un principal et un autre mineur, ce dernier tour est utilisé pour compenser les erreurs dans le tour principal ; FDDI utilise un token ring qui est utilisé pour détecter et corriger les erreurs. Ce qui signifie que si une MAU échoue, le réseau continuera à fonctionner.

5. Principaux élément d'un réseau :

L'interconnexion est:

Locale: lorsque les réseaux sont géographiquement sur le même site .dans le cas d'un équipement standard (Répéteur, routeur …etc.) fit à réaliser la liaison physiquement.

Concerne des réseaux distants où Il est nécessaire de relier ces réseaux par une liaison téléphonique (modems, etc..) [7].

5.1. La carte réseau :

Pour que l'ordinateur soit connecté au réseau, il doit disposer d'une carte réseau NIC (Network Interface Card) ce dernier est l'interface entre l'ordinateur et le support. Il dispose de deux voyants lumineux :

LED verte signifie l'alimentation de la carte.

LED orange signifie l'activité du réseau.

Figure 1.7 : Carte réseau.[7]

5.2. Le concentrateur (*Hub*) :

Le concentrateur est un périphérique qui opère au niveau 1 du modèle OSI (*couche physique*), son unique but est de récupérer les données binaires provenant d'un port et de les diffuser sur l'ensemble des ports.

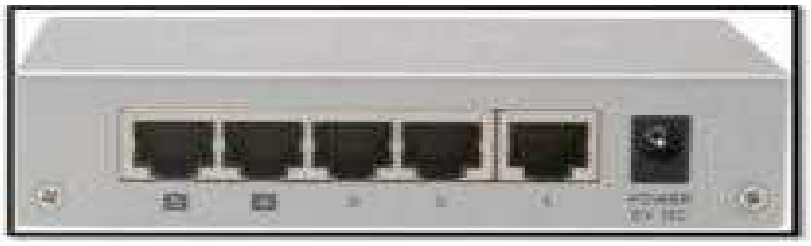


Figure 1.8 : un concentrateur.[7]

On distingue deux catégories de hubs :

Concentrateur Actif : ils sont alimentés électriquement, permettant de générer le signal sur les différents ports.

Concentrateur passif : diffuser le signal à tous les hôtes ans amplification

5.3. Le commutateur (*Switch)* :

Un commutateur est un système qui garantit l'interconnexion des stations ou des segments d'un LAN en leur allouant l'intégralité de la bande passante, contrairement a celui du concentrateur qui la partage.

En conséquence, des commutateurs ont été introduits pour augmenter la bande passante globale du réseau d'entreprise et en tant qu'évolution des concentrateurs Ethernet (ou HUB).

Figure 1.9 : un commutateur.[7]

5.4. Le pont (*Bridge)* :

Le pont est un équipement qui permet de relier deux réseaux de technologies de liaison déférents (*Ethernet, Token ring, ..).* Son rôle essentiel est de relier les réseaux en filtrant les trames selon les adresses physiques des stations d'émission et de destination, il permet de réduire la charge d'un réseau local en le divisant en deux sous- réseaux.

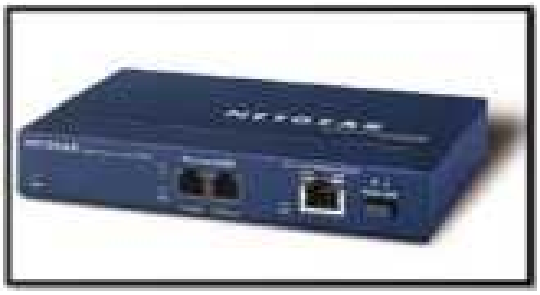


Figure 1.10 : un pont.[7]

5.5. Le routeur (*Router*) :

C'est l'élément intermédiaires dans un réseau informatique, assurer le routage des paquets en choisissant un chemin selon l'une des règles de formation de la table de routage. Il dispose des ports souvent RJ45 pour la connexion avec un Switch ou un PC, il peut avoir des antennes pour le sans fil.

Figure 1.11 : un retour.[7]

5.6. Le répéteur (*Repeater*) :

C'est un équipement simple qui opère au niveau 1 du modèle OSI et qui ne nécessite aucune administration, qui permet de régénérer le signal entre deux nœud du réseau, afin d'étendre la distance du câblage.

Figure 1.12 : un retour.[7]

On distingue deux catégories du répéteur :

Stand Alone : les débits sur les deux câbles doivent être les même.

Store And Forward : avec mémoire, il support les vitesses différents sur les différents tronçons.

5.7. La passerelle (Gateway) :

Sont des appareils qui permettent l'interconnections des architectures de réseaux différentes. Par conséquent, ils assurent la conversion de tous les protocoles, à travers les 7 couches du modèle OSI.

L'objectif est d'avoir une architecture de réseau évolutive, qui tend à connecter les réseaux à l'aide de routeurs, ce qui fait baisser leurs prix.

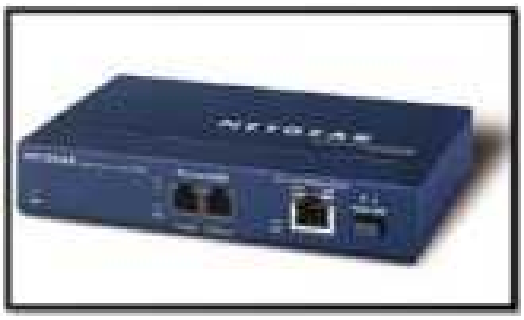


Figure 1.13 : une passerelle.[7]

5.8. Le modem :

C'est un équipement utilisé pour relier un réseau téléphonique à un autre informatique. Souvent pour transmettre des données informatiques sur de longues distances, une ligne téléphonique est utilisée comme support de transmission. Le rôle du modem est de convertir le

signal en analogique et vice versa. Par conséquent, les modems utilisent des techniques de modulation et de démodulation.

Figure 1.14 : un modem.[7]

6. Réseau sans fil :

Un réseau sans fil est un réseau dans lequel au moins deux terminaux peuvent communiquer sans connexion filaire, il est très facile de connecter des appareils sur une distance d'une dizaine de mètres à plusieurs kilomètres. Les réseaux sans fil utilisent une liaison des ondes radioélectriques et place des câbles habituels [5,8].

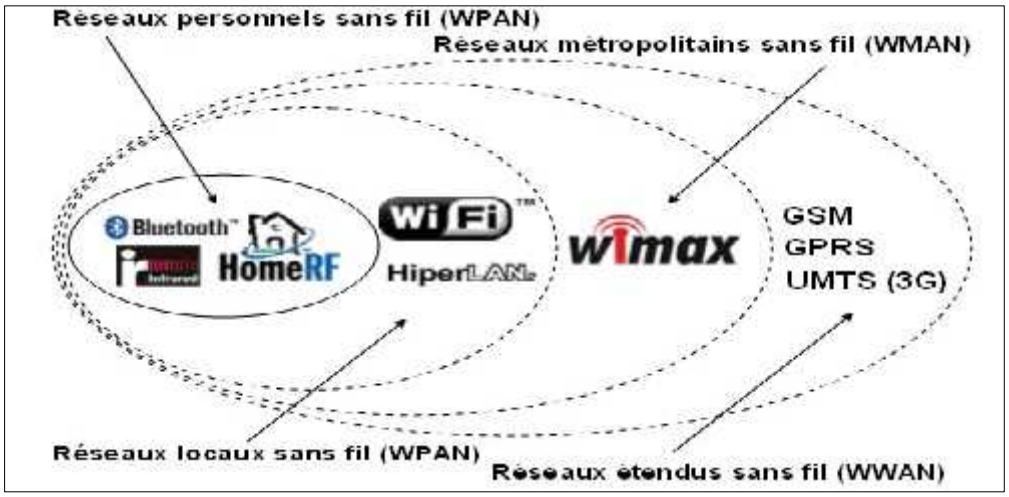


Figure 1.15 : Schéma d'un réseau sans fil.[8]

6.1. Catégories des réseaux sans fils :

Il existe plusieurs catégories

6.1.1. WPAN (Wireless Personal Area Network) :

est destiné aux réseaux sans fil à courte portée *(de l'ordre de quelques dizaines mètres*). Ce type de réseau est souvent utilisé pour connecter un assistant personnel (*imprimante, téléphone portable, appareils domestiques,* ...) à un ordinateur sans connexion, ou pour permettre des connexions sans fil entre des machines très éloignées [5,8].

Bluetooth : nom commercial relatif à la norme IEE 802.15.1 introduite par Ericson en 1994, atteignant un débit théorique de 1Mb/s pour une portée de quelques mètres.

HomeRF (*pour Home Radio Frequency*) : Introduite par le l HomeRF Working Group en 1998 (formé notamment par les constructeurs Compaq, HP, Intel, Siemens, Motorola et Microsoft) offre une vitesse théorique de 10 Mbps avec une portée d'environ 100 mètres sans amplificateur. La norme spéciale HomeRF prise en charge par Intel.

Liaison infrarouge : Cette technologie permet de créer une liaison sans fil de plusieurs mètres, comme indiqué, avec des vitesses jusqu'à quelques mégabits par seconde, elle est très utilisée en domotique (télécommandes,..).

Zig Bee : La technologie ZigBee permet d'obtenir des liaisons sans fil à très faible coût et avec une très faible consommation, elle fonctionne sur une bande de fréquence de 2, 4GHz permettant d'atteindre des débits jusqu'à 250 Kbps avec une portée maximale d'environ 100 mètres.

6.1.2. WLAN (Wireless Local Area Network) :

Local Area Networks ouLAN, qui correspond à leurs tailles intranet. entreprises.

Ils sont utilisés pour transporter toutes les informations numériques de l'entreprise.

En règle générale, les bâtiments sont câblés sur plus de centaines de mètres.

Les vitesses de ces réseaux varient aujourd'hui de quelques à plusieurs centaines de mégabits par seconde [5,8].

Ces réseaux sont principalement basés sur les technologies suivantes :

WIFI: nom commercial lié à la norme IEEE.802.11, cette technologie est destinée à de nombreuses entreprises associées au monde des télécommunications sur internet, elle offre un débit théorique de 11Mbps pour une portée de 50 mètres.

HiperLAN : Hiperlan (HIgh PERformance Radio LAN), la norme européenne développée par l'ETSI. (European Telecommunications Standards Institute).

HiperLAN offre un débit théorique de 54 Mbps sur une surface d'une centaine de mètres avec des fréquences comprises entre 5 150 et 5 300 Mhz.

6.1.3. WMAN (Wireless Metropolitan Area Network) :

Est connu sous le nom de Boucle Locale Radio(BLR). Le réseau WMAN est basé sur la norme IEEE 802.16. La boucle radio locale fournit un débit utile de 10 Mbit/s pour une portée de 4 à km, principalement orienté vers cette technologie pour les opérateurs télécoms [5,8] .

LMDS : un système de télécommunications sans fil point à multipoint spécifique au multimédia qui fournit une bande passante critique permettant des vitesses allant jusqu'à 155Mbps.

HiperMAN : Il s'agit d'une évolution du standard HiperLAN, permettant une très grande vitesse de type point à multipoint dans un rayon de 5km.

WiMAX : nom commercial IEEE 802.16 qui permet la transmission de données dans la bande de fréquence 2 à 11 GHz avec une vitesse maximale de 70Mb/s sur une portée de 50km.

6.1.4. WWAN (Wirless Wide Area Network) :

A pour but de transporter des données numériques à l'échelle d'un pays, voire d'un continent ou de plusieurs continents. Les principales technologies sont les suivantes : GSM (*Global System for Mobile Communication ou en français Groupe Spécial Mobile),* GPRS (*General Packet Radio Service), UMTS* (*Universal Mobile Télécommunication System).*

Les adresses IP, la transmission, le routage et l'adressage réseau sont des concepts importants et largement utilisés en réseautique Internet [5,8].

7. Adressage :

Étant donné qu'Internet est un réseau, la détermination de l'adresse est particulièrement importante. L'adresse IP a été configurée pour être traitée rapidement. Les routeurs qui effectuent le routage en fonction du nombre de réseaux dépendent de cette structure. Ainsi, les adresses IP pouvant être représentées sur 32 sont regroupées en 4 octets de 8 bits séparés par un point décimal. Ces 32 bit sont décomposés en deux régions contiguës :

Network ID : une section qui décrit le nombre de pièces auxquelles la station est rattachée.

Host ID : une partie correspond au numéro de la station dans le réseau local lui-même, appelée numéro d'hôte.

Selon l'adresse IP, différentes classes d'adresses sont définies. Il existe cinq classes d'adresses avec TCP/IP version 4, car les parties réseau et serveur n'ont pas toujours la même taille [1].

Il est important de savoir que l'adressage IP a des adresses réservées, par exemple :

10.0.0.0 à 10.255.255.255

172.16.0.0. à 172.31.255.255

192.168.0.0. à 192.168.255.255

Quelques normes : Ces normes régissent les réseaux locaux en activant les équipements informatiques [8].

802.1 établit le contexte général des réseaux.

802.2 établit les parties communes aux différents réseaux locaux.

802.3 Bus logique sur une topologie physique en bus ou en étoile.

802.5 anneau du type Token Ring.

802.9 Réseaux numériques.

802.11 Réseaux sans fil dans la bande de fréquence 2400 -2480Ghz.

802.11a et 802.11b les futures normes pourront atteindre une dizaine de Mbit/s.

8. Le routage :

Le routage est un processus qui permet à un datagramme d'être routé vers un destinataire, lorsque ce dernier ne se trouve pas sur le même réseau physique que l'expéditeur. Les routeurs forment une structure coopérative, de sorte que le schéma de données se déplace d'un port à un autre, jusqu'à ce que l'un d'eux le transmette au récepteur. Une des techniques de filtrage consiste à remplacer les adresses privées par des adresses publiques : c'est le NAT.

Il existe deux types de NAT, statique et dynamique [4].

NAT statique : Chaque adresse privée est convertie en adresse publique par le routeur. L'intérieur de la machine est accessible de l'extérieur. En revanche, la nécessité d'avoir le plus d'adresses internes possible ne résout pas le problème de pénurie.

NAT dynamique : [masque rading] Une adresse externe peut être attribuée à plusieurs adresses internes. Ce mécanisme nécessite de gérer les liens entre l'adresse interne et l'adresse externe compte tenu du temps et de la complexité du logiciel du routeur.

8.1. Mode de routage :

L'acheminement des informations dans le réseau consiste à s'assurer que le bloc est acheminé du point d'entrée au point de sortie spécifié par son adresse. Chaque nœud du réseau possède une table de routage, généralement appelée table de routage, qui représente la route à suivre pour atteindre le récepteur.

Il faut distinguer une politique de routage qui dicte une route choisie, d'un routage ou protocole de routage qui décrit comment les tables sont construites, c'est a dire qu'elle spécifie l'échange d'informations entre les nœuds, calcule les routes, et les coûts existent donc.

Différents modes de routage [8].

8.1.1. Routage statique ou routage fixe :

Dans ce routage il est question de construire, dans chaque nœud, une table indiquant, pour chaque destination, l'adresse du nœud suivant. Cette table est construite par l'administrateur réseau lors de la configuration du réseau et à chaque changement de topologie. Un routage simple et fixe garantit que les informations peuvent être stockées dans l'ordre même en mode déconnecté. Il n'y a pas besoin de s'inquiéter du bouclage de chemin, mais il n'y a pas de solution si le lien est rompu. Le routage statique n'est pas optimal, c'est un choix idéal pour les petits réseaux et les réseaux sans redondance dans le routage [8].

8.1.2. Routage par diffusion (de 1 vers n) :

Les informations sont acheminées vers plusieurs destinataires ou groupes d'utilisateurs en même temps. Le message doit être copié en autant de copies qu'il y a de destinataires. Cette technique oblige l'expéditeur à connaître tous les destinataires et surcharge le réseau.

Dans ce cas, on utilise, généralement, une adresse de chaque nœud, puis, uniquement les répliques nécessaires ou le dernier destinataire qu'il dessert (adresse de diffusion) [8].

8.1.3. Routage par inondation (de 1 vers tous) :

Dans le routage d'inondation, chaque nœud envoie un message sur toutes ses lignes de sortie, à l'exception de la ligne source du message. Afin d'éviter la surcharge du réseau, chaque message dispose d'un compteur de sauts. Le compteur est initialisé lors de la transmission (le nombre de sauts autorisés) et est décrémenté par chaque nœud. Lorsque le compteur de sauts est à zéro, le message est détruit. Pour éviter les bouclages, les messages sont numérotés, et chaque nœud se souvient de cet identifiant et détruit les messages qu'il a déjà vus.

Ce système est très robuste, il résiste à la destruction de plusieurs lignes et garantit de trouver toujours le plus court chemin ; il est utilisé dans certaines communications militaires et par certains protocoles de routage pour diffuser les informations d'états du réseau [8].

8.1.4. Routage par le chemin le plus court ou au moindre coût :

Dans ce mode de routage, chaque nœud tient à jour des tables indiquant quel est le plus court chemin pour atteindre le nœud destination. Dans ce mode de routage, chaque lien a un coût affecté ou calculé [8].

8.2. Le protocole de routage :

En général, tous les protocoles de routage visent à maintenir les tables de routage d'un réseau stables et cohérentes. Pour ce faire, les protocoles diffusent des informations vers d'autres systèmes du réseau pour propager des tables de routage. Ces protocoles reçoivent en retour les informations de routage du système du réseau pour les mises à jour de routage, il existe donc plusieurs familles de protocoles de routage :

8.2.1. EGP :

C'est le protocole le plus utilisé parmi les protocoles externes. La passerelle utilise EGP pour annoncer qu'elle peut atteindre les réseaux qui se trouvent dans son système autonome.

Contrairement aux protocoles internes, EGP n'essaie pas de choisir une meilleure route. L'EGP met à jour les informations de distance mais ne les met pas à jour. Ces informations de distance ne peuvent pas être directement comparées car chaque système indépendant utilise des critères différents pour ces valeurs. Les structures de routage qui dépendent d'un groupe d'unités centralisé ne peuvent pas être inadaptées à une croissance rapide.

C'est l'une des raisons pour lesquelles Internet évolue vers une architecture distribuée où le processus de routage s'exécute sur un système indépendant [4].

8.2.2. IS-IS :

Conçu à l'origine pour transporter des informations de routage respectant le formalisme CLNS, la simplicité et la robustesse de l'IS-IS ont conduit à son adaptation au modèle IP. Cette adaptation comprenait la prise en compte des préfixes IP des feuilles du nouveau type RFC 1195. Elle propose trois modes d'utilisation possibles du protocole IS-IS :

Le mode OSI-only.

Le mode IP-only.

Le mode Dual supportant simultanément deux formats d'adresses.

Quel que soit le mode d'utilisation choisi, ce protocole est sur le routage à deux niveaux de hiérarchie, niveau L1 et niveau L2 où chacun est associé à une base topologique indépendante [4].

8.2.3. BGP :

Un autre protocole commence à remplacer EGP. Comme EGP, BGP échange des informations entre les systèmes, mais BGP peut fournir des informations supplémentaires pou chaque route qui peut utiliser ces informations pour choisir la meilleure route. Une note importante à retenir est que la plupart des systèmes n'exécutent pas de protocoles externes. Ces protocoles ne sont utiles que pour les systèmes qui échangent des informations avec d'autres systèmes indépendants. La plupart des machines d'un système autonome exécutent des protocoles de routage internes. Seules les passerelles connectant de systèmes autonomes exécutent le protocole externe.

8.2.4. RIP :

RIP est le plus largement utilisé dans les protocoles de routage interne car il est inclus dans UNIX. Ce protocole choisit la route avec la longueur la plus faible comme la meilleure route. La longueur d'une route pour RIP est le nombre de ports que les données doivent traverser pour atteindre.

RIP suppose que la meilleure route est celle qui utilise moins de passerelles. [4]

9. Conclusion :

Dans cette partie, nous montrons de manière globale divers concepts sur la technologie des réseaux informatiques, ce qui est l'objet de notre recherche. Pour cette raison, nous avons décrit de manière séquentielle les étapes par lesquelles cette approche conceptuelle nous permet de comprendre ce qu'est un réseau informatique. C'est pourquoi l'une des questions de ce chapitre est d'expliquer le concept, la technologie de réseau utilisée (Ethernet, Bluetooth, etc.).

Chapitre 2: Sécurité et cryptographie des données

1. Introduction :

La sécurité des systèmes informatiques et télécommunications vise à protéger l'accès et la manipulation des données et des ressources d'un système par des mécanismes d'authentification, d'autorisation et de contrôle d'accès, etc. Néanmoins, avec l'ouverture et l'interconnexion des systèmes informatiques, des attaques exploitant les failles de ces systèmes et contournant leurs mécanismes de sécurité sont toujours possibles. Il n'est donc pas suffisant d'agir préventivement, c'est-à-dire de définir une politique de sécurité (*en termes de confidentialité, d'intégrité et de disponibilité des données et ressources du système à protéger*) et de mettre en œuvre des mécanismes implantant cette politique. Il faut aussi être capable de détecter toute tentative de violation de la politique de sécurité, c'est-à-dire toute intrusion. Nous définissons dans ce chapitre le terme de sécurité des réseaux ainsi que les méthodes utilisées.

2. Qu'est-ce que la sécurité d'un réseau ?

La sécurité du réseau est un niveau qui garantie que toutes les machines du réseau fonctionnent au mieux et que les utilisateurs autorisés ne autorisés ne disposent que des autorisations qui leur sont accordées.

Il peut s'agir :

Empêcher le personnel non autorisé d'effectuer des opérations malveillantes sur le système.

Empêcher les utilisateurs d'effectuer des opérations non intentionnelles qui pourraient endommager le système.

Protéger les données en prédisant les pannes.

Garantir le non interruption d'un service [18].

3. Les menaces :

C'est l'action ou l'événement potentiel qui attaque l'environnement ou les ressources et compromet leur sécurité.

Par conséquent, une menace compromet la sécurité, l'intégrité et la disponibilité d'un actif en exploitant la faiblesse d'un système accidentellement ou intentionnellement [10].

3.1. Les catégories des menaces :

On distingue plusieurs catégories [18] :

Divulgation: utilisation non autorisée des ressources du système d'information, entraînant la transmission d'informations confidentielles à des tiers.

Interruption : toute menace attaquant la disponibilité des informations ou des services (*panne de courant, inondation, etc*.).

Modification: violation et modification de l'intégrité des données lors du stockage (*Erreur d'entretien de données, piratage informatique,…*).

Destruction: tout ce qui participe au changement des données ou des systèmes d'information *(incendie, séisme,…).*

Enlèvement: englobe tout ce qui s'approprier frauduleusement (*vol*) aux données ou du système.

Répudiation: les menaces de cette catégorie proviennent d'utilisateurs qui refusent de prendre des mesures, les autres parties ne peuvent pas prouver le contraire.

4. Les risques:

Un risque est un dommage qui est plus ou moins susceptible de se produire.

Il est mesuré par sa probabilité d'occurrence, d'impact et de dommage après sa réalisation.

Il exprime la probabilité qu'un problème survient lorsqu'une vulnérabilité liée à une menace, ou à un danger [9].

4.1. Les critères principaux des risques :

La vulnérabilité : s'agit de défaut ou de faiblesse qui peut être exploité par des personnes malveillante pour causer des dommages. Elles peuvent être dévissées en plusieurs catégories (humaines, Technologique, organisationnelle, mise en œuvre).

Tous les systèmes informatique sont fragile, peu importe a quel point ils sont vulnérables.

La sensibilité : La sensibilité fait référence à la nature stratégique des composants du réseau. Celui-là Compte tenu de son caractère stratégique mais presque invulnérable, il peut être très sensible grâce à toutes les mesures de protection qui ont été prises pour le prémunir contre la plupart des risques.

5. Les Domaines de la sécurité :

Toutes les sphères d'activité sont concernées par la sécurité du système d'information. En fonction de son domaine d'application la sécurité se distingue en :

Sécurité physique

Sécurité d'exploitation

Sécurité logique

Sécurité applicative

Sécurité des télécommunications.

5.1. Sécurité physique:

La sécurité physique concerne tous les aspects fondamentaux liés au contrôle du système et de l'environnement dans lequel ils se situent..

Pour assurer la disponibilité des ressources vitales du réseau, on applique les moyens de protection suivants:

La protection des sources énergétiques (alimentation…),

Les normes de sécurité,

La protection de l'environnement (incendie, humidité, température,…),

Limitez l'accès physique et utilisez une supervision appropriée.

La sûreté de fonctionnement des matériels (*composants, câble,..).*

5.2. Sécurité de l'exploitation:

Elle est comprise comme tout ce qui permet au système de fonctionner correctement Cela inclut la mise en œuvre d'outils et implique une méthodologie pour l'exploitation, la maintenance, les tests, les diagnostics et les mises à jour.

En particulier, la sécurité d'exploitation dépend fortement de son industrialisation, qui est attestée par un degré de surveillance des applications et d'automatisation des tâches.

Bien que sous responsabilité opérationnelle, ceux-ci sont directement liés à leur conception et à leur réalisation. Les principaux points concernant la sécurité d'exploitation sont les suivants :

Gestion des configurations et des mises à jour.

Automatisation, contrôle et sécurité de l'exploitation.

Plan de sauvegarde.

5.3. Sécurité logique:

Une sécurité logique fait référence à la mise en œuvre de la sécurité via un logiciel. Elle repose principalement sur une implémentation complète du processus de contrôle d'accès logique, basé sur le service d'identification, d'authentification et d'autorisation. Ainsi que elle est complétée par des mesures antivirus et la sauvegarde des informations sensibles et elle vient d'être évoquée principalement, sous l'angle de la confidentialité. C'est pour cela qu'elle doit être complétée en ce qui concerne le développement, le cycle de vie et l'intégration des applications.

5.4. Sécurité applicative:

La sécurité applicative fait référence aux processus, outils et pratiques qui protègent les applications contre les menaces tout au long de leur cycle de vie. Elle repose essentiellement sur :

Une méthodologie de développement en particulier le respect des normes

L'intégration de mécanismes de sécurité, d'outils d'administration et de contrôle de qualité dans les applications,

La robustesse des applications

Un plan d'assurance sécurité.

5.5. Sécurité des télécommunications:

La sécurité des télécommunications empêchera l'intrusion dans le circuit d'échange et protégera la vie privée des individus. Elle comprend la fourniture aux utilisateurs, c'est-à-dire des applications qui communiquent, une connectivité de bout en bout et de manière fiable. Pour cela il est nécessaire mettre en place un canal de communication sécurisé entre les partenaires, quels que soient le nombre et la nature des intermédiaires (réseaux ou systèmes) nécessaires pour acheminer les données. Cela implique de créer une infrastructure réseau sécurisée en termes de droits d'accès, des protocoles de communications, des systèmes d'exploitation et des appareils.

6. Les critères de la sécurité :

Les solutions de sécurité doivent contribuer à satisfaire les critères de base de la sécurité qui sont :

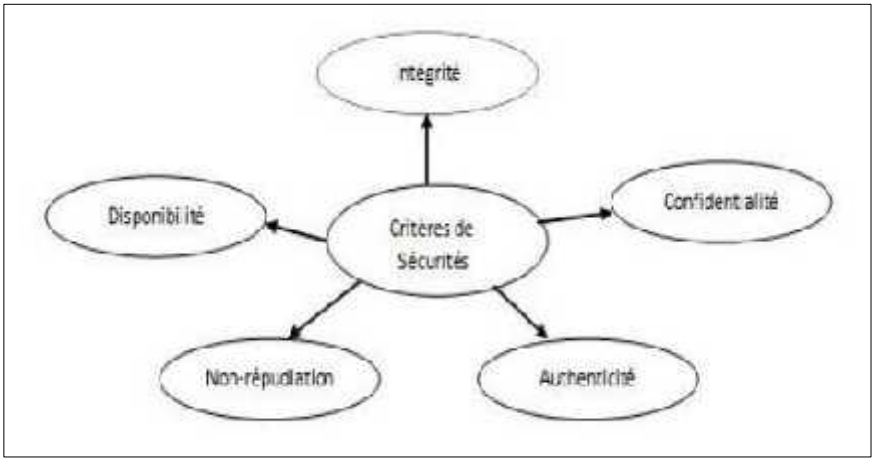


Figure 2.1 : les différents critères de la sécurité.[10]

La confidentialité: Y compris en rendant les informations incompréhensibles pour les autres et pas seulement pour les personnes impliquées dans la transaction. L'objectif est de faire en sorte que l'offre ne circule qu'entre de bonnes mains

L'intégrité: La Vérification de l'intégrité des données consiste à déterminer si les données n'ont pas été altérées au cours du processus de communication (de manière fortuite ou intentionnelle).

Le but est de s'assurer que les données arrivent en bon état.

La disponibilité: L'objectif de la disponibilité est d'assurer un accès ininterrompu à un service ou une ressource sans retard, ni dégradation.

La non-répudiation: La non-répudiation consiste à garantir qu'aucun des correspondants ne pourra refuser une transaction ou entreprendre une action.

l'authentification: consiste à assurer l'identité d'une entité pour pouvoir assurer son authentification [2,5,4].

7. Politique de sécurité :

La politique de sécurité définit un certain nombre de règles, de procédures une bonnes pratiques, permettant pour s'assurer qu'il répond au niveau de sécurité requis besoin par l'organisation. Elle a pour objectif:

Déterminer les exigences de temps de sécurité, les risques informatiques et leurs éventuelles conséquences.

Etablir des règles et procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiées.

Surveiller et détecter les vulnérabilités du système d'information et connaitre vulnérabilités à temps concernant l'application et les matériaux utilisés.

Définir ce qu'il faut faire lorsqu'une menace est détectée et qui contacter [10].

7.1. Les types de politique de sécurité :

On distingue dans cette partie deux types de sécurité [18] :

La politique qui interdit tout par défaut : Dans cette approche, toute ambiguïté est interdite. Il s'agit notamment de définir les services à autoriser (SMTP pour l'hôte serveur de courrier, http pour l'hôte devant accéder au web) et les permissions de chaque utilisateur.

La politique qui autorise tout par défaut : dans cette approche tout est permis sauf ce qui est considéré comme dangereux donc tout ce qui n'est pas interdit est permis.

Cela Cela comprend l'analyse des différents risques de l'application en cours d'exécution, en déduisant les interdictions applicables et en permettant le reste.

8. La cryptographie :

8.1. Définition :

Issu du grec cryptos (*cacher*) et graphie (*écriture*), La cryptographie est l'étude des technique mathématiques pour le cryptage et le décryptage de données pour réaliser un certain nombre d'objectif afin d'assurer la sécurité de communication. Elle permet ainsi de stocker des informations confidentielles ou de les transmettre sur des réseaux non sécurisés (*tels que l'Internet*), afin qu'aucune personne autre que le destinataire ne puisse les lire.

Le cryptage ou chiffrement (*encryption*) peut être défini comme une fonction réversible de transformation des données en considération de la protection d'information contre toute acquisition ou modification des connaissances de contenu.

Le décryptage ou déchiffrement (*decryption*) est l'opération inverse du chiffrement, qui vise a récupérer des informations cachées [13].

Cryptologie = Cryptographie + Cryptanalyse

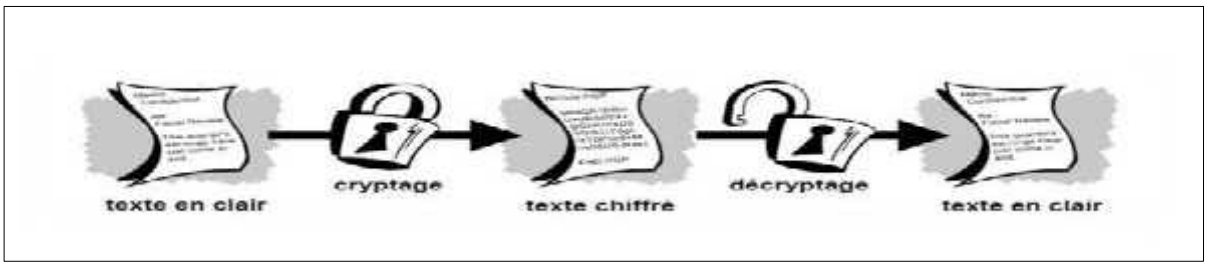


Figure 2. 2 : Schéma général de la cryptographie.[10]

8.2. La cryptographie classique :

La cryptographie classique décrit la période de l'antiquité jusqu'à la création des ordinateurs.

Elle traites des systèmes reposant sur les lettres et les caractères d'une langue naturelle.

Les crypto-systèmes classiques sont groupés en chiffrement mono alphabétique et poly-alphabétique. Le chiffrement mono alphabétique est très élémentaire, il s'agit d'une substitution simple. Chaque lettre est remplacée par une autre lettre ou symbole conformément à un certain algorithme [13].

8.2.1. LA cryptographie par substitution:

La substitution consiste à remplacer certaines entités (*généralement des lettres*) par d'autres ou par des symboles dans un message. On distingue généralement plusieurs types de crypto systèmes par substitution :

a). La substitution mono-alphabétique: est le plus simple à visualiser consistant à remplacer le caractère de la lettre par une autre lettre de l'alphabet. Comme le chiffrement par décalage.

b). La substitution poly alphabétique: Consiste à utiliser une suite de chiffres mono alphabétique réutilisée périodiquement.

c). La substitution homophonique: Permet de faire correspondre à chaque lettre du message en clair un ensemble possible d'autres caractères.

d). La substitution de poly grammes: comprend le remplacement d'un groupe de caractères (*poly gramme*) dans le message par un autre.

8.2.2.Chiffrement par transposition ou chiffrement par permutation:

Le procédé de cryptage par transposition consiste à réorganiser les données à crypter. Cette façon les rend incompréhensibles. Cela implique généralement de réorganiser les données géométriquement pour les rendre visuellement inutilisables.

Selon le principe de transposition, toutes les lettres du message sont affichées, mais dans un ordre différent.

a). Transposition complexe par colonnes: Un mot-clé secret est utilisé pour dériver Une séquence de chiffres commençant par 1 et se terminant par le nombre de lettres qui composent le mot-clé.

Cette séquence est obtenue en numérotant les lettres du mot-clé de gauche à droite et en donnant l'ordre dans lequel elles apparaissent dans l'alphabet.

Les nombres sont lus en écrivant d'abord le message en lignes dans le rectangle, puis en lisant le texte dans les colonnes dans l'ordre déterminé par la séquence.

b). Transposition par carré poly-bique: La clé secrète est utilisée pour construire l'alphabet dans un tableau.

Les coordonnées des lignes et des colonnes correspondant aux lettres du texte à chiffrer sont utilisées pour transcrire le message en chiffres.

Grâce à ce processus, chaque lettre du texte en clair est représentée par deux nombres écrits verticalement, puis les deux coordonnées sont transposées en un corps de recombinaison par les deux sur la droite ainsi obtenue.

8.3. La cryptographie moderne:

La cryptographie moderne s'intéresse généralement aux problèmes de sécurité des communications.

Les méthodes utilisées aujourd'hui sont plus complexes, mais le concept reste le même.

La différence fondamentale est que la méthode moderne manipule des bits, tandis que l'ancienne méthode manipule les caractères alphabétiques.

Elle recouvre aujourd'hui également l'ensemble des procédés informatiques devant résister à des adversaires.

Pour assurer les objectifs de la cryptographie moderne nous pouvons utiliser des algorithmes basés sur des clés. Ces algorithmes sont définis par plusieurs types de cryptographie moderne, on distingue deux approches :

La cryptographie symétrique.

La cryptographie asymétrique [6,7] .

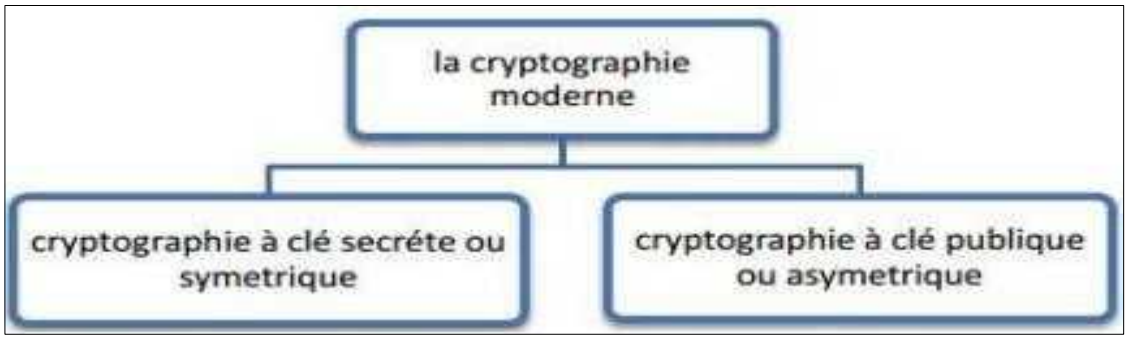


Figure 2.3 : Les méthodes de la cryptographie moderne.[14]

8.3.1. La cryptographie symétrique :

Un crypto-systèmes symétrique consiste à utiliser une clé identique pour le chiffrement et le déchiffrement, comme elle sert à crypter et à décrypter les messages.

L'émetteur et le récepteur doivent donc se mettre d'accord sur la clé secrète avant qu'ils puissent communiquer d'une façon sécurisée.

Figure 2.4 : Chiffrement symétrique.[13]

Les algorithmes symétriques sont plus rapides et plus facile à mettre en œuvre sur le matériel sur le matériel.

Les crypto-systèmes symétriques ont des problèmes de gestion des clés. En effet, lorsqu'un grand nombre de personnes souhaitent communiquer ensemble, le nombre de clés va augmenter de manière significative, ce qui devient peu pratique.

Pour **n** participants à la communication, on aura besoin de : **n*(n- 1)/2** clés secrètes enregistrés. [7]

Le cryptage symétrique fonctionne selon deux procédés différents :

a). Le cryptage par bloc : Chaque message à chiffrer est décomposé en blocs de taille fixe, et le chiffrement utilise la permutation (transposition) et la substitution pour agir sur l'ensemble du bloc. [1]

b). Le cryptage à flots de données: ces chiffrements sont généralement les plus rapides, et le taux de caractères (*débit*) adaptés au cryptage n'est pas constant. Ces chiffrements sont généralement exploités au niveau du bit ou de l'octet (bit par bit ou octet par octet) [1].

8.3.2.La cryptographie asymétrique :

La crypto-système asymétrique est basée sur des problèmes mathématiques complexes (*Décomposition de grands entiers ou d'équations logarithmiques discrètes*).

Elle repose sur le principe de deux clés : une privée et n'est connue que par l'utilisateur, l'autre publique et donc tout le monde tout le monde peut y accéder.

Ce type de cryptage élimine la problématique de la transmission de la clé .

Ce mode de cryptage est également nommé le cryptage à clé publique. Il est essentiel que l'on ne puisse pas déduire la clé privée de la clé publique [14].

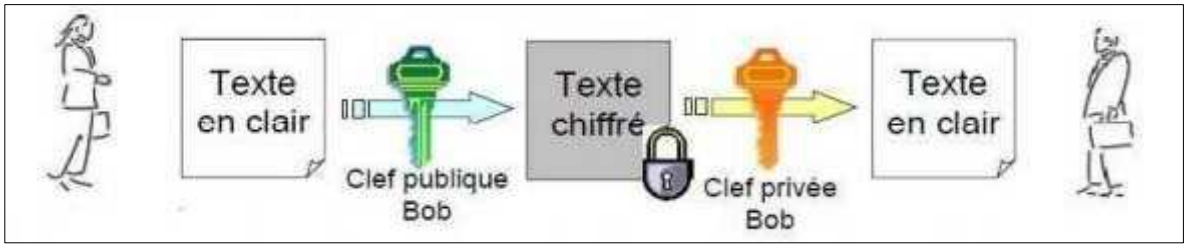


Figure 2.5 : Chiffrement asymétrique.[10]

Pour bien comprendre le principe, on peut l'illustrer avec l'échange d'une lettre entre un émetteur et un destinataire :

L'émetteur possède deux clés : privé et publique. Il envoie sa lettre contenant la clé publique au destinataire.

Le destinataire utilise la clé publique pour crypter son message; il envoie tout à l'émetteur initial. Ce dernier utilise sa clé privée pour décrypter le message.

8.4. L'algorithme symétrique :

Ce sont les algorithmes basés sur le chiffrement et déchiffrement à clé secrète.

8.4.1. DES (Data Encryption Standard) :

La norme DES a été adoptée par la NSA en 1967. Il s'agit d'un algorithme de chiffrement par bloc qui combine deux technologies de base : la confusion et la diffusion.

Et inclut le cryptage d'un bloc de texte 64 bits pour générer un mot de passe 64 bits à partir d'une clé 56 bits. Et DES peut être utilisé pour la protection par mot de passe, le cryptage de bout en bout et le cryptage des fichiers stockés sur des supports amovibles [14].

8.4.2. BLOWFISH :

a). Introduction : Blowfish a été conçu par Bruce Schneier en 1993 comme alternative à l'algorithme Existant, rapide et gratuit.

b). Caractéristiques et fonctionnement de Blowfish: Blowfish est un algorithme de chiffrement par bloc. La taille de bloc qu'il utilise est Les clés de longueur variable 64 bits peuvent aller de 32 à 448 bits. Il est basé sur l'idée qu'en utilisant une très grande clé pseudo-aléatoire, une bonne sécurité contre les attaques de cryptanalyse peut être obtenue.

Blowfish présente une bonne rapidité d'exécution excepté lors d'un changement de clé, est qu'il est environ 5 fois plus rapide que Triple DES et deux fois plus rapide que IDEA. Il reste toujours fort en cryptage, avec relativement peu d'attaques efficaces sur les versions avec moins de tours. La version complète avec 16 balles est encore totalement fiable à ce jour, et des recherches détaillées sont toujours le seul moyen de l'attaquer. Il y a deux parties dans l'algorithme : une première partie qui manipule l'expansion de la clé et une deuxième partie qui manipule le chiffrement des données.

Le principe de l'algorithme repose sur la génération de deux ensembles de clés, il utilise un tableau P contenant 18 entrées et 4 S-Box contenant chacun 256 éléments.

Les S-Boxes acceptent en entrée un mot a 8 bits et a 32 bits en sortie.

Une entrée dans le tableau P est utilisé à chaque tour. Au dernier tour, la moitié du bloc de données un XOR avec l'un des deux éléments restants de P.

Pour préparer la structure à partir de la clé on commence par l'initialisation du tableau P et les S-Boxes.

On opère alors un XOR entre la clé secrète et les entrées de la table P, un bloc de 64 de tout à zéro qui est alors chiffré.

Le résultat remplace le premier élément et le deuxième élément P, nous continuons donc jusqu'à ce que nous remplacions tous les éléments du tableau P et S-Boxes.

La mise en œuvre de l'algorithme Blowfish semble être une option pour chiffrer les données car elle doit être rapide, propre, simple et relativement sécurisée [18] .

9. Les avantages et les inconvénients de cryptographies symétriques et asymétriques :

Cryptographie	Avantages	Inconvénients
Symétrique	-Système rapide de chiffrement /déchiffrement. -Clés relativement courtes (128 ou 256 bits). -Primitive de mécanismes cryptographiques, et Bonne performances et sécurité bien étudié. -Assure la confidentialité des données.	-Gestion des clés difficiles (nombreux clés). -Point faible : l'échange de la clé secrète. -Dans un réseau de N entités susceptibles de communiquer secrètement il faut distribuer N ∗ (N-1) /2 clés.
Asymétrique	-Pas de secret à transmettre. -Nombre clés à distribuer est réduit par rapport aux clés symétriques. -Très utile pour échanger des messages facilement. -La distribution est simplifiée : La clé privée n'est jamais révélée ou transmise et la clé publique est disponible à tous les utilisateurs.	-Les algorithmes à clé publique nécessitent une capacité de traitement importante, ce qui n'est pas raisonnable pour les systèmes à ressources limitées. -La relation clés publique/clés privée impose : -La taille de clés et relativement longue (généralement entre 512 et 2048 bits). -Gestion de certificats de clés publiques. -Lenteur de calcul. -Pas d'authentification de la source.

Tableau 2.1 : Les avantages et les inconvénients symétriques/asymétrique.[14]

10. Conclusion :

Dans les environnements informatiques et de télécommunications, la mise en œuvre de système de sécurité et de techniques de cryptage permet d'assurer la confidentialité des données et de vérifier l'intégrité et l'authentification des entités. A cette fin, le système utilise une variété d'algorithmes de chiffrement existant qui feront l'objet du prochain chapitre.

Chapitre 3:

Implémentation et Réalisation d'un réseau informatique client /serveur

1. Introduction :

Comment nous l'avons présenté, la cryptographie à clé secrète brille par sa facilité d'implantation et sa rapidité.

Les algorithmes symétrique sont les plus rapides et plus facile à mettre en œuvre sur le matériel.

Dans le chapitre précédent nous avons parlé sur le principe de fonctionnement de l'algorithme Blowfish connu par sa rapidité d'exécution et sa bonne sécurité contre les attaques de cryptanalyse.

En pratique, nous allons faire une implémentation de cet algorithme dans un réseau pour testé et voir sa protection et sa fiabilité pendant une communication client/serveur.

Pour ce faire nous commencerons par la présentation du simulateur utilise, puis nous expliquerons en détaille les différentes étapes suivis pour la réalisation de notre réseau (client/serveur).

2. Principe du client/serveur :

L'architecture client/serveur désigne un mode de communication entre plusieurs composants d'un réseau. Chaque entité est considérée comme un client ou un serveur. Chaque logiciel client peut envoyer des requêtes à un serveur. Un serveur peut être spécialisé en serveur d'applications, de fichiers, de terminaux, ou encore de messagerie électronique.

Un client : Les caractéristiques d'un client sont les suivantes : il est d'abord actif (ou maître), il envoie des requêtes au serveur, il attend et reçoit les réponses du serveur.

Un serveur : Un serveur est initialement passif, il attend, il est à l'écoute, prêt à répondre aux requêtes envoyées par des clients. Dés qu'une requête lui parvient, il la traite et envoie une réponse.

Le dialogue : Le client et le serveur doivent bien sûr utiliser le même protocole de communication. Un serveur est généralement capable de servir plusieurs clients simultanément.

3. Présentation et utilisation de Packet Tracer :

CISCO Unified Communications Manager – précédemment appelé CCM (Cisco Call Manager) – est un système de gestion de communications qui réunit toutes les fonctionnalités de traitement d'appel, y compris les options suivantes : transfert d'appel, messagerie vocale, interphone, audioconférence, communication mobile.

Packet Tracer est un logiciel de CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau a l'aide d'équipements tels que les routeurs, les commutateurs ou les ordinateurs. Ces équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc [20].

3.1. Description générale :

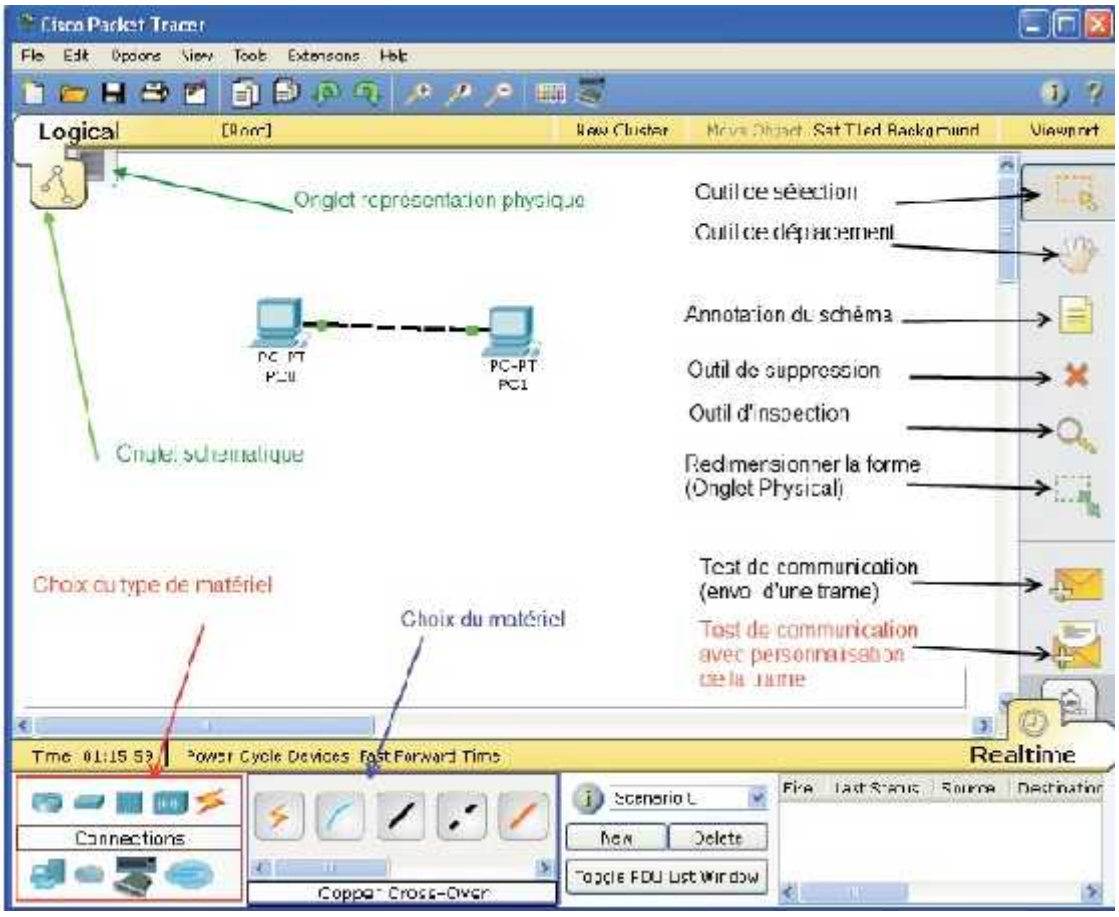


Figure 3.1 : L'aperçu général de Packet Tracer.[20]

4. Java :

Java est un langage de programmation et une plateforme informatique qui ont été créés par Sun Microsystems en 1995. Beaucoup d'applications et de sites Web ne fonctionnent pas si Java n'est pas installé et leur nombre ne cesse de croître chaque jour. Java est rapide, sécurisé et fiable. Des ordinateurs portables aux centres de données, des consoles de jeux aux superordinateurs scientifiques, des téléphones portables à Internet, la technologie Java est présente sur tous les fronts [21].

5. Construire un réseau :

Pour construire un réseau, l'utilisateur doit choisir les 8 catégories proposée par packet tracer : les routeurs, les Switch, les hubs, les équipements sans-fil, les connexions, les équipements dits terminaux (ordinateur, serveurs), des équipements personnalisés et enfin, une connexion multi utilisateurs. Lorsqu'une catégorie est sélectionnée, l'utilisateur a alors le choix entre plusieurs équipements différents. Pour ajouter un équipement il suffit de cliquer dessus puis de cliquer à l'endroit choisi.

Types d'équipements

Les differentes connexions proposées

Figure 3.2 : équipements et connexions proposées.

Pour relier deux équipements, il faut choisir la catégorie « connexion » puis cliquer sur la connexion désirée. Dans nos différents travaux pratiques, nous n'utiliserons que 2 sortes de connexions : les câbles droits et les câbles croisés.ils sont en position 3 et 4 sur la partie droite de la figure 2.

5.1. Configuration d'un équipement :

Lorsqu'un ordinateur a été ajouté (appelé PC-PT dans Packet tracer),il est possible de configurer en cliquant dessus, une fois ajouté dans le réseau.

Une nouvelle fenêtre s'ouvre comportant 3 onglets Physical, Config et Desktop.

Dans l'ongle Config, il est possible de configurer la passerelle par défaut, ainsi que l'adresse de serveur DNS.il est possible aussi de configurer l'adresse IP et le masque de sous réseau.

5.2. Construire la topologie Sur Packet Tracer :

Dans cette étape, nous allons construire un réseau selon une architecture (client/serveur).

Le réseau comportera un serveur DHCP qui servira à distribuer une IP à chaque terminal du réseau.

Nous aurons donc besoin d'une topologie avec :

Un routeur

Un Switch

Trois Laptop

Un PC

Deux Serveurs

Un routeur Wi-Fi (WRT300N)

Un Point d'accès

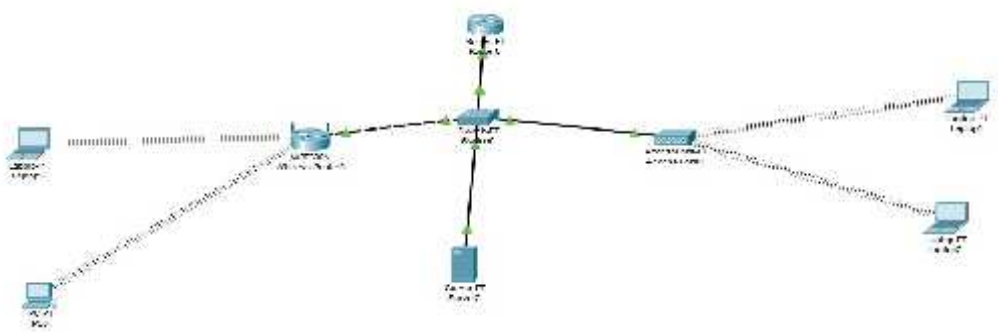


Figure 3.3 : La topologie utilisée.

5.3. Configuration basique des équipements :

Effectuer la configuration basique des équipements :

Routeur :

Définir le nom d'hôte comme indiquer sur la figure ci-dessous

Définir le mot de passe « enable »

Désactiver les recherches DNS « no shutdown »

Définir les adresses IP comme indiquer dans la figure ci-dessous

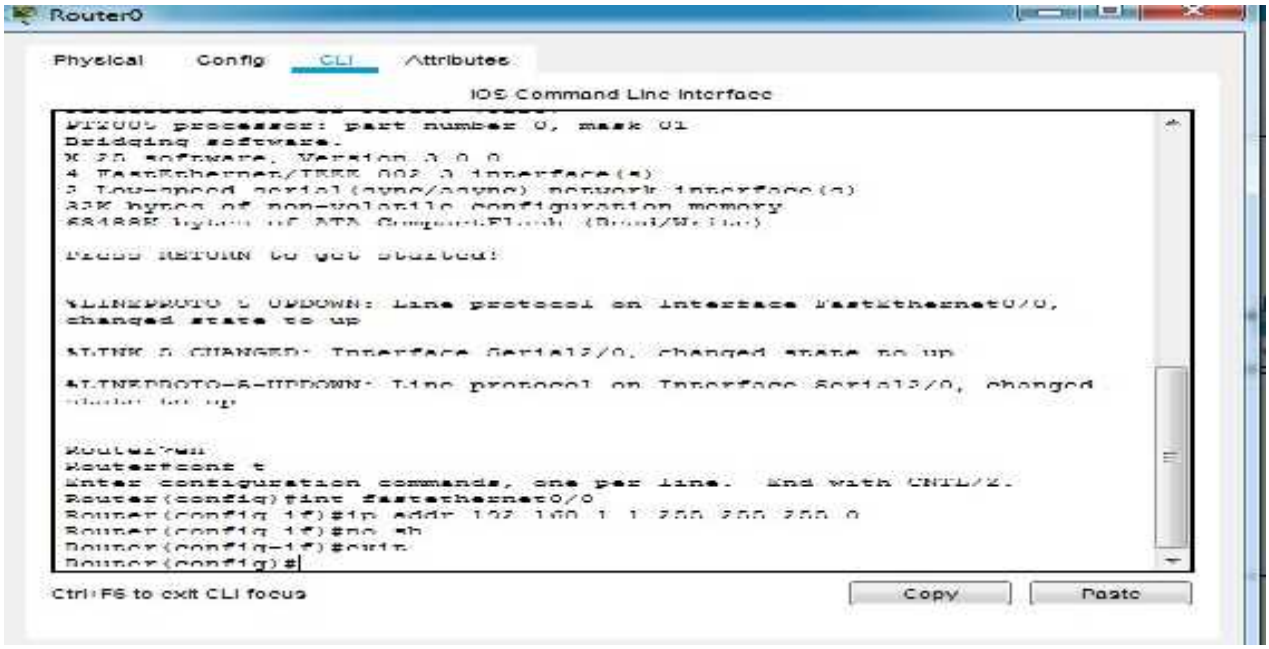


Figure 3.4 : Configuration de Routeur.

Routeur Wi-Fi (WRT300N) :

Pour configurer ce routeur wifi il suffit de cliquer sur le routeur puis sur « GUI » ensuite « Setup » et on lui définie une adresse IP comme indiquer dans la figure ci-dessous.

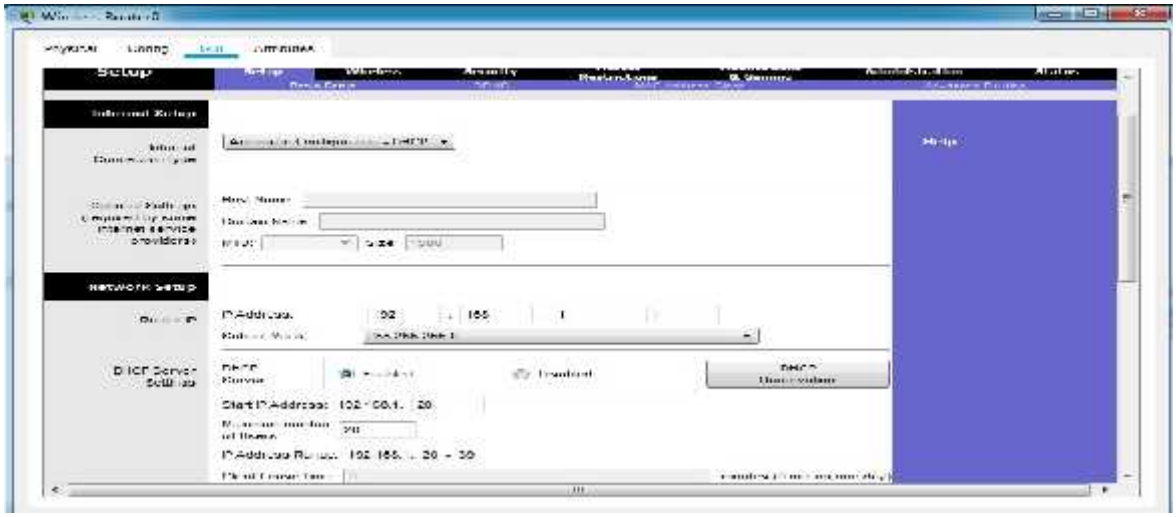


Figure 3.5 : Configuration de Routeur WRT300N.

Pour nommer le routeur on clique sur « Wireless » ensuite en cliquant sur « Wireless Security » pour choisir le mode de sécurité ainsi qu'un mot de passe pour notre routeur Wi-Fi comme indiquer dans la figure ci-dessous.

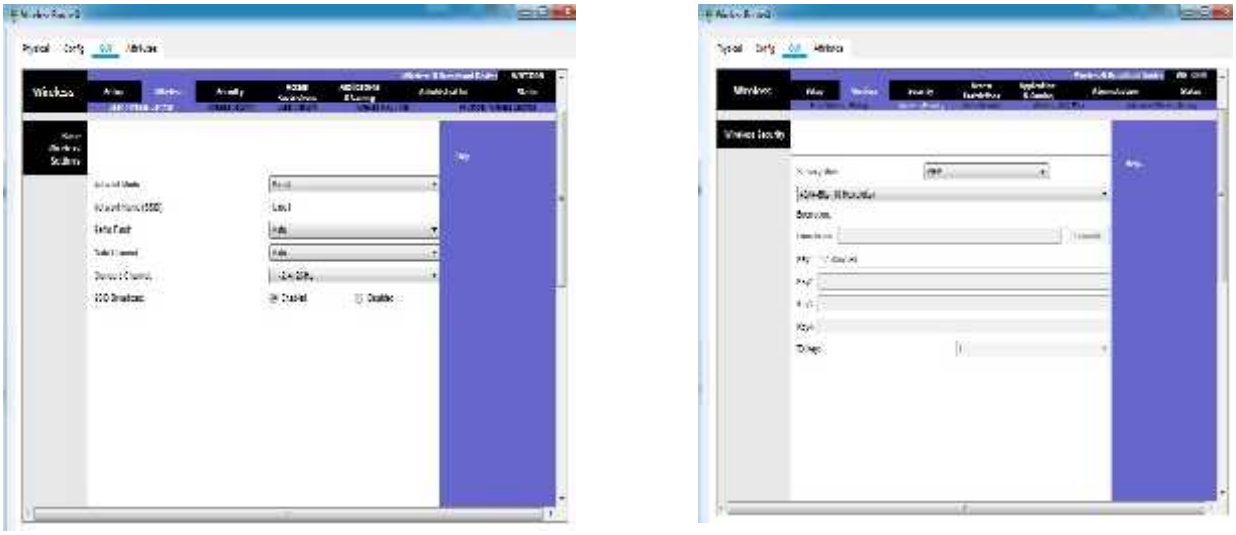


Figure 3.6 : Sécurisation de Routeur(WRT300N)

Point d'accès :

Pour la sécurité de point d'accès, on suit les étapes suivantes :

Nous allons sur « config »puis « port1 » pour lui indiquer un nom ainsi que choisir un mode de sécurité « WEP »ensuite on lui définie un mot de passe (clé).

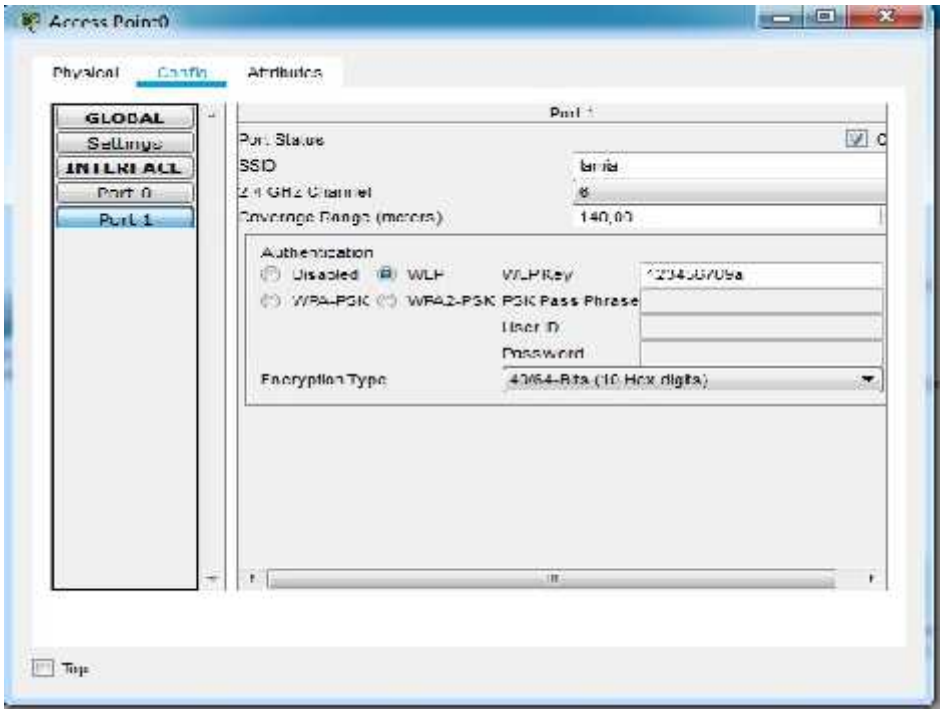
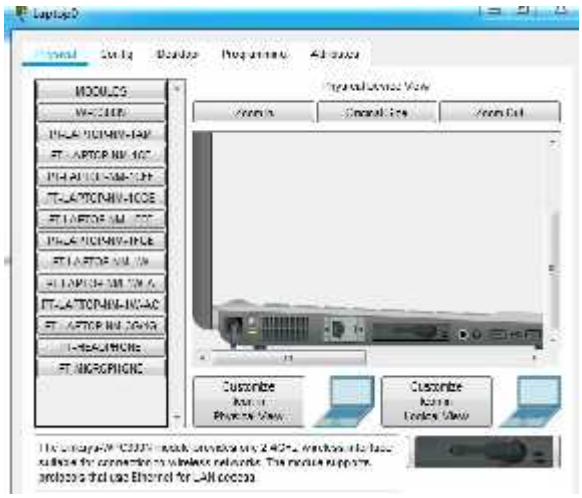
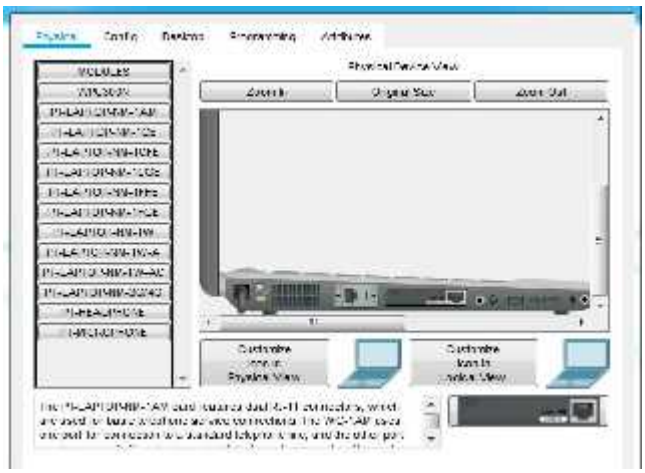


Figure 3.7 : la sécurisation de point d'accès.

Après cette étape on doit connecter les pc/Laptop avec le routeur WIFI et le point d'accès.

Pour effectuer cette étape on doit retirer l'interface internet des pc et les remplacer par l'interface wifi pour que les pc soit connecté au routeur wifi comme indiquer ci-dessous**.**





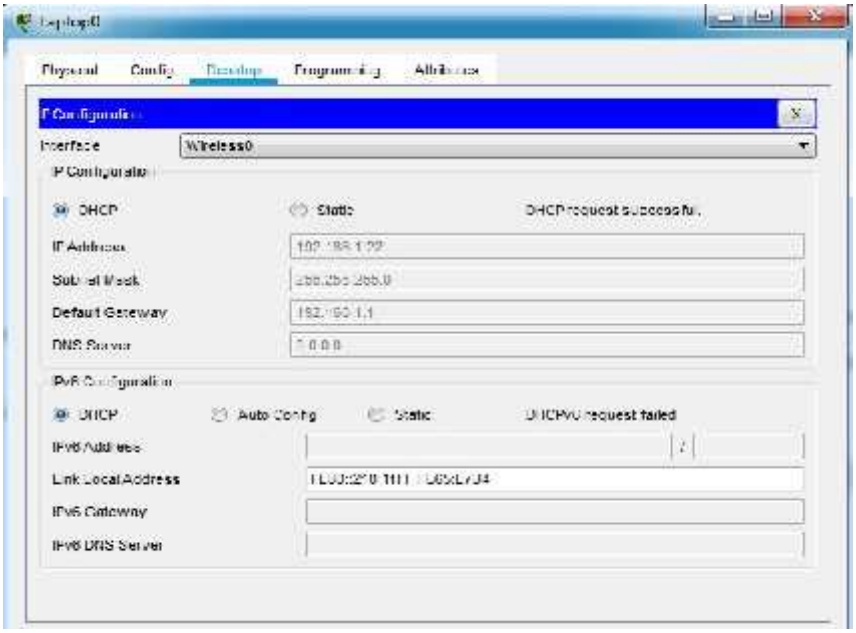
Connexion des Pc/Laptop au Routeur Wi-Fi : Cette étape s'effectue ainsi :

Nous allons sur « Desktop » Puis Pc sans fil, ensuite en passe vers connect.

En cliquant sur refresh , le nom de notre réseau Wi-Fi s'apparaît , on choisissant le réseau qui nous correspond ,une demande de mot de passe serait exigé , comme les figures ci-dessous le montre :

Figure 3.8 : Connexion des Pc/Laptop au Routeur Wi-Fi.

Attribution des adresses IP des PC/Laptop par le serveur DHCP : Maintenant une des dernières étapes est de prévenir nos ordinateurs qu'ils peuvent obtenir leurs adresses IP grâce au serveur DHCP. Pour cela il suffit de cliquer sur l'ordinateur, dans l'onglet « Desktop » puis « IP configuration » et cocher « DHCP ».



Ensuite l'ordinateur envoie une requête au serveur afin de recevoir son adresse IP. Apres avoir attendre quelque secondes « DHCP request successful » apparaître. On suit la même opération pour le reste des Pc/Laptop.

Vérification de l'interconnexion client/serveur : Les résultats obtenus sont satisfaisants comme le monte la figure ci-dessous :

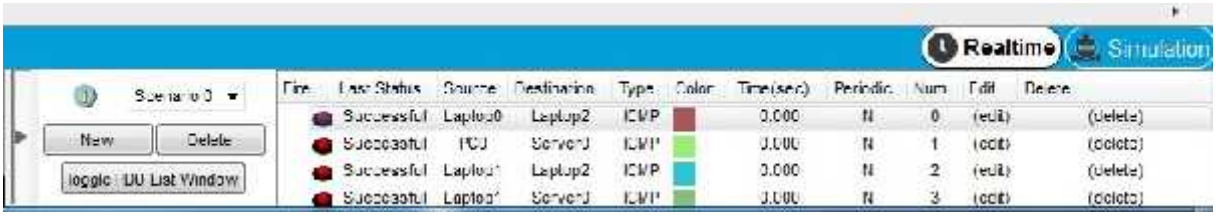


Figure 3.9 : Résultat de la simulation client/serveur.

Après la simulation on constate que notre architecture client/serveur fonctionne d'une manière correcte**.**

6. Programmation de l'architecture client/serveur sous Java :

Programme de serveur : La figure3.10 illustre le programme de serveur, dance ce programme on a crée un serveur sous le port numéro '55667' et ce port choisi aléatoirement parmi 2^{16}valeurs, ainsi que ce dernier accepte les sockets de serveur qui atteint le même port. Pour assurer le bon fonctionnement de serveur nous allons lui attribuer la méthode toUppercase qui permet de convertir tout les lettres qui sont minuscule en majuscule

```
12      ServerSocket socket= null;
13
14      try{
15          socket = new ServerSocket(55667);
16
17          while(true){
18              Socket client = socket.accept();
19              PrintWriter out = new PrintWriter(client.getOutputStream());
20              Scanner in = new Scanner(client.getInputStream());
21
22              String s = in.nextLine();
23              s = s.toUpperCase();
24              out.println(s);
25              out.flush();
```

Figure 3.10: ilustration de programme de Serveur.

Résultat obtenue après l'exécution de serveur : La figure que ce suite montre que notre serveur est bien fonctionné et prés pour recevoir les sockets de client

Figure 3.11 : Resultat de Programmation de Serveur.

Programme de Client : Dance ce programme on a créé un client qui contient le même port que le serveur, ensuite on lui a définie une adresse local host (127.0.0.1). Puis nous avons intégré l'algorithme Blowfish au niveau de client pour crypter les message de client a envoyer au serveur et les décrypter au niveau de serveur puis les mettre en majuscule.

```
Socket socket = new  Socket("localhost", 55667);

PrintWriter out= new PrintWriter(socket.getOutputStream());
Scanner in =new Scanner(socket.getInputStream());
KeyGenerator keyGenerator = KeyGenerator.getInstance("blowfish");
SecretKey secretKey = keyGenerator.generateKey();
Cipher cipher = Cipher.getInstance("blowfish");
cipher.init(Cipher.ENCRYPT_MODE, secretKey);
System.out.println("connected!");

Scanner scan=new Scanner(System.in);
System.out.println("enter a String");
String s = scan.nextLine();

byte[] encrypt = cipher.doFinal(s.getBytes());
cipher.init(Cipher.DECRYPT_MODE,secretKey);
byte[] decrypt = cipher.doFinal(encrypt);
System.out.println("Word after Encryption:"+ new String(encrypt));
System.out.println("Word after Decryption: "+ new String(decrypt));
```

Figure 3.12 : illustration de programme de client.

Les résultats obtenue : Dans La figure 3.13 représente les résultats obtenue ainsi que notre architecture client/serveur est bien fonctionné avec un bon échange des sockets sous l'algorithme de sécurité blowfish

Figure 3.13 : Réseltat de programme de l'architecture client/serveur.

7. Interprétation des résultats :

D'Après la simulation de programme on peut constater que effectivement le chiffrement et le déchiffrement ce fait au niveau de client.

En comparant ce qui a été donné par le standard et ce que nous avons obtenue comme résultat, on remarque que notre algorithme fonctionne correctement et suit bien ce qui à été spécifié par le standard.

On constate que le résultat de chiffrement/déchiffrement correspond bien au texte clair.

La fiabilité de notre algorithme de sécurité est bien vérifiée.

8. Conclusion :

Pour finaliser notre projet, nous avons commencé par introduire le simulateur Packet tracer, nous l'avons par la suite utilisé pour la configuration de notre architecture réseau (Client/serveur), puis nous avons expliqué comment configurer les équipements utilisées (Routeur, Pc/Laptop..), par la suite nous avons présenté les résultats de l'implantation de notre algorithme Blowfish sous Java sur l'architecture (client/serveur), ce qui était satisfaisants.

On peut conclure que Blowfish est un algorithme de sécurité performant, fiable et rapide dans les transmissions des données.

Conclusion Générale

La croissance de l'utilisation d'Internet met la sécurité au premier plan. L'objectif de la sécurité du réseau est de comprendre ses faiblesses et ses limites afin de pouvoir les surveiller de manière spéciale.

Dans notre travail on a mis l'accent sur l'importance de la cryptographie dans la sécurité des réseaux et l'apport des algorithmes de cryptage en particulier Blowfish qui résiste bien aux différentes attaques des cryptanalyses jusqu'à maintenant. L'objectif principal assigné à notre travail est l'implémentation de l'algorithme Blowfish sous Java dans une architecture client/ serveur crée sous Packet Tracer pour permettre le chiffrement et déchiffrement des messages avec une clé secrète qui répond bien à nos ambitions.

Ce travail nous permet d'améliorer nos connaissances dans le domaine de la sécurité des réseaux, incluant la cryptographie et la programmation.

Le domaine de la sécurité des réseaux reste ouvert aux développements avec l'évolution des réseaux et les systèmes d'information et aux contraintes liées à leurs faiblesses.

Références bibliographiques

1.Théses:

[1]. TAHAR Zahia, *Etude et simulation d'un réseau de téléphonie sur IP(TOIP),* Mémoire de fin d'étude en vue de l'obtention du Diplôme d'ingénieur d'état en Informatique, Option : Informatique Industrielle, Université de Ouargla, 2008.

[2]. N.LAHFA, A.HENAOUI, *Administration Réseaux informatiques*, Mémoire de Master, Option: Modèle Intelligent et Décision, Université de Tlemcen, 2013.

[3]. N.BELAID, C.ARKOUB, *Services d'accélération des applications et optimisation des liens WAN (WAAS : Wide Area Application services) au niveau de la CNAS d'Alger*, Mémoire de fin d'étude, Option : Communication, Université de Tizi-Ouzou, 2011.

[4]. K.NOUALI, D.MOUMOU, *Mise en place d'une solution ToIP sous le réseau intranet d'Algérie Télécom*, *Mémoire de Master en électronique*, Option : Réseaux et télécommunication, Université de Tizi-Ouzou, 2018.

[5] **https://www.memoireonline.com/11/12/6515/m_Etude-portant-sur-limplantation-dun-reseau-sans-fil-WIFI.html> (consulté de 15.06.2021)**

[6] **https://www.memoireonline.com/02/17/9624/Etude-de-la-mise-en-place-dun-reseau-informatique-dans-une-entite-etatique-decentralisee-ca.html> (consulté de 10.06.2021)**

[7]. R.KHAILA et ces collaborateurs, Installation, Configuration et administration d'un réseau local avec contrôleur de domaine, Mémoire de fin d'étude au sien de : la caisse National d'Assurance Chômage(CNAC), Option : Réseau et Système Informatique, Institut de Guelma,2018.

[8] **https://www.memoireonline.com/11/18/10447/Conception-et-deploiement-d-un-reseau-informatique-pour-la-transmission-des-donnees.html (consulté de 10.06.2021)**

[9] . JEAN-CHRISTOPHE Deneuville , *Contributions à la Cryptographie Post-Quantique*, Thèse de Doctorat en Informatique et Applications, université de Limoges, France, 2016.

[10] . M.MIHOUBI, N.MEDJANI, *Sécurisation d'une infrastructure LAN/WAN A base d'équipement Cisco*, Mémoire de Fin d'Etudes de Master académique, Option : Réseaux et télécommunication, Université de Tizi-Ouzou, 2015.

[11]. F.RIHANI, F.BOUARROUDJ, *Utilisation de tics dans la sécurité*, Mémoire de fin d'étude de Master, Université de Guelma ,2011.

[12] . M. BOUCHEMA, *Exploitation des transformées paramétriques dans le cryptage des images fixes,* Mémoire de Fin d'étude de Magister, Université FERHAT ABBAS –Sétif 1, 2012.

[13]. Z.DAHMANE, L.ABDELLI, *Implémentation d'un algorithme de cryptage sur un circuit FPGA,* Mémoire de Master en Electronique, Option : Instrumentation et Maintenance Industrielle, Université de M'sila ,2017.

[14]. A.BEN AMMAR, K.HADDOUCHE, *Amélioration de la génération des sous clés de l'algorithme cryptographique DES,* Mémoire de Master en Systèmes électroniques complexes, Université de Bouira , 2017.

[15]. REZKALLAH Louiza, *De la Cryptologie classique a la Cryptologie moderne théorie et application,* Mémoire de Magister en mathématiques, Option : Recherche Opérationnelle, USTHB, 2007.

[16]. N.MAHAMMEDI, H.MAHDADI, *Implémentation de benchmark d'opérations crypto basées ECC pour l'étude et comparaison de courbes elliptiques Fpet F2n,* Mémoire de Master académique en Informatique Industrielle, Université de Ouargla, 2013.

[17]. BENDELLA Zineb, *Gestion de la sécurité d'une application Web à l'aide d'un IDS comportemental optimisé par l'algorithme des K-means,* Mémoire de Master , Option : Réseaux et Systèmes Distribués, Université de Tlemcen, 2013.

[18]. S. ALLOU, K.ALLOUANE, *Cryptographie et sécurité des Réseaux Implémentation de l'AES sous MATLAB,* Mémoire de Master en Communication-Contrôle, Université de Tizi-Ouzou , 2008.

[19]. A. DIALLO, T.HAMDOUN, *Etude et mise en place d'un réseau informatique sécurisé à l'hôpital de jour du centre Hospitalier Universitaire Sanou Souro de Bobo-Dioulasso,* Mémoire De Fin DE Cycle pour L'obtention du diplôme d'ingénieur de travaux informatiques, Option : Réseaux et maintenance informatiques, ESI, 2010.

[20]. K.KACED ET Y.KHELILI ,Etude sur la technologie MSAN et Réalisation d'une plate forme VoIP simulée a base de la solution Vlan et le protocole DHC ,Mémoire de fin d'étude de Master académique, Spécialité : Télécommunication et Réseaux, université de Tizi-Ouzou,2015.

[21]. R.KEDADRA et I.REZZAG BARA, Les approches formelles pour les applications JAVA, Mémoire de fin d'étude master académique, Université D'El-Oued ,2014.

ملخص

مجال شبكات الكمبيوتر هو مجال شاسع للغاية يتطور بسرعة كبيرة. الشبكة الاتصال تجمع الإدارة بين خدمات الإنترنت (Telnet و ftp والبريد وما إلى ذلك) للشبكة بأكملها التي تحميها، يتطلب ذلك إنشاء حسابات مخصصة لهذه الخدمات، يمكن الوصول إلى هذه الحسابات من قبل عدد معين من الأشخاص في الشبكة، قمنا بتنفيذ مشروع نهاية الدراسة يستهدف هذه المنطقة. وضعنا لأنفسنا هدفا ؛ أمن البيانات والتشفير من خلال تنفيذ Blowfish؛ خوارزمية تشفير الكتلة في بنية العميل / الخادم لضمان كفاءتها وسرعتها وموثوقيتها في نقل البيانات.

الكلمات المفتاحية: مفاتيح ، أمن ، تشفير ، Blowfish

Résumé

Le domaine des réseaux informatiques est un domaine trop vaste, qui évolue trop vite. L'administration réseau rassemble les services Internet (Telnet, ftp, mail,...) pour tout le réseau qu’elle protège. Ceci nécessite de créer des comptes dédiés à ces services, ces comptes sont accessibles par un certain nombre de personnes du réseau. Nous avons réalisé un projet de fin d'étude visant ce domaine. On s’est proposé comme objectif ; la sécurité et la cryptographie des données en faisant une implémentation d’un algorithme de chiffrement par bloc <blowfish> dans une architecture client/serveur pour but d’assurer son efficacité, rapidité et fiabilité dans la transmission des données.

Mots clés : : clés, sécurité, cryptographie, blowfish.

Abstract

The field of computer networks is too vast a field, which evolves too quickly. Network administration brings together Internet services (Telnet, ftp, mail, etc.) for the entire network it protects. This requires creating accounts dedicated to these services, these accounts are accessible by a certain number of people in the network. We carried out an end-of-study project targeting this area. We set ourselves as a goal; data security and cryptography by implementing a <blowfish>; block cipher algorithm in a client / server architecture to ensure its efficiency, speed and reliability in data transmission.

Keywords: keys, security, cryptography, blowfish.