الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

UNIVERSITE BADJI MOKHTAR - ANNABA
BADJI MOKHTAR – ANNABA UNIVERSITY

جامعة باجي مختار – عنابـــة

Faculté : Science de l'ingéniorat

Département : Electronique

Domaine : Science et technologie

Filière : Télécommunication

Spécialité : Systèmes des Télécommunications

Mémoire

Présenté en vue de l'obtention du Diplôme de Master

Thème :

Mise en place d'un réseau 4G (LTE) sécurisé

Présenté par : *DJABOURABI Ines* & *MOKHTARI Asma*

Encadrant : *REDJATI Abdelghani* *MCB* *Université Badji Mokhtar Annaba*

Jury de Soutenance :

TAIBI Mahmoud	Professeur	UBMA	Président
REDJATI Abdelghani	MCB	UBMA	Encadrant
BOULMAIZ Amira	MCB	UBMA	Examinateur

Année Universitaire : 2019/2020

RESUME

Tout le monde sait que nous nous trouvons dans un monde où il y a un énorme problème de sécurité dans les systèmes d'information et les réseaux 4G/ LTE. Les chercheurs en sécurité ont découvert un ensemble de vulnérabilités sévères dans le protocole 4G/LTE qui pourraient être exploitées pour espionner les appels téléphoniques et les messages texte des utilisateurs, envoyer de fausses alertes d'urgence, usurper l'appareil et même déconnecter complètement les appareils.
L'objectif recherché dans ce mémoire est de permettre au lecteur, familiarisé avec les systèmes d'information et les réseaux 4G/LET, d'acquérir un ensemble de connaissances sur la sécurité qui lui permettront de mieux comprendre les divers mécanismes permettant de protéger les systèmes d'information et les réseaux 4G/LTE contre les principaux risques de piratage et d'intrusion.
Mot clé : Réseaux mobiles, 4G/LTE, Sécurité, Cisco Packet Tracer.

ABSTRACT

Everyone knows that we are in a world where there is a huge security problem in information systems and 4G/LTE networks. Security researchers have discovered a set of severe vulnerabilities in the 4G/LTE protocol that could be exploited to spy on phone calls and text messages from users, send false emergency alerts, usurp the device, and even completely disconnect the devices.

The objective of this dissertation is to provide the reader, familiar with 4G/LTE information systems and networks, with a body of security knowledge that will enable him/her to better understand the various mechanisms for protecting 4G/LTE information systems and networks against the main risks of hacking and intrusion.

Keyword: Mobile networks,4G/LTE,Security,Cisco Packet Tracer.

ملخـص

الجميع يعلم أننا في عالم حيث توجد مشكلة أمنية ضخمة في أنظمة المعلومات وشبكات الجيل الرابع
اكتشف الباحثون في مجال الأمان مجموعة من الثغرات الأمنية الخطيرة في بروتوكول الجيل الرابع التي يمكن استغلالها للتجسس على المكالمات الهاتفية والرسائل النصية من المستخدمين وإرسال تنبيهات طوارئ زائفة واغتصاب الجهاز وحتى فصل الأجهزة تمامًا.

والهدف من مذكرة التخرج هو تزويد القارئ، الذي يعرف بأنظمة وشبكات المعلومات الجيل الرابع ، بكيان من المعرفة الأمنية التي ستمكنه من فهم الآليات المختلفة لحماية أنظمة وشبكات المعلومات الجيل الرابع من المخاطر الرئيسية للقرصنة والتطفل بشكل أفضل
الكلمة المفتاح : شبكات الهاتف المحمول ,الحماية , الجيل الرابع, *Cisco Packet Tracer*.

REMERCIEMENT

Tout d'abord, nous remercions le bon Dieu qui nous a éclairé sur le chemin du savoir et nous a donné la patience, la volonté et le courage nécessaire à la réalisation de ce projet.

Nous adressons nos remerciements à notre encadreur Monsieur

REDJATI ABDELGHANI

Nous remercions les membres du jury, Monsieur TAIBI Mahmoud

Et Madame BOULMAIZ Amira

Nos remerciements sont adressés également à nos chers parents et nos fréres et sœurs pour tous les sacrifices consentis à notre égard et leur énorme soutien.

A tous nos proches amis (e). A tous nos enseignants et membres du département d'électronique de l'université BADJI MOKHTAR ANNABA

DEDICACE

Ce modeste travail est dédié :

Tous ceux qui nous aiment et qu'on aime

A nos chers parents qui nous ont soutenus et encouragés durant toute notre scolarité.

A nos frères et sœurs.

A nos enseignants.

A nos amis(e).

A toutes les personnes qui nous ont apportés de l'aide.

DJABOURABI Ines , MOKHTARI Asma

Liste des Figures

Figure I.1	L'évolution des réseaux mobile	01
Figure I.2	Architecture du réseau GSM	05
Figure I.3	Architecture du réseau GPRS	07
Figure I.4	Architecture du réseau UMTS	09
Figure I.5	Les différentes technologies d'accès sans fil pour l'utilisateur 4G	12
Figure I.6	Architecture du réseau 4G LTE	13
Figure I.7	Architecture simplifiée d'EPS	14
Figure I.8	Architecture de l'e-UTRAN	16
Figure I.9	Architecture EPC	17
Figure II.1	Classifications des attaques dans les réseaux	24
Figure II.2	L'interruption	26
Figure II.3	La modification	26
Figure II.4	La fabrication	26
Figure II.5	Architecture pare-feu	33
Figure II.6	Architecture DMZ	34
Figure II.7	Architecture d'un VPN	35
Figure II.8	Architecture de la cryptographie	37
Figure II.9	Architecture SSH	38
Figure II.10	Exemple VLAN	40
Figure III.1	La fenêtre de Packet Tracer	41
Figure III.2	L'architecture réseau avant la configuration	43
Figure III.3	Configuration S1 (Nomination, attribution et chiffrement des mots de passe)	44
Figure III.4	Attribution d'une adresse IP et l'adresse du serveur DNS au serveur web.	45
Figure III.5	Activation du serveur web.	46
Figure III.6	Attribution d'une adresse au serveur.	47
Figure III.7	Configuration du serveur DNS.	47
Figure III.8	Attribution d'une adresse au serveur.	48
Figure III.9	Configuration du serveur FTP.	49
Figure III.10	Attribution d'une adresse au serveur.	50

Figure III.11	Configuration du serveur mail	50
Figure III.12	Configuration PC «IT 1»	51
Figure III.13	Configuration R2 (Routeur)	52
Figure III.14	Configuration des interfaces et de routage statique	53
Figure III.15	Configuration Pare-feu (1)	54
Figure III.16	Configuration Pare-feu (2)	54
Figure III.17	Configuration Pare-feu (Filtrage des ports)	55
Figure III.18	Configurations ACLs	56
Figure III.19	Configurations DMZ	57
Figure III.20	L'architecture réalisée après les configurations	57
Figure III.21	Résultat de ping entre IT1 ET PC4	58
Figure III.22	Accès au site web	59
Figure III.23	Résultat de ping entre serveur FTP et IT1	60
Figure III.24	Résultat de ping entre serveur FTP et PC4	60
Figure III.25	Résultat ping entre UE1 et le serveur de liaison CO	

Liste des Symboles

1G :Première Génération

2G :Deuxième Génération

3G :Troisième Génération

3GPP : 3rd génération partnership Project

4G :Quatrième Génération

5G : Cinquième Génération

ACL : Liste de control d'accès

AMPS :Advanced Mobile Phone System

BSC :Base Station Controlers

BSS : Base Station Sub-system (access list)

BTS :Base Transceiver System

CDMA :Code Division Multiple Access

DCS : Digital Communication System

DMZ : Demilitarized Zone

DNS : Domain Name Service

DoS : Denial of Service

EDGE :Enhanced Data for GSM Evolution

eNodeB : evolved NodeB

EPC : Evolved Packet Core

EPS : Evolved Packet System

EPS : Evolved Packet System

ETACS :Extended Total Access Communication System

ETSI : European Télécommunications Standards Institute

E-UTRAN : Evolved UMTS Terrestrial Radio Access Network Le Réseau d'accès

FDD : Frequency Division Duplex

FTP : File Transfer Protocol

GGSN :Gateway GPRS Support Node

GPRS :General Packet Radio Service

GSM : Global Systeme for Mobile

GSN : GPRS support nodes

HSDPA : High Speed Downlink Packet Access

HSPA : High Speed Packet Access

HSS : Home Subscriber Server

HSUPA :High Speed UplinkPacket Access

HTTP : Hypertext Transfer Protocol

IMS : IP Multimedia Subsystem

IS-136 :Interim Standard-136

IS-95 :Interim Standard-95

LAN : Local Area Network

LTE :Long Term Evolution

MITM : man in the middle

MME : Mobility Manager Entity

MMS :Multimedia Message Service

MPF : Modular Policy Framework

MSC :Mobile Switching Center

NMT :Nordic Mobile Telephone

OFDMA : Orthogonal Frequency Division Multiple Access

OSI : Open Systems Interconnection

PC : Personnel Computer

PCRF : Policy and Charging Rules Function

PCRF : Policy and Charging Rules Function

PDNGW : Packet Data Network Gateway

P-GW : Packet Data Network Gateway

PTMP: Point To Multie Point

PTP :Point To Point

RNC : Radio Network Controller

RRC : Radio Resource Control

RRC : Radio Ressource Control

RTC : réseau téléphonique commuté

SB : Stations de Base

SGSN : Serving GPRS Support Node

SGW : Serving Gateway

SMS :Short Message Service

SMTP : Simple Mail Transfer Protocol

SSH : Secure Shell

TACS :Total Access Communication System

TCP :Transmission Control Protocol

TDD : Time Division Duplex

TDMA :Time Division Multiple Access

UDP : User Datagram Protocol

UE : User équipement

UIT : union internationale des télécommunications

UMTS: Universal Mobile Télécommunications System

USIM : Universal Subscriber Identity Module

UWB : ultra-wideband

VLAN :Virtual Local Area Network

VoIP : Voice Over IP

WEB : World Wide Web

WiFi : Wireless Fidelity

Table des matières

RESUME..... I
REMERCIEMENT..... II
DEDICACE..... III
Liste des figures..... IV
Liste des Symboles..... VI
Table des matières..... IX
Introduction générale 1

CHAPITRE I: Généralités sur les réseaux mobiles

I.1 Introduction 3
I.2 Evolution des réseaux mobiles 3
I.2.1 La première génération des réseaux mobiles 3
I.2.2 La deuxième génération des réseaux mobiles (2G) 4
I.2.3 La troisième génération des réseaux mobiles 3G 5
I.2.4 La quatrième génération des réseaux mobiles 4G 5
I.2.5 La cinquième génération des réseaux mobiles 5G 5
I.3 Les différentes normes téléphoniques mobiles sans fil 5
I.3.1 La première génération des téléphones mobile (1G) 6
I.3.2 La deuxième génération des téléphones mobiles (2G) 6
I.3.3 La troisième génération des téléphones mobiles 3G (UMTS) 10
I.3.4 La quatrième génération des téléphones mobiles 4G (LTE) 12
I.4 Généralités sur la 4G 13
I.4.1 Définition de 4G/LTE 13
I.4.2 Objectifs de la 4G 14
I.4.3 Avantages de la 4G de mobiles 15
I.4.4 Architecture de la 4G/LTE 15
I.4.4.1 UE 16
I.4.4.2 E-UTRAN 17
I.4.4.3 EPC 19
I.4.5 Performances et caractéristiques des réseaux 4G 21
I.4.5.1 Les Débits 21
I.4.5.2 La latence 22
I.4.5.3 L'agilité en fréquence 22
I.4.5.4 Le multiplexage 22
I.4.5.5 La mobilité 22
I.5 Conclusion 23

CHAPITRE II: La sécurité dans les réseaux mobiles 4G

II.1 Introduction 24
II.2 Les objectifs de la sécurité 24
II.3 Les attaques dans les réseaux 4G 25
II.3.1 Les scénarios d'attaques 25
II.3.1.1 Attaque Passives 26
II.3.1.2 Attaque actives 26
II.3.2 Description de quelques attaques 29
II.3.2.1 Attaque par déni de service (DoS) 29
II.3.2.2 Écoute du réseau (sniffer) 29
II.3.2.3 Intrusion 29
II.3.2.4 Cheval de Troie 30
II.3.2.5 Man in middle 30
II.3.2.6 L'attaque IP spoofing 31
II.4 Mis en place d'une politique de sécurité 31
II.5 Détermination des moyens nécessaires 32
II.6 Développement des procédures adaptées 33
II.7 Conclusion 42

CHAPITRE III: Simulations et résultats

III.1 Introduction 43
III.2 Présentation du simulateur Cisco « Packet Tracer » 43
III.3 Présentation de l'architecture réseau avant la configuration 44
III.4 Configuration des équipements 45
III.4.1 Configuration des commutateurs 45
III.4.2 Configuration des serveurs et des Pcs 46
III.4.3 Configuration des routeurs 53
III.5 Configuration de pare feu, liste d'accès et DMZ 55
III.5.1 Configuration Pare Feu : 55
III.5.2 Configuration liste d'accès (ACLs) 57
III.5.3 Configuration DMZ 58
III.6 Architecture réalisée 59
III.7 Tests et validation des configurations 60
III.8 Conclusion 63

Conclusion Générale 64
Bibliographie

Introduction générale

Le succès des technologies sans fil et des communications mobiles a déterminé l'existence d'une variété de standards qui permettent aux utilisateurs d'avoir accès à l'Internet. Chaque technologie cherche à atteindre un certain type de client avec des besoins spécifiques. L'avantage d'avoir une telle diversité est que l'utilisateur a plusieurs choix du point de vue d'accès Internet, de la bande passante et de la couverture. Dans ces conditions, l'expansion des services qui reposent sur tous ces réseaux pose des problèmes d'interconnexion et de gestion de la mobilité en général.

Les réseaux de quatrième génération (4G) représentent l'évolution des communications sans fil et sont basés sur l'infrastructure existante, sur l'interconnexion des réseaux déjà déployés. Ce pas évolutif semble assez naturel dans les conditions où les opérateurs ont investi beaucoup dans les réseaux de troisième génération.

Les évolutions se poursuivent, tant dans le monde des réseaux spécialisés (capteurs, systèmes intelligents, etc.) que des réseaux télécoms. Ceux-ci voient désormais des solutions concurrentes apparaître provenant de divers horizons : le monde télécoms classiques avec HSDPA, le monde des réseaux sans fil avec le WiMAX, voire le monde de la diffusion télévision terrestre et satellite (DVB-T, DVB-H, DVB-S).

Mais avec toutes ces évolutions, certaines implémentations de réseaux 4G et d'applications mobiles sont actuellement vulnérables à plusieurs échelles. Ils peuvent entraîner une perte de confidentialité, une facturation incorrecte et une falsification de données. C'est ce qui nous a poussé à nous demander comment sécuriser les réseaux 4G/LTE à travers les mécanismes de sécurité : l'authentification, le chiffrement et la confidentialité ; permettant de protéger les systèmes d'information et les réseaux 4G/LTE contre les principaux risques de piratage et d'intrusion.

A travers cette problématique en ressort un certain nombre de questions tel que :

Quelles sont les différentes générations de téléphonies mobiles ?

Quelles sont les spécificités et les technologies dans les réseaux 4G/LTE ?

Qu'est-ce qui menace la sécurité des réseaux 4G/LTE ?

Comment protéger et améliorer la sécurité des réseaux 4G/LTE ?

Afin d'atteindre notre objectif, nous avons réparti notre travail en trois chapitres présentés comme suit :

1. Le premier chapitre présente les 5 principaux générations de réseaux mobiles en détails.
2. Le deuxième chapitre « La sécurité dans les réseaux mobiles 4G » aborde les différents mécanismes de sécurité.
3. Le troisième chapitre présente les résultats de simulation à l'aide du logiciel Cisco Packet Tracer ainsi que les discussions.

Au final, nous terminerons ce travail par une conclusion générale résumant les connaissances acquises durant la réalisation du projet

Chapitre I : Généralités sur les réseaux mobiles

I.1 Introduction

Depuis plusieurs années le développement des réseaux mobiles n'a pas cessé d'accroitre, plusieurs générations ont vues le jour (1G, 2G, 3G, 4G) et connues une évolution remarquable, en apportant un débit exceptionnel et qui ne cesse d'augmenter, une bande passante de plus en plus large et un des avantages d'une telle bande passante est le nombre d'utilisateurs pouvant être supportés.

I.2 Evolution des réseaux mobiles

Les réseaux mobiles ont beaucoup évolué depuis leur apparition dans les années 1970 à nos jours. Cette évolution, de la première a la quatrième génération des réseaux cellulaires.

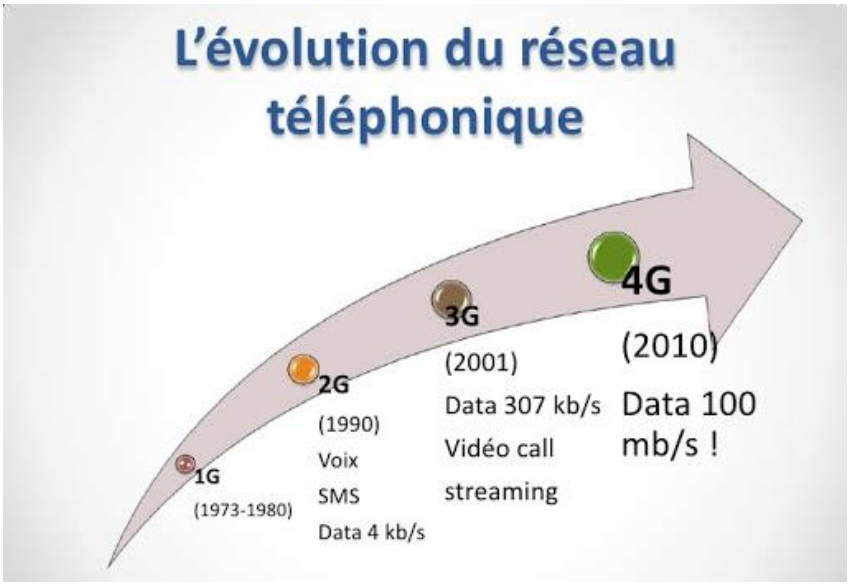

Figure I.1 - L'évolution des réseaux mobile

I.2.1 La première génération des réseaux mobiles

La 1g a été le début d'une grande révolution dans le monde de la téléphonie. Celle-ci possédait un fonctionnement analogique et était composée de nombreux appareils volumineux suivants [1] :

- Apparu en 1976 aux États-Unis, l'AMPS (Advanced Mobile Phone System) constitue le premier standard réseau cellulaire utilisé principalement en Outre-Atlantique, en Russie

ainsi qu'en Asie. Il était facile de pirater ce système puisqu'il possédait de faibles mécanismes de sécurité rendant le piratage des lignes téléphoniques plus propices.

- La TACS (Total Access Communication System) est la version européenne du modèle AMPS cité ci-dessus. Ayant une bande de fréquence plus performante (900MHz), ce système fut plus utilisé notamment dans en Angleterre, puis en Asie (Hong-Kong et Japon) par la suite.
- Par la suite en 1983, ETACS (Extended Total Access Communication System) est une version améliorée du standard TACS et donc AMPS développé au Royaume-Uni utilisant un nombre plus important de canaux de communication.

Les réseaux cellulaires de premières génération ont été rendus obsolètes avec l'apparition d'une seconde génération entièrement numérique.

I.2.2 La deuxième génération des réseaux mobiles (2G)

Elle est apparue au début des années 90 avec le mode de transmission numérique. Il devient ainsi possible de transmettre, en plus de la voix, des données numériques de faible volume telles que les SMS (Short Message Service) et les MMS (Multimedia Message Service).

Les standards 2G les plus utilisés sont le GSM, l'IS-95 (Interim Standard-95) qui est basé sur le codage CDMA (Code Division Multiple Access) et l'IS-136 (Interim Standard-136) qui se base sur le codage TDMA (Time Division Multiple Access).

Le GSM est cependant le standard ayant connu la plus grande percée avec l'utilisation de la bande des 1900MHz en Amérique du Nord et au Japon et de la bande des 900MHz et 1800Mhz sur les autres continents.

C'est d'ailleurs sur ce standard que se basent les réseaux GPRS (General Packet Radio Service : 2.5G) et EDGE (Enhanced Data for GSM Evolution : 2.75G) qui sont venus corriger les faibles débits du GSM (environ 9,6 kbps). Le kbps permettant ainsi la transmission simultanée de la voix et de données. L'utilisation des applications multimédias est rendue possible par EDG kbps [2].

I.2.3 La troisième génération des réseaux mobiles 3G

Elle propose d'échanger 1.9 mégabits par seconde, soit environ 5 fois plus rapidement que la génération précédente. Elle a permis d'utilisation des applications vidéos sur le mobile et l'amélioration des multimédias. Elle a également permis l'augmentation du débit pour pouvoir passer d'un service de téléphonie (à connexion circuit) vers un service DATA (connexion par paquets). Elle ajouta des amplificateurs pour amplifier le signal pour qu'il puisse être accueilli par une autre antenne.

I.2.4 La quatrième génération des réseaux mobiles 4G

Le LTE (Long Term Evolution) a été envisagé dès novembre 2004 comme l'évolution à long terme de l'UMTS (d'où son nom de Long Term Evolution) par l'organisme 3GPP dans le contexte de la 4G, Cette évolution était alors destinée à maintenir la compétitivité de l'UMTS. Ce dernier peut atteindre un débit de 50 Mb/s en lien montant et 100 Mb/s en lien descendant.

I.2.5 La cinquième génération des réseaux mobiles 5G

La 5G pour 2020, elle est déjà en phase de test par plusieurs opérateurs dans diverses villes européennes. Celle-ci devrait permettre des débits de télécommunications mobiles hyper rapides, avec des débits pouvant aller jusqu'à 5Go/s grâce à une bande passante de 28 GHz.
Une capacité qui se développe en parallèle des habitudes des utilisateurs et de leurs besoins de connexions plus rapides pour streamer des films et séries en 4K, mais aussi les nouvelles technologies de réalité augmentée et de réalité virtuelle. Au-delà du mobile, la 5G devrait également avoir un profond impact sur le marché automobile, les objets connectés, la domotique et le monde des entreprises. Évidemment, ce genre de connexion demandera des terminaux compatibles avec ce réseau. Les constructeurs de smartphones travaillent déjà dessus et le premier modèle 5G devrait arriver en magasin en 2019 [3].

I.3 Les différentes normes téléphoniques mobiles sans fil

Pour une bonne explication de la technologie utilisée aujourd'hui, il faut d'abord connaitre l'évolution de ces techniques, cela va nous aider à savoir de quoi nous sommes partis pour mieux se positionner à l'heure actuelle.

I.3.1 La première génération des téléphones mobile (1G)

La première génération de systèmes cellulaires (1G) reposait sur un système de communications mobiles analogiques. Cette génération a bénéficié de deux inventions techniques majeures des années 1970 : le microprocesseur et le transport numérique des données entre les téléphones mobiles et la station de base. Les appareilles utilisés étaient particulièrement volumineux [1].
La première génération de système cellulaire 1G utilisait essentiellement les standards suivants :

- **AMPS (Advanced Mobile Phone System)** lancé aux Etats-Unis, est un réseau analogique reposant sur la technologie FDMA (Frequency Division Multiple Access)
- **NMT (Nordic Mobile Telephone)** a été essentiellement conçu dans les pays nordiques et utilisés dans d'autres parties de la planète.
- **TACS (Total Access Communications System)**, qui repose sur la technologie AMPS, a été fortement utilisé en grande Bretagne.

Cette première génération de réseaux cellulaires utilisant une technologie analogique a été remplacée dès l'apparition d'une seconde génération plus performante utilisant une technologie numérique.

I.3.2 La deuxième génération des téléphones mobiles (2G)

La deuxième génération (2G) de système cellulaire repose sur une technologie numérique a été développé à la fin des années 1980. Ces systèmes cellulaires utilisent une technologie numérique pour la liaison ainsi que pour le signal vocal. Ce système apporte une meilleure qualité ainsi qu'une plus grande capacité à moindre coût pour l'utilisateur [4].

La deuxième génération de systèmes cellulaires (2G) utilise essentiellement les standards suivants :

- **GSM (2G)**
- **GPRS (2.5G)** est un système mobile intermédiaire entre la (2G) et la (3G) (débits
- inferieurs à 100 kbit /s)
- **EDGE (Enhaced Data Rates for GSM Evolution, 2.75G)**

1) Le réseau GSM (2G)

Le réseau GSM (*Global system for mobile communication*) est un système cellulaire, numérique de télécommunication radio-mobile. Son développement remonte aux années 80 mais son exploitation à commencer en 1992 après une longue phase de normalisation est de coopération international. Les premiers réseaux ouvrent en GSM 900 et deux ans plus tard, la norme GSM s'étend en DCS 1800 (digital communication system). La figure I.2 présente l'architecture du réseau GSM.

Un réseau de radiotéléphonie a pour premier rôle de permettre des communications entre abonnées mobiles et abonnées du réseau téléphonie commuté (RTC). Il s'interface avec le RTC et comprend des commutateurs.
Enfin, comme tout réseau, il doit offrir à l'opérateur des facilités d'exploitation et de maintenance.

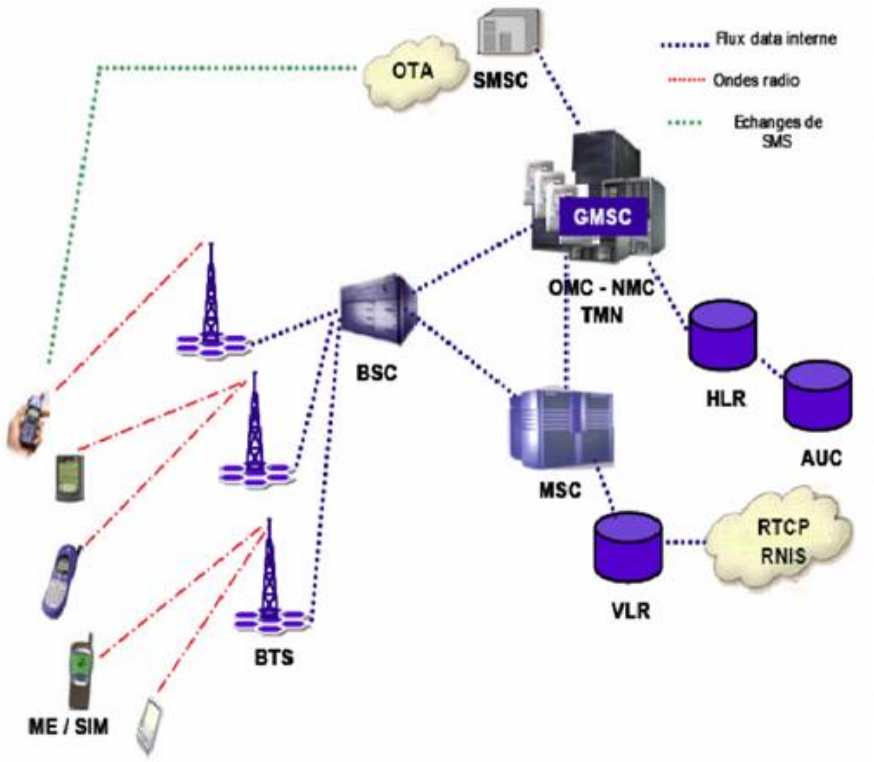

Figure I.2 - Architecture du réseau GSM

Les équipements du réseau GSM comprennent :

a. **Les BTS (Base Tranceiver System) :** Il s'agit des antennes et des équipements électroniques (amplificateurs, alimentations, …) installés à proximité de celles-ci.
b. **Les BSC (Base Station Controlers) :** Chaque BSC contrôle un certain nombre de BTS ; il constitue un nœud de communications vers et en provenance de ces BTS.
c. **Un MSC (Mobile Swithching Center) :** Il n'y a qu'un MSC par réseau GSM ; il s'agit essentiellement d'un commutateur qui constitue le nœud central du réseau de téléphonie mobile ; il est connecté au réseau de téléphonie fixe, ainsi qu'aux réseaux GSM des opérateurs concurrents.

2) Le réseau GPRS (2.5)

Le standard GPRS (*General Packet Radio Service*) est une évolution de la norme GSM, ce qui lui vaut parfois l'appellation GSM++ (ou GMS 2+). Etant donné qu'il s'agit d'une norme de téléphonie de seconde génération permettant de faire la transition vers la troisième génération (3G), on parle généralement de 2.5G pour classifier le standard GPRS.

Le GPRS permet d'étendre l'architecture du standard GSM, afin d'autoriser le transfert de données par paquets, avec des débits théoriques maximums de l'ordre de 171,2 kbit/s (en pratique jusqu'à 114 kbit/s). Grâce au mode de transfert par paquets, les transmissions de données n'utilisent le réseau que lorsque c'est nécessaire. Le standard GPRS permet donc de facturer l'utilisateur au volume échangé plutôt qu'à la durée de connexion, ce qui signifie notamment qu'il peut rester connecté sans surcoût.

Ainsi, le standard GPRS utilise l'architecture du réseau GSM pour le transport de la voix, et propose d'accéder à des réseaux de données (notamment internet) utilisant le Protocol IP et le Protocol X.25.

Le GPRS permet de nouveaux usages que ne permettait pas la norme GSM, généralement catégorisés par les classes de services suivants :

- Services point à point (PTP), c'est-à-dire la capacité à se connecter en mode client-serveur à une machine d'un réseau IP,

- Services point à multipoint (PTMP), c'est-à-dire l'aptitude à envoyer un paquet à un groupe de destinataires (*Multicast*).
- Services de messages courts (SMS).

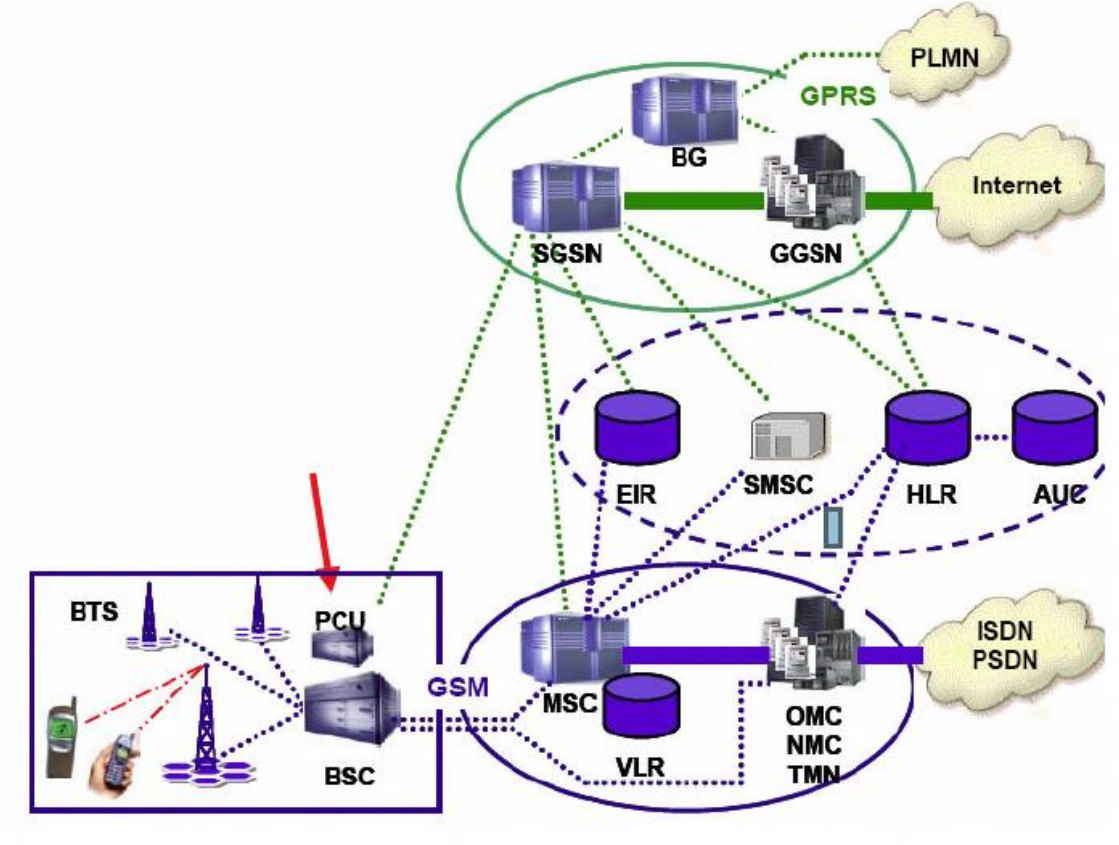

Figure I.3 - Architecture du réseau GPRS

L'intégration du GPRS dans une architecture GSM nécessite l'ajonction de nouveaux nœuds réseau appelés GSN (GPRS support nodes) situés sur un réseau fédérateur (*backbone*) :

- Le SGSN (*Serving GPRS Support Node*, soit en français *Noeud de support GPRS de service*), routeur permettant de gérer les coordonnées des terminaux de la zone et de réaliser l'interface de transit des paquets avec la passerelle *GGSN*.
- Le GGSN (*Gateway GPRS Support Node*, soit en français *Noeud de support GPRS passerelle*), passerelle s'interfaçant avec les autres réseaux de données (internet). Le GGSN est notamment chargé de fournir une adresse IP aux terminaux mobiles pendant toute la durée de la connexion.

3) Le réseau EDGE (2.75)

Avec le GPRS, le système GSM permet un accès au monde de l'internet et ouvre la porte aux applications multimédias par l'utilisation de la commutation de paquets et l'augmentation du débit. Cependant, les débits restent limités à environ 50kbits/s dans la pratique, du fait de la modulation binaire (GMSK) véhiculant environ 1bit/symbole.

Afin de dépasser ces limitations, une proposition a été faite par l'ETSI (European Telecommunications Standards Institute) en 1997 pour l'utilisation d'une modulation à plus forte efficacité spectrale appelée 8-PSK (environ 3bits/symbole). Des études de faisabilité s'en sont suivi et ont conduit au concept d'EDGE (Enhanced Data rates for the Global Evolution).

Le standard EDGE est une évolution de la norme GSM, modifiant le type de modulation.
Tout comme la norme GPRS, le standard EDGE est utilisé comme transition vers la troisième génération de téléphonie mobile (3G). On parle ainsi de 2.75G pour désigner le standard EDGE.

EDGE utilise une modulation différente de la modulation utilisée par GSM, ce qui implique une modification des stations de base et des terminaux mobiles. Il permet ainsi de multiplier par un facteur 3 le débit des données avec une couverture plus réduite. Dans la théorie, EDGE permet d'atteindre des débits allant jusqu'à 384 kbit/s pour les stations fixes (piétons et véhicules lents) et jusqu'à 144 kbit/s pour les stations mobiles (véhicules rapides).

L'EDGE est une extension du réseau GPRS. Seule le sous-système radio est sensiblement modifié.
Le déploiement de L'EDGE nécessite :

- La mise à jour du BSC et de la BTS.
- L'ajout d'un émetteur-récepteur (EDGE Transceiver) au niveau de la BTS, capable de supporter la modulation 8-PSK.

I.3.3 La troisième génération des téléphones mobiles 3G (UMTS)

Le réseau UMTS vient se combiner aux réseaux déjà existants GSM et GPRS apportent des fonctionnalités respectives de Voix et de Data ; le réseau UMTS apporte ensuite les fonctionnalités Multimédia.

La mise en place d'un réseau UMTS a permet à un opérateur de compléter son offre existante par l'apport de nouveaux services en mode paquet complétant ainsi les réseaux GSM et GPRS. L'idée fondatrice du système 3G est d'intégrer tous les réseaux de deuxième génération du monde entier en un seul réseau et de lui adjoindre des capacités multimédia (haut débit pour les données).

a) Infrastructure du réseau UMTS

Le réseau UMTS s'appuie sur les éléments de base du réseau GSM et GPRS. Il est en charge de la commutation et du routage des communications (voix et données) vers les réseaux externes. Dans un premier temps, le réseau UMTS devrait s'appuyer sur le réseau GPRS.

Le réseau UMTS vient se combiner aux réseaux déjà existants GSM et GPRS, qui apportent des fonctionnalités respectives de Voix et de Données, le réseau UMTS apporte ensuite les fonctionnalités Multimédia.

Le réseau sur se décompose en deux parties : le domaine circuit dans un premier temps et le domaine paquet.

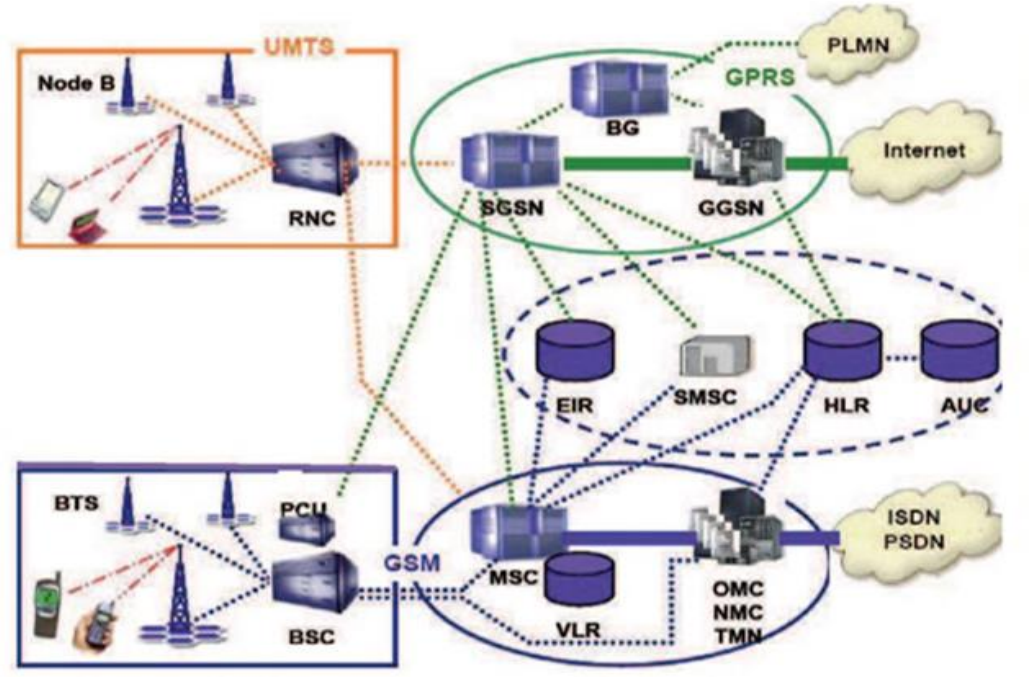

Figure I.4 - Architecture du réseau UMTS

b) Les équipements d'un réseau UMTS

La mise en place du réseau UMTS implique la mise en place de nouveaux éléments sur le réseau.

- **Le « Node B » :** Le Node B est un ensemble de stations de base (BS) et de contrôleurs de site qui sont chargés en outre de gérer la macro-diversité (1 mobile ↔ plusieurs nodes B). Chaque station de base gère une cellule.
- **Le RNC :** Le RNC est un contrôleur de Node B et est encore ici l'équivalent du BSC dans le réseau GSM.
- **La carte USIM :** La carte USIM assure la sécurité du terminal et la confidentialité des communications.
- **Le mobile :** Les technologies de l'informatique et des télécommunications se rapprochent par l'intégration de système d'exploitation et d'applications sur les terminaux UMTS.

I.3.4 La quatrième génération des téléphones mobiles 4G (LTE)

La norme LTE (Long Term Evolution), permet le « très haut débit mobile », c'est-à-dire des transmissions de données à des débits théoriques supérieurs à 100 Mbit/s, voir supérieurs à 1 Gbit/s (débit minimum défini par l'UIT pour les spécifications IMT-Advanced pour la norme LTE Advanced). En pratique, les débits sont de l'ordre de quelques dizaines de Mbit/s selon le nombre d'utilisateurs, puisque la bande passante est partagée entre les terminaux actifs des utilisateurs présents dans une même cellule radio.

Une des particularités de la 4G est d'avoir un « cœur de réseau » basé sur IP et de ne plus offrir de mode commuté (établissement d'un circuit pour transmettre un appel « voix »), ce qui signifie que les communications téléphoniques utilisent la voix sur IP (en mode paquet VoIP « Voice Over IP »)

Avec la 4G, on se dirige vers la transmission de toutes les informations « voix et données » par IP, le même protocole qu'on utilise sur Internet. Pour les fournisseurs, c'est plus facile et moins cher à gérer. Ça facilite aussi le développement d'applications multimédias. Cette technologie permet des vitesses de téléchargement plus rapides et des temps de latence plus courts

		LTE	LTE-Advanced
Débits crêtes maximums	DownLink	300 Mb/s	1 Gb/s
	UpLink	75 Mb/s	500 Mb/s
Bandes de fréquence		1.4 à 20 MHz	100 MHz
Latence	Données	10 ms	10 ms (RTT)
	Session	100 ms	50 ms
Efficacité spectrale (DL/UL)	Max	5.0/2.5 b/s/Hz	30/15 b/s/Hz
	Moyen	1.8/0.8 b/s/Hz	2.6/0.2 b/s/Hz
	En limite	0.04/0.02 b/s/Hz	0.009/0.07 b/s/Hz

Tableau I.1 - Différents Paramètres du LTE / LTE-Advanced.

I.4 Généralités sur la 4G

I.4.1 Définition de 4G/LTE

Le réseau 4G (4ème génération) est proposé comme future génération des réseaux de mobiles après la 3G (3ème génération). Ce réseau a également pour objectif d'améliorer la mobilité. Avec le réseau 4G, un utilisateur pourra se connecter où qu'il se trouve : à l'intérieur des bâtiments avec les technologies Bluetooth, UWB ou WiFi…, à l'extérieur (dans la rue et les lieux publics) avec l'UMTS ou le WiMAX. En général, le passage d'un réseau à l'autre deviendra transparent pour l'utilisateur.

Les débits supposés sont entre 20 et 100 Mb/s à longue portée et en situation de mobilité, et 1 Gb/s à courte portée vers des stations fixes. Par définition, la 4G assure la convergence de la 3G avec les réseaux de communication radio fondés sur le protocole IP. La connexion devra être possible quel que soit le mode de couverture.

La définition de la 4G a évolué comme une nouvelle vague d'efforts de données de commercialisation des mobiles qui se déplace le terme dans l'oeil du public à différencier les marques. L'union internationale des télécommunications (UIT), qui supervise le développement de la plupart des normes de données cellulaires, a récemment publié une

déclaration soulignant que la 4G terme n'est pas défini. En réponse, les opérateurs mobiles avec des architectures 3G avancés a commencé la commercialisation des services «4G» .
Les différentes technologies sans fil qui sont représentées, dans la figure I.5.

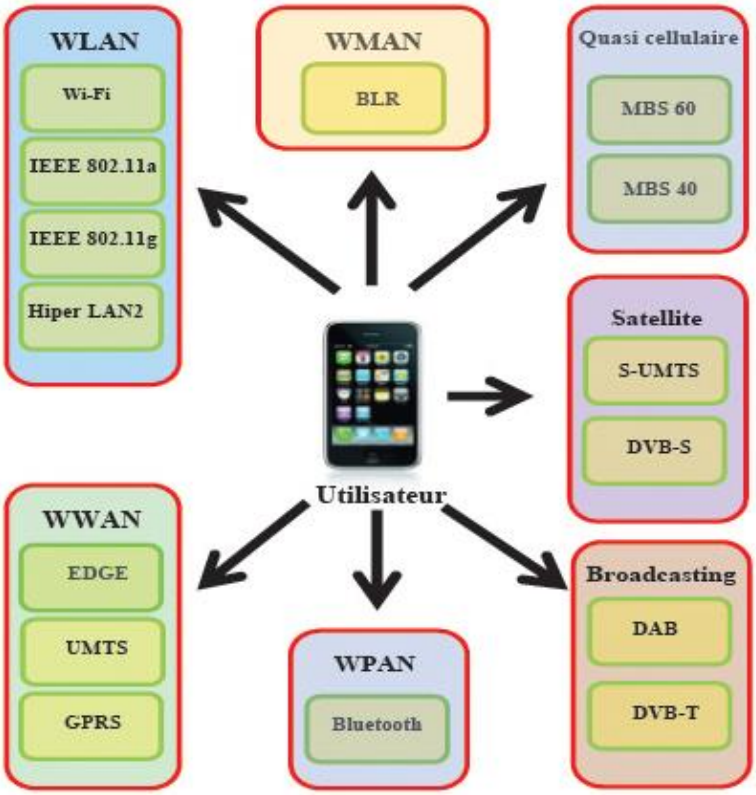

Figure I.5 - Les différentes technologies d'accès sans fil pour l'utilisateur 4G.

I.4.2 Objectifs de la 4G

La 4ème génération vise améliorer l'efficacité spectrale et à augmenter la capacité de gestion du nombre mobiles dans une même cellule. Elle tente aussi d'offrir des débits élevés en situation de mobilité et à offrir une mobilité totale à l'utilisateur en établissant l'interopérabilité entre différentes technologies existantes. Elle vise à rendre le passage entre les réseaux transparents pour l'utilisateur, à éviter l'interruption des services durant le transfert intercellulaire, et à basculer l'utilisation vers le tout-IP. [5]

Les principaux objectifs visés par les réseaux de 4ème génération sont les suivants :

a. Assurer la continuité de la session en cours.
b. Réduire les délais et le trafic de signalisation.
c. Fournir une meilleure qualité de service.

d. Optimiser l'utilisation des ressources.
e. Réduire le délai de relève, le délai de bout-en-bout, la gigue et la perte de paquets.
f. Minimiser le cout de signalisation.

I.4.3 Avantages de la 4G de mobiles

La quatrième génération des réseaux cellulaires est de plus en plus utilisée pour répondre au besoin d'une connectivité flexible et constante, et fournir une solution de secours de basculement pour la continuité des activités dans le cadre des réseaux câblés traditionnels.
Avec la 4G, on se dirige vers la transmission de toutes les informations voix et données par IP, le même protocole qu'on utilise sur Internet. Pour les fournisseurs, c'est plus facile et moins cher à gérer. Ça facilite aussi le développement d'applications multimédias.
Cette génération permet des vitesses de téléchargement plus rapide et des temps de latences plus courts. Selon le critère de l'internationale de télécommunication(UIT), qui établit les normes pour les réseaux cellulaires, le réseau 4G devrait offrir des vitesses de téléchargements de 100 Mbits/s pour un utilisateur en mouvement et de 1 Gbits/s en mode stationnaire.

I.4.4 Architecture de la 4G/LTE

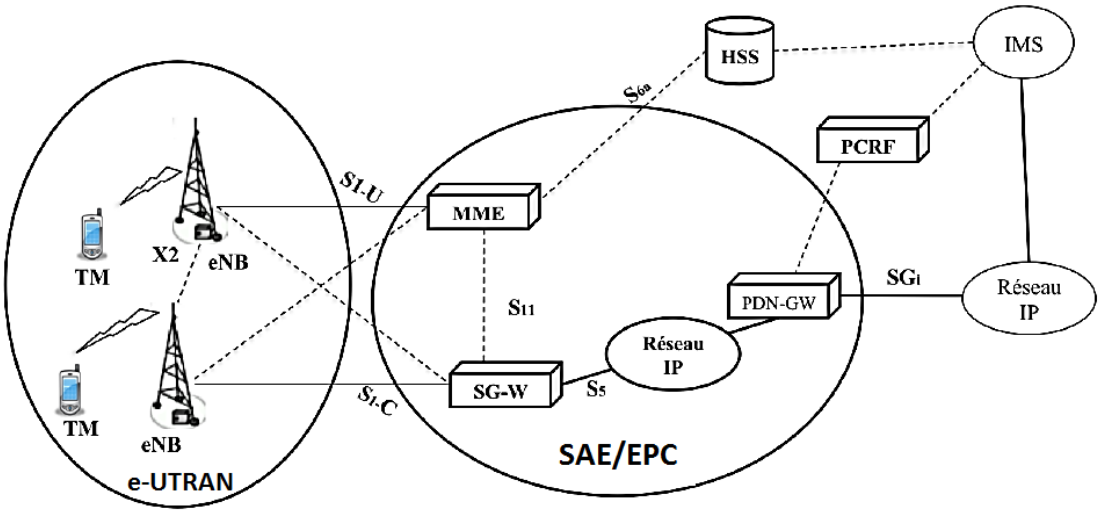

Figure I.6 - Architecture du réseau 4G LTE [6]

La technologie LTE a apporté une efficacité spectrale, une amélioration de débit, une augmentation de couverture et du nombre d'appels supporté par la cellule.

De même que ces précédentes, elle est caractérisée par son architecture connus sous le nom d'EPS (Evolved Packet System), qui comporte :

- L'équipement usager (UE) : il est utilisé pour désigner la station mobile dans un réseau LTE, il représente le vecteur qui permet à l'abonné d'accéder au réseau et également à ses services.
- Un réseau d'accès E-UTRAN : il contient des eNodeB (station de base responsable de la transmission et de la réception radio avec l'UE).
- Un réseau coeur (EPC) : Réseau tout IP.

L'IMS (*IP Multimedia Subsystem*) est une architecture récemment appliquée dans les réseaux mobiles qui permettent aux opérateurs de télécommunications d'offrir des services sur IP à valeur ajoutée.

La Figure I.7 présente une architecture simplifiée de la partie EPS du réseau LTE.

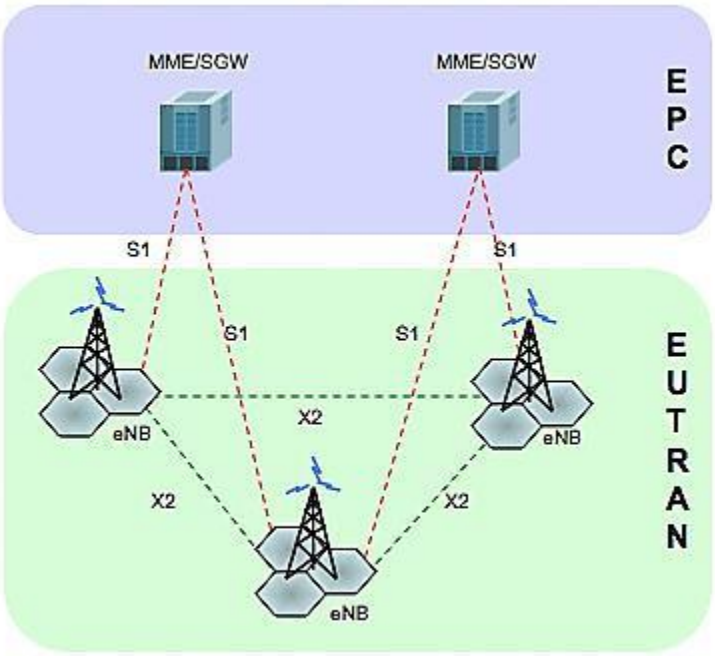

Figure I.7 - Architecture simplifiée d'EPS.

I.4.4.1 UE : User Equipement

C'est l'équipement exploité par l'utilisateur afin d'accéder aux différents services fournis par l'UMTS via l'interface radio UTRA

Le 3GPP (3rd generation partner ship Project) qui gère cette norme, est constamment améliorée, notamment pour augmenter les débits et pouvoir prendre en charge un nombre plus important d'abonnés. Les normes associées à cette génération sont :

• La norme HSDPA (High Speed Downlink Packet Access) : Elle offre des
Performances dix fois supérieures à la 3G, uniquement sur le flux descendent.

• La norme HSUPA (High Speed UplinkPacket Access) : Elle apporte des améliorations uniquement au flux montant.

• La norme HSPA+ (High Speed Packet Access) : nommée H+, 3GPP, est une norme de téléphonie mobile 3G de la famille UMTS ; c'est une évolution de la norme HSPA permettant d'atteindre des débits de : 42Mb/s (montant) et 11Mb/s(descendent).

I.4.4.2 E-UTRAN : Evolved UMTS Terrestrial Radio Access Network Le Réseau d'accès

La partie radio du réseau, appelée « e-UTRAN » est simplifiée par rapport à celles des réseaux 2G et 3G, par l'intégration des fonctions de contrôle dans les stations de base « eNodeB », qui étaient auparavant implémentées dans les RNC (Radio Network Controller) des réseaux 3G UMTS.

La partie radio d'un réseau LTE , se compose donc des eNodeB, d'antennes locales ou distantes, de liaisons en fibres optiques vers les antennes distantes et des liens IP reliant les eNodeB entre eux (liens X2) et avec le cœur de réseau.

a) Les entités du réseau d'accès (e-UTRAN) :

La Figure I.8 décrit l'architecture de l'e-UTRAN avec ses eNodeBs, les interfaces X2 (entre les eNodeBs) et S1 (entre eNodeB et entités du réseau coeur MME/SGW).

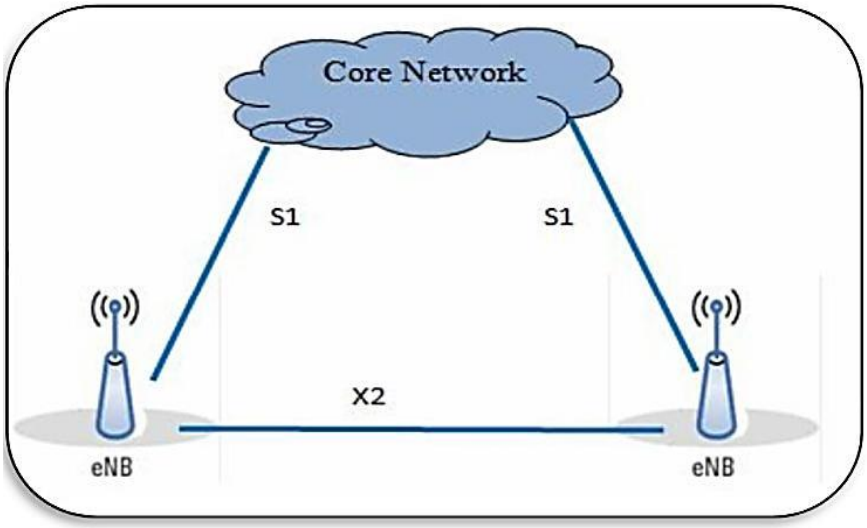

Figure I.8 - Architecture de l'e-UTRAN [7]

- **L'eNodeB :** L'eNodeB est l'équivalent de la BTS dans le réseau GSM et le NodeB dans l'UMTS. La fonctionnalité de *Handover* est plus robuste dans le LTE. Ce sont des antennes qui relient les UE (User Equipment) avec le réseau cœur du LTE via les RF (Radio Frequency) air interface. La fonctionnalité du contrôleur radio réside dans eNodeB, le résultat est plus efficace, et le réseau est moins latent, par exemple la mobilité est déterminée par eNodeB a la place du BSC ou RNC des réseaux GSM et l'UMTS. Les eNodeBs sont reliés entre eux par une interface X2.

- **L'interface X2 :** C'est une interface logique, elle est introduite dans le but de permettre aux eNodeB d'échanger des informations de signalisation durant le *Handover* ou la signalisation, sans faire intervenir le réseau cœur. Lorsque l'usager se déplace en mode ACTIF (Handover) d'un eNodeB à un autre eNodeB, de nouvelles ressources sont allouées sur le nouvel eNodeB pour l'UE ; or le réseau continue à transmettre ses données vers l'ancien eNodeB tant qu'il n'a pas été informé du changement. Afin de minimiser la perte de ses paquets de données, l'ancien eNodeB relaie les paquets entrants sur l'interface X2 au nouvel eNodeB qui les remet à l'UE. L'eNodeB est relié au cœur du réseau à travers l'interface S1.

- **L'interface S1 :** C'est l'interface intermédiaire entre le réseau d'accès et le réseau cœur, elle peut être divisée en deux interfaces élémentaires :

- ✓ S1-U (S1-Usager) entre l'eNodeB et le SGW,
- ✓ S1-C (S1-Contrôle) entre l'eNodeB et le MME.

Les eNodeB ont offert deux qualités au réseau :

- La sécurité : en cas de problème d'un relais.
- Un partage des ressources équitable : partage de ressource en cas de saturation du lien principale [8].

I.4.4.3 EPC (Evolved Packet Core) ou Réseau Cœur

Le cœur de réseau appelé EPC (Evolved Packet Core), utilise des technologies Tout- IP, c'est-à-dire basées sur les protocoles Internet pour la signalisation, le transport de la voix et des données.

Ce cœur de réseau permet l'interconnexion via des routeurs avec les autres eNodeB, les réseaux des autres opérateurs mobiles, les réseaux de téléphonie fixe et le réseau Internet.

Il assure la gestion des utilisateurs, la gestion de la mobilité, la gestion de la qualité de service QoS et la gestion de la sécurité, au moyen des équipements tels que le MME, le SGW, le PDNGW (Packet Data Network Gateway) et le PCRF (*Policy and Charging Rules Function*). [6]

L'utilisation du protocole IP de bout en bout dans le cœur du réseau, permet des temps de latence réduits pour l'accès internet et les appels vocaux LTE. Son architecture est simplifiée, comme montre la Figure I.9, en la comparant à celle de 2G/3G

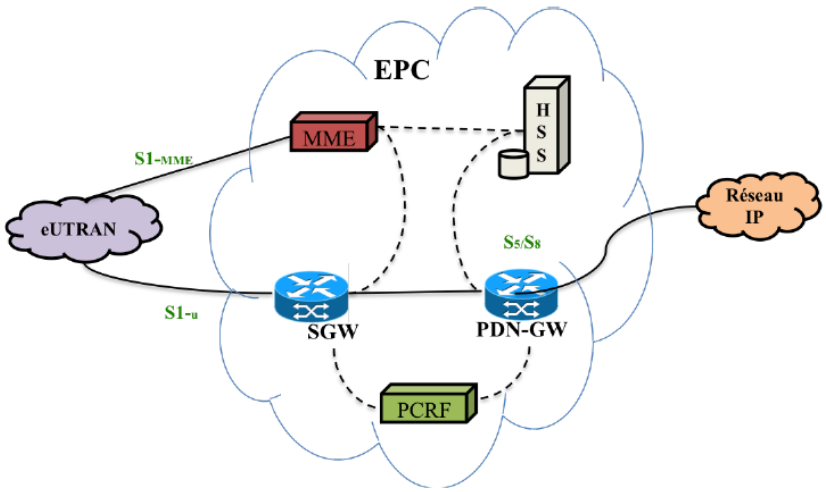

Figure I.9 - Architecture EPC [6]

a) Description et rôles des entités du réseau cœur :

Voici les différentes entités du réseau cœur ainsi que leur rôle :

- **MME : (Mobility Manager Entity) "3GPP Release 8":** C'est une entité de gestion de mobilité, le **MME** c'est le noeud principal de contrôle du réseau d'accès **LTE/SAE**, elle gère toutes les procédures (authentification, chiffrement, mobilité.) des **UE**. Les fonctions de l'entité **MME** incluent :

  - ✓ **Signalisation « EMM » et « ESM » avec l'UE :** Les terminaux LTE disposent des protocoles EMM et ESM qui leur permettent de gérer leur mobilité (attachement, détachement, mise à jour de localisation et leur session (établissement/libération de session de données) respectivement. Ces protocoles sont échangés entre l'UE et le MME.
  - ✓ **Authentification :** Le MME est responsable de l'authentification des UEs à partir des informations recueillies du HSS.
  - ✓ **Gestion de la liste de « Tracking Area » :** L'**UE** est informé des zones de localisation prises en charge par le **MME,** appelées Tracking Area. L'**UE** met à jour sa localisation lorsqu'il se retrouve dans une Tracking Area qui n'est pas prise en charge par son **MME**.
  - ✓ **Sélection du « SGW » et du « PDN GW » :** C'est au **MME** de sélectionner le Serving **GW** et le **PDN GW** qui serviront à mettre en œuvre le Default Bearer au moment du rattachement de l'UE au réseau.
  - ✓ **Sélection du MME lors du Handover avec changement de MME :** Lorsque l'usager est dans l'état ACTIF et qu'il se déplace d'une zone prise en charge par un MME à une autre zone qui est sous le contrôle d'un autre MME, alors il est nécessaire que le Handover implique l'ancien et le nouveau MME.
  - ✓ **Roaming avec interaction avec le HSS nominal :** Lorsque l'usager se rattache au réseau, le MME s'interface au HSS nominal afin de mettre à jour la localisation du mobile et obtenir le profil de l'usager. [9]

- **Le SGW (Serving Gateway) "3GPP Release 8" :** C'est la jonction principale entre le réseau radio accès et le réseau coeur SGW (Serving GateWay). Elle achemine les paquets de données, maintient la connexion de l'inter-eNodeB Handover, puis inter-système Handover entre LTE et GSM/UMTS. L'échange des paquets est acheminé par le SGW au

PDN-GW par l'interface S5. Le SGW est connecté à l'E-UTRAN via l'interface S1-U qui sert de relai entre l'utilisateur et l'EPC.

- **Le P-GW (Packet Data Network Gateway) "3GPP Release8" :** Le P-GW est le nœud qui relie l'utilisateur mobile aux autres réseaux PDN, tels que les réseaux IP, PSTN et NON-3GPP. L'accès aux réseaux IP et PSTN se fait par l'intermédiaire de l'IMS. Le PDN Gateway agit comme un routeur par défaut par lequel transitent les requêtes de l'utilisateur. Il effectue l'allocation d'adresses IP pour chaque Terminal Mobile, le filtrage des paquets pour chaque usager et comptabilise les octets échangés dans la session de ce dernier à des fins de facturation.

- **Le HSS (Home Subscriber Server) :** Le **HSS** se présente comme une version évoluée du **HLR**, il permet de stocker des informations d'abonnement pouvant servir au contrôle des appels et à la gestion de session des utilisateurs réalisé par le **MME**. Il entrepose, pour l'identification des utilisateurs, la numérotation et le profil des services auxquels ils sont abonnés. En plus des données d'authentification des utilisateurs, il contient les informations de souscription pour les autres réseaux, comme le **GSM**, le **GPRS, 3G, LTE** et **IMS**.

- **La PCRF (Policy and Charging Rules Function) "3GPP Release7" :** Le PCRF est une entité qui exécute principalement deux grandes tâches :
  - ✓ La première est de gérer la qualité de service QoS que requiert le réseau et alloue en conséquence les porteuses Bearer appropriées.
  - ✓ La deuxième tâche se rapporte principalement à la tarification.

En effet, le PCRF gère les politiques de facturation qui doivent être prises en compte par le PDN-GW et applicables en fonction des actions de l'utilisateur.

I.4.5 Performances et caractéristiques des réseaux 4G

I.4.5.1 Les Débits

Les objectifs du débit maximale définit pour LTE sont les suivantes :

- 100Mb/s en voie descendante pour une largeur de bande allouée de 20Mhz
- 50Mbit/s en voie montante pour une largeur de bande allouée de 20Mhz

Le débit de la cellule doit être atteignable au moins par 95% des utilisateurs.

I.4.5.2 La latence

C'est la capacité à réagir rapidement à des demandes d'utilisateurs ou de service.
On a deux plans :

- *Latence du plan de contrôle* : Son objectif est d'améliorer la latence du plan de contrôle, par rapports à l'UMTS, avec un temps de transition inferieur à 100ms.
- *Latence du plan usager* : correspond au délai de transmission d'un paquet IP au sein de réseau d'accès. Le réseau LTE vise une latence du plan usager inferieur a 5ms

I.4.5.3 L'agilité en fréquence

Le **LTE** doit pouvoir opérer sur des porteuses des différentes largeurs afin de s'adapter à des allocations spectrales variées. Les largeurs de bande initialement requises ont par la suite été modifiées pour devenir les suivantes : 1,4Mhz, 3Mhz, 5Mhz, 10Mhz, 15Mhz et 20Mhz.
Le codage et la sécurité
L'**OFDMA** (orthogonal frequency division multiple Access) est une technologie de codage radio de type « Accès multiple par répartition en fréquence). L'**OFDMA** et sa variante **SC-FDMA** sont dérivés du codage **OFDM** (utilisé dans l'**ADSL** et **WiFi**), mais contrairement à L'**OFDM**, l'**OFDMA** est optimisé pour l'accès multiple, c'est-à-dire le partage simultané de la ressource spectrale (bande de fréquence) entre plusieurs utilisateurs distants les uns des autres

I.4.5.4 Le multiplexage

Il existe deux modes du multiplexage de fréquences :

- FFD (frequency division duplexing) : L'émission et la réception se font à des fréquences différentes.
- TDD : L'émission et la réception se transitent à une même fréquence, mais à des instants différents.

I.4.5.5 La mobilité

Le réseau LTE doit rester fonctionnel pour des UE qui se déplacent à des vitesses élevées.

I.5 Conclusion

Nous avons présenté dans ce chapitre d'une façon générale les différentes générations de téléphonie mobile ainsi que les principales caractéristiques d'un réseau cellulaire. En commençant par la 1G qui est née dans les années 80. Etant le point de départ de toutes les générations, elle a montré ses limites ce qui a nécessité la naissance de la 2G. Celle-ci est toujours utilisée jusqu'à nos jours, mais étant plus développée que la précédente. Concernant la 3G, elle est venue avec des nouvelles qualités notamment son haut débit pour l'accès à Internet et le transfert de données.

La naissance de la 4G, qui est le successeur évolué de la 3G, montre d'une manière claire que le développement des réseaux augmente considérablement. Nous avons constaté aussi que l'architecture du réseau 4G/LTE permet de faciliter l'évolution du réseau en intégrant des technologies plus performantes, qui leur permettent de fournir en même temps des services de bonne qualité.

En tenant compte du fait que notre projet est plus focalisé sur la sécurité du réseau de la quatrième génération du réseau4G/LTE, nous allons étudier la sécurité dans les réseaux 4G/LTE en profondeur dans le chapitre suivant.

Chapitre II : La sécurité dans les réseaux mobiles 4G

II.1 Introduction

Les réseaux mobiles LTE (Long Term Evolution) offrent des possibilités à la fois riches et nouvelles pour la croissance et le développement commercial et sont actuellement déployés à travers le monde. Ces réseaux LTE mobiles utilisent la commutation complète de paquets et le protocole IP, contrairement aux itérations précédentes du réseau mobile, ce changement de la commutation de circuit à la commutation de paquet permet de nouvelles attaques qui n'étaient pas possibles auparavant.

Certaines implémentations de réseaux LTE et d'applications mobiles sont actuellement vulnérables à plusieurs échelles. Ce qui entraîne une perte de confidentialité, une facturation incorrecte et une falsification de données

Dans ce chapitre nous allons vous présenter les politiques de sécurité utilisée

II.2 Les objectifs de la sécurité

En générale, la sécurité consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

Parmi les objectifs qu'elle vise généralement, on cite :

- Confidentialité des données La confidentialité consiste à refuser l'accès aux informations échangées entre deux nœuds dans le réseau par tout nœud malveillant ou non désiré. Son principe est d'assurer que seuls les acteurs de la transaction sont en mesure de comprendre les données secrètes échangées. Des contrôles d'accès stricts doivent être mis en place pour garantir la confidentialité des données].
- Intégrité des données C'est un service qui garantit que les données échangées n'ont pas été altérées durant leur transit dans le réseau de manière volontaire ou accidentelle contre toute modification ou altération par une personne non autorisée
- L'authentification de l'origine des données Dans un réseau, un adversaire peut facilement injecter des paquets additionnels, ainsi le récepteur doit s'assurer que les données reçues proviennent effectivement de la source supposée pour assurer que la communication entre ces derniers se fais d'une manière authentique
- Disponibilité La disponibilité garantit le fonctionnement en permanence des services et garantit l'accès des usagers à ces services. Son principe permet de s'assurer que les services réseau désirés sont toujours disponibles même à la présence des attaques, le

système qui assure la disponibilité dans un réseau cherche à combattre les dénis de service et les nœuds qui se comportent mal tels que les nœuds égoïstes

- Le non répudiation de l'origine C'est un mécanisme destiné à prévenir que la source ou la destination désavoue ses actions ou nier l'envoi ou bien la réception d'un message
- La fraîcheur de données Garantir que les données présentes échangées sur le réseau sont viables. Ce service permet de lutter contre la réinjection d'anciens messages interceptés par un attaquant et de garantir que les données échangées sur le réseau sont actuelles

Les objectifs des dispositifs de sécurité présentés ci-dessus peuvent être résumés comme suit :

- Assurer la sécurité de l'utilisateur vers le réseau : en protégeant l'identité de l'utilisateur et la confidentialité du périphérique, ainsi que l'authentification de l'entité, ce qui peut être obtenu à l'aide d'une identification et d'un chiffrement temporaires. En tant que protocole d'authentification, la procédure EPS AKA est utilisée dans les réseaux LTE pour une authentification mutuelle entre utilisateurs et réseaux.
- Assurer la confidentialité des données utilisateur et des données de signalisation : en fournissant un algorithme de cryptage et un chiffrement à la signalisation RRC afin d'empêcher le suivi de l'UE.
- Assurer l'intégrité des données utilisateur et des données de signalisation : en protégeant l'intégrité de l'authentification d'origine des données de signalisation et en assurant l'authentification du réseau par l'UE.

II.3 Les attaques dans les réseaux 4G

Le réseau mobile est un environnement hostile qui est soumis à des attaques de différents types et dû à la nature du réseau et ses spécificités la sécurité présente un véritable dé.
Un attaquant peut effectuer une variété d'attaques n'ayant pas forcément le même objectif ou motivations. Ainsi le choix d'une stratégie de sécurité doit se baser sur une modélisation de l'attaque, ceci d'éviter un déploiement excessif de moyens de protection conduisant à des solutions irréalistes

II.3.1 Les scénarios d’attaques

Les attaques sont classifiées selon plusieurs critères, Ceci est illustré dans la figure suivante

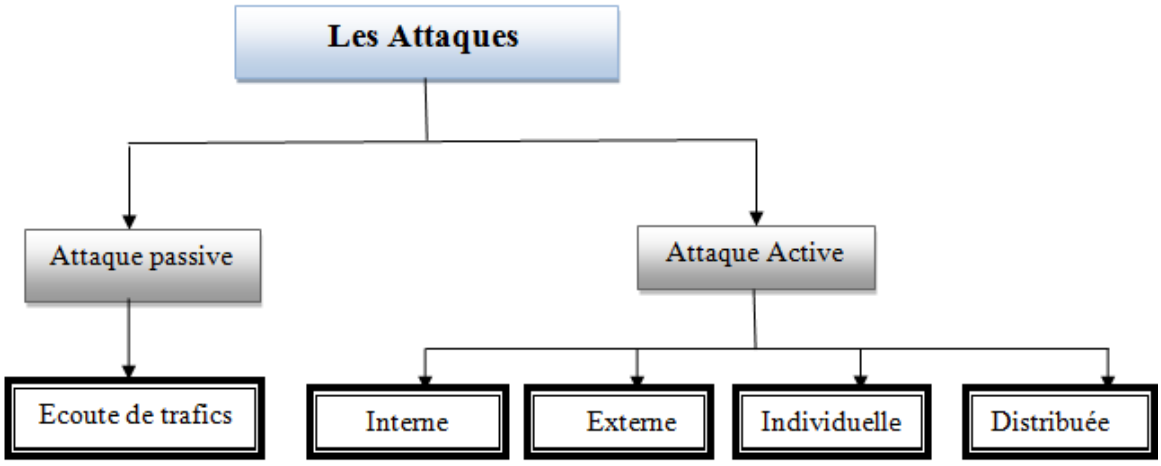

Figure II.1 - Classifications des attaques dans les réseaux

II.3.1.1 Attaque Passive

Les attaques passives se limitent à l'écoute et l'analyse du trafic échangé, une écoute se produit lorsqu'un attaquant capture un nœud et étudie le trafic qui le traverse sans en altérer le fonctionnement.

Ce type d'attaques est plus facile à réaliser et difficile à détecter puisque l'intrus n'apporte aucune modification sur les informations échangées.

L'intention de l'intrus peut être la connaissance des informations confidentielles des utilisateurs ou bien la connaissance des nœuds importants dans le réseau, en analysant les informations de routage, pour se préparer à une attaque active. Un adversaire passif ne fait que menacer la confidentialité des données.

II.3.1.2 Attaque active

Une attaque est active lorsqu'un nœud non autorisé altère des informations de routage en transit par des actions de modification, suppression, ou fabrication, ce qui conduit à des perturbations dans le fonctionnement du réseau. L'intrus peut aussi injecter son propre trafic ou rejouer d'anciens messages pour perturber le fonctionnement du réseau ou provoquer un déni de service. [10]

3

a. Catégories des attaques active

Selon le domaine d'appartenance d'un nœud, les attaques actives peuvent elles-mêmes être classées en deux catégories, à savoir les attaques externes et internes.

- **Attaque Interne** : Les attaquants internes sont des nœuds faisant légitimement partie du réseau, sont considérée comme la plus dangereuse du point de vue sécurité et menées par des noeuds compromis qui sont autorisés à participer au fonctionnement du réseau.

  Puisque l'attaquant qui capture un nœud, peut lire sa mémoire et avoir accès à son matériel et par conséquent peut s'authentifier comme un nœud légitime et émettre des messages aléatoires erronés sans qu'il soit identifié comme intrus, puisqu'il utilise des clés valides
- **Attaque Externe** : Les attaquants externes sont réalisés par des nœuds qui n'appartiennent pas au domaine du réseau, seuls les nœuds ayant les autorisations nécessaires pourront accéder au réseau ou déchiffrer le contenu.

Etant donné que les attaquants font d'ores et déjà partie du réseau de noeuds autorisés, les attaques internes sont généralement plus pernicieuses et di ciles à détecter que les attaques externes

Attaque individuelle ou attaque distribuée : Les attaques peuvent être de type individuelles ou par collusion ou appelée également distribuée

- **Attaque individuelle** : Les attaques individuelles sont menées par un seul nœud attaquant. Puisque les capacités de communication et de calcul de l'attaquant sont en général similaires à celles des autres nœuds du réseau, ces attaques demeurent relative- ment simples, et sont d'autant plus limitées que des mécanismes de sécurité sont mis en œuvre

- **Attaque Distribuée** : Attaques distribuées issues de plusieurs nœuds répartis à différents endroits dans le réseau, sont généralement plus évoluées et plus dangereuses. Par ailleurs, en raison de l'intervention de plusieurs nœuds intermédiaires, leur détection et l'identification précise de leur origine sont rendues plus complexes

b. Les cas possibles dans une attaque active

Il y a trois cas possible pour mener une attaque active :

• L'interruption : L'intrus intercepte le message envoyé par l'utilisateur A pour B et l'interrompt, ceci illustré par la figure II..2 :

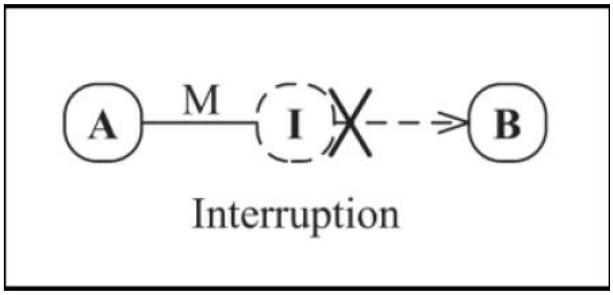

Figure II.2 – L'interruption.

• La modification : L'intrus intercepte le message envoyé par l'utilisateur A et le modifie avant de le faire suivre à l'utilisateur B, ceci présenté par la figure II.3 :

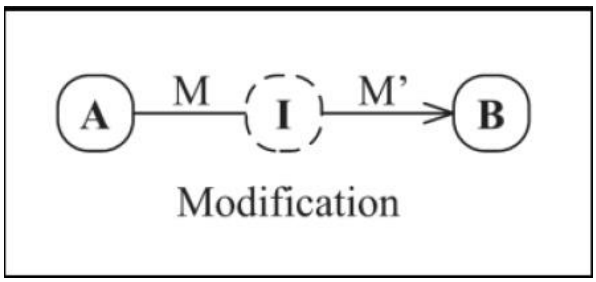

Figure II.3 – La modification.

• La fabrication : L'intrus fabrique un message et l'envoie à l'utilisateur B en se passant pour l'utilisateur A, ceci exposé par la figure II.4 :

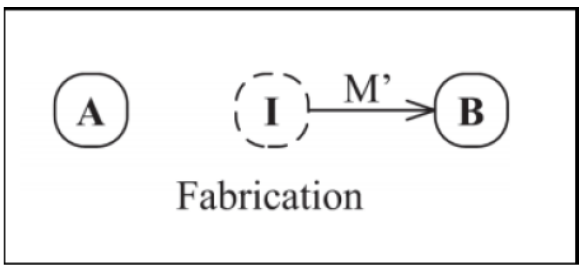

Figure II.4 – La fabrication

II.3.2 Description de quelques attaques

La présence des failles et de plusieurs outils d'attaque a mis les réseaux en un grand risque
Les attaques touchent généralement les trois composants suivant d'un système : la couche réseau, le système d'exploitation et la couche application.
De plus, beaucoup d'attaques peuvent infecter le réseau, On cite quelques-unes

II.3.2.1 Attaque par déni de service (DoS)

L'attaque par déni de service, ou DoS (Denial of Service), vise à perturber, ou paralyser totalement, le fonctionnement d'un service ou d'un réseaux complet en le bombardant à outrance de requêtes erronées et en saturant une des ressources du système dans le but de le rendre indisponible pendant un temps indéterminé De ce fait, les utilisateurs ne peuvent plus accéder aux ressources. [11]

Les deux exemples principaux sont : le « ping flood » ou l'envoi massif de courrier électronique pour saturer une boîte aux lettres (mailbombing). La meilleure parade est le firewall ou la répartition des serveurs sur un réseau sécurisé .

II.3.2.2 Écoute du réseau (sniffer)

Un sniffer est un formidable outil permettant d'étudier le trafic d'un réseau, mais malheureusement, comme tous les outils d'administration, le sniffer peut également servir à une personne malveillante ayant un accès physique au réseau pour collecter des informations.
Il existe des logiciels qui permettent d'intercepter certaines informations qui transitent sur un réseau local, en transcrivant les trames dans un format plus lisible (Network packet sniffing). C'est l'une des raisons qui font que la topologie en étoile autour d'un hub n'est pas la plus sécurisée, puisque les trames qui sont émises en «broadcast» sur le réseau local peuvent être interceptées. De plus, l'utilisateur n'a aucun moyen de savoir qu'un pirate a mis son réseau en écoute.
La meilleure solution est l'utilisation de mot de passe redoutable, de carte à puce ou de calculette à mot de passe. [12]

II.3.2.3 Intrusion

En exploitant un réseau internet ou intranet, il est tout à fait possible de consulter le disque dur d'un ordinateur distant, voir d'agir sur le contenu de celui-ci. Des logiciels sont précisément

conçus pour effectuer ce genre de manipulation, à la condition que les ordinateurs distants soient équipés de petits programme chargés d'établir la liaison avec l'ordinateur pilote. Mais quelques spécialistes sont capables des mêmes effets et résultats en utilisant des programmes plus confidentiels

Le principal moyen pour prévenir les intrusions est le pare-feu (Firewall en anglais). Il est efficace contre les fréquentes attaques de pirates amateurs, mais d'une efficacité toute relative contre des pirates expérimentés et bien informés, une politique de gestion des accès et des mots de passe est complémentaire [13].

II.3.2.4 Cheval de Troie

A la façon du virus, le cheval de Troie est un code (programme) nuisible placé dans un programme sain (imaginez une fausse commande de listage des fichiers, qui détruit les fichiers au-lieu d'en afficher la liste).

Un cheval de Troie peut par exemple :

- Voler des mots de passe
- Copier des données sensibles
- Exécuter tout autre action nuisible

Pire, un tel programme peut créer, de l'intérieur de votre réseau, une brèche volontaire dans la sécurité pour autoriser des accès à des parties protégées du réseau à des personnes se connectant de l'extérieur.

Pour se protéger de ce genre d'intrusion, il suffit d'installer un firewall, c'est-à-dire un programme filtrant les communications entrant et sortant de votre machine de sécuriser au maximum l'accès à votre machine et de mettre en service un antivirus régulièrement mis à jour. Un nettoyeur de troyens peut aussi s'avérer utile.

II.3.2.5 Man in middle

L'attaque « man in the middle » parfois notée MITM désigne un modèle de cyberattaque dans lequel un cybercriminel installe, physiquement ou logiquement, un système contrôlé entre le système de la victime et une ressource Internet qu'elle utilise. L'objectif de l'attaquant est d'intercepter, de lire ou de manipuler toute communication entre la victime et sa ressource sans se faire remarquer.

En règle générale, il est difficile pour les personnes concernées de reconnaître la présence d'une attaque d'homme au milieu. La meilleure protection est donc la prévention

II.3.2.6 L'attaque IP spoofing

L'IP spoofing est une méthode de hacking ou les paquets de données TCP/IP ou UDP/IP sont envoyés avec une adresse expéditeur usurpée. Ainsi l'attaquant accède et utilise une adresse d'un système autorisé et de confiance. De cette façon, il peut injecter ses propres paquets de données dans un autre système, qui autrement serait bloqué par un système de filtrage. Dans la plupart des cas, l'usurpation d'adresse IP est utilisée pour effectuer des attaques DoS et DDoS. Dans certaines circonstances, l'attaquant avec une adresse IP volée ou manipulée peut même intercepter le trafic entre deux ou plusieurs systèmes informatiques. Des attaques de « l'homme du milieu » qui utilisent la technique de l'IP spoofing nécessitent cependant (sauf pour quelques cas exceptionnels) que l'attaquant soit sur le même sous-réseau que la victime [14].

II.4 Mise en place d'une politique de sécurité

La définition et l'application d'une politique de sécurité représente le cœur de la sécurité d'un système d'information.

Une politique de sécurité définit un ensemble des propriétés de sécurité, chaque propriété représentant un ensemble de conditions que le système doit respecter pour rester dans un état considéré comme sûr. Une définition incorrecte ou l'application partielle d'une politique peut entraîner le système dans

- un état non-sûr
- autorisant le vol d'informations ou de ressources
- la modification d'informations
- la destruction du système.

Dans cette section, nous donnons une définition générale des propriétés de sécurité, d'une politique de sécurité et des mécanismes utilisés pour l'application d'une politique.

La définition et l'application d'une politique de sécurité représente le cœur de la sécurité d'un système d'information.

Une politique de sécurité définit un ensemble des propriétés de sécurité, chaque propriété représentant un ensemble de conditions que le système doit respecter pour rester dans un état

considéré comme sûr. Une définition incorrecte ou l'application partielle d'une politique peut entraîner le système dans

- Un état non-sûr
- Autorisant le vol d'informations ou de ressources
- La modification d'informations
- La destruction du système.

II.4.1 La sécurité dans les entreprises

L'application correcte des politiques de sécurité d'entreprise dans un environnement de réseau étendu est une tâche difficile pour les administrateurs réseau. Une grande partie de l'application de la politique de sécurité au niveau du réseau consiste à configurer les stratégies de classification des paquets

Et pour cela la sécurité des systèmes d'information repose sur trois propriétés fondamentales : la confidentialité, l'intégrité et la disponibilité

- **La confidentialité** : assurer qu'une information n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.
- **L'Intégrité** : assurer que l'information contenue dans les objets n'est ni créée, ni altérée, ni détruite de manière non autorisée.
- **La Disponibilité** : assurer qu'un objet est accessible et utilisable sur demande par une entité autorisée.
- **L'Utilisation légitime** : assurer que les ressources ne sont pas utilisées par des personnes non autorisées ou de manière non autorisée.
- **La traçabilité et la transparence des traitements** : Il s'agit de journalier et de suivre les actions et traitements de données afin de pouvoir détecter et dans la mesure du possible, prévenir que la confidentialité, l'intégralité ou la disponibilité soient compromises.

II.5 Détermination des moyens nécessaires

Les mécanismes de sécurité sont employés pour mettre en application les règles indiquées dans la politique de sécurité. Ils peuvent être divisés en trois classes :

- Mécanismes de prévention : Un mécanisme de prévention est un mécanisme qui empêche une violation de sécurité de se produire avant l'exécution d'un système
- Mécanismes de Détection : Un mécanisme de détection est employé pour détecter les tentatives de violation de la sécurité et les violations réussies de sécurité, pendant ou après qu'elles se soient produites dans un système.
- Mécanismes de recouvrement : Un mécanisme de recouvrement est un mécanisme utilisé pour restaurer l'état d'avant la violation de la sécurité.

L'entreprise doit réfléchir aux moyens de parvenir aux objectifs fixés, tout en maintenant les coûts engagés pour sa protection à un niveau raisonnable. Cela peut passer par la mise en place de diverses mesures :

- Un pare-feu, un réseau virtuel privé (VPN) et un contrôle d'accès au réseau interne avec des profils protégés par mots de passe.
- Des supports ou des serveurs de sauvegarde stockés sur place ou chez un prestataire et un dispositif de protection pour l'accès aux données sauvegardées.
- Un système d'alimentation électrique secondaire (sans coupure) capable de fournir une réserve de quelques minutes, pour mémoriser tous les documents cruciaux

II.6 Développement des procédures adaptées

II.6.1 Un pare-feu

Un pare-feu (appelé aussi coupe-feu, garde-barrière ou firewall en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

- Une interface pour le réseau à protéger (réseau interne) ;
- Une interface pour le réseau externe.

Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs

réseaux externes. Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel système pourvu que :

- La machine soit suffisamment puissante pour traiter le traffic.
- Le système soit sécurisé.
- Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur.

Dans le cas où le système pare-feu est fourni dans une boîte noire « clé en main », on utilise le terme d'« appliance ».

II.6.1.1 Fonctionnement d'un système pare-feu

Un système pare-feu contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (allow) ;
- De bloquer la connexion (deny) ;
- De rejeter la demande de connexion sans avertir l'émetteur (drop).

a. Le filtrage simple de paquets

Un système pare-feu fonctionne sur le principe du filtrage simple de paquets (en anglais « stateless packet filtering »). Il analyse les en-têtes de chaque paquet de données (datagramme) échangé entre une machine du réseau interne et une machine extérieure [14].

Ainsi, les paquets de données échangée entre une machine du réseau extérieur et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants, systématiquement analysés par le firewall :

- Adresse IP de la machine émettrice ;
- Adresse IP de la machine réceptrice ;
- Type de paquet (TCP, UDP, etc.) ;
- Numéro de port (rappel: un port est un numéro associé à un service ou une application réseau).

Les adresses IP contenues dans les paquets permettent d'identifier la machine émettrice et la machine cible, tandis que le type de paquet et le numéro de port donnent une indication sur le type de service utilisé.

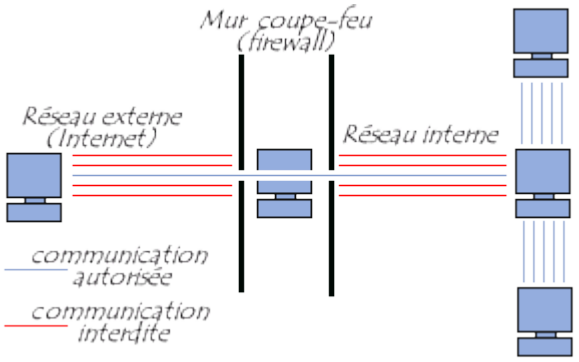

Figure II.5 – Architecture pare-feu

b. Le filtrage dynamique

Le filtrage simple de paquets ne s'attache qu'à examiner les paquets IP indépendamment les uns des autres, ce qui correspond au niveau 3 du modèle OSI. Or, la plupart des connexions reposent sur le protocole TCP, qui gère la notion de session, afin d'assurer le bon déroulement des échanges. D'autre part, de nombreux services (le FTP par exemple) initient une connexion sur un port statique, mais ouvrent dynamiquement (c'est-à-dire de manière aléatoire) un port afin d'établir une session entre la machine faisant office de serveur et la machine cliente.

Ainsi, il est impossible avec un filtrage simple de paquets de prévoir les ports à laisser passer ou à interdire. Pour y remédier, le système de filtrage dynamique de paquets est basé sur l'inspection des couches 3 et 4 du modèle OSI, permettant d'effectuer un suivi des transactions entre le client et le serveur. Le terme anglo-saxon est « stateful inspection » ou « stateful packet filtering », traduisez « filtrage de paquets avec état » [14].

c. Le filtrage applicatif

Le filtrage applicatif permet de filtrer les communications application par application. Le filtrage applicatif opère donc au niveau 7 (couche application) du modèle OSI, contrairement au filtrage de paquets simple (niveau 4). Le filtrage applicatif suppose donc une connaissance des protocoles utilisés par chaque application.

Le filtrage applicatif permet, comme son nom l'indique, de filtrer les communications application par application. Le filtrage applicatif suppose donc une bonne connaissance des applications présentes sur le réseau, et notamment de la manière dont elle structure les données échangées (ports, etc.).

Enfin, un tel système peut potentiellement comporter une vulnérabilité dans la mesure où il interprète les requêtes qui transitent par son biais. Ainsi, il est recommandé de dissocier le pare-feu (dynamique ou non) du proxy, afin de limiter les risques de compromission.

II.6.2 Zone démilitarisée (DMZ)

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, un serveur de messagerie, un serveur FTP public, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise. On parle ainsi de « zone démilitarisé » (notée DMZ pour DeMilitarized Zone) pour désigner cette zone isolée hébergeant des applications mises à disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile [14].

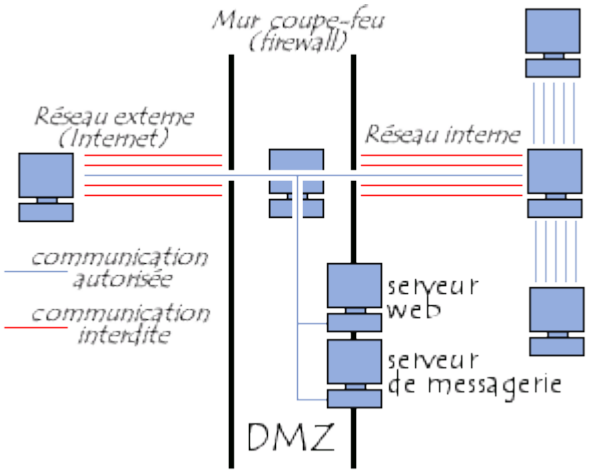

Figure II.6 – Architecture DMZ

Les serveurs situés dans la DMZ sont appelés « **bastions** » en raison de leur position d'avant-poste dans le réseau de l'entreprise.

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

- Traffic du réseau externe vers la DMZ **autorisé** ;
- Traffic du réseau externe vers le réseau interne **interdit** ;
- Traffic du réseau interne vers la DMZ **autorisé** ;
- Traffic du réseau interne vers le réseau externe **autorisé** ;
- Traffic de la DMZ vers le réseau interne **interdit** ;
- Traffic de la DMZ vers le réseau externe **refusé**.

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques pour l'entreprise.

Il est à noter qu'il est possible de mettre en place des DMZ en interne afin de cloisonner le réseau interne selon différents niveaux de protection et ainsi éviter les intrusions venant de l'intérieur.

II.6.3 Réseau Privé Virtuel (VPN)

Un réseau privé virtuel repose sur un protocole, appelé protocole de tunnelisation (tunneling), c'est-à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie. [14]

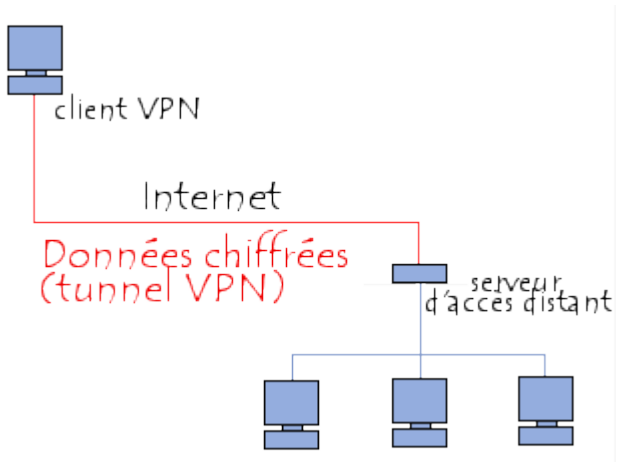

Figure II.7 – Architecture d'un VPN

Le terme de "tunnel" est utilisé pour symboliser le fait qu'entre l'entrée et la sortie du VPN les données sont chiffrées (cryptées) et donc incompréhensible pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. Dans le cas d'un VPN établi entre deux machines, on appelle client VPN l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client) et serveur VPN (ou plus généralement serveur d'accès distant) l'élément chiffrant et déchiffrant les données du côté de l'organisation.

De cette façon, lorsqu'un utilisateur nécessite d'accéder au réseau privé virtuel, sa requête va être transmise en clair au système passerelle, qui va se connecter au réseau distant par l'intermédiaire d'une infrastructure de réseau public, puis va transmettre la requête de façon chiffrée. L'ordinateur distant va alors fournir les données au serveur VPN de son réseau local qui va transmettre la réponse de façon chiffrée. A réception sur le client VPN de l'utilisateur, les données seront déchiffrées, puis transmises à l'utilisateur [14].

II.6.4 La cryptographie

Le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique. Le verbe crypter est parfois utilisé mais on lui préfèrera le verbe chiffrer.

La cryptologie est essentiellement basée sur l'arithmétique : Il s'agit dans le cas d'un texte de transformer les lettres qui composent le message en une succession de chiffres (sous forme de bits dans le cas de l'informatique car le fonctionnement des ordinateurs est basé sur le binaire), puis ensuite de faire des calculs sur ces chiffres pour :

- D’une part les modifier de telle façon à les rendre incompréhensibles. Le résultat de cette modification (le message chiffré) est appelé cryptogramme (en anglais ciphertext) par opposition au message initial, appelé message en clair (en anglais plaintext)
- Faire en sorte que le destinataire saura les déchiffrer.

Le fait de coder un message de telle façon à le rendre secret s'appelle chiffrement. La méthode inverse, consistant à retrouver le message original, est appelée déchiffrement [14].

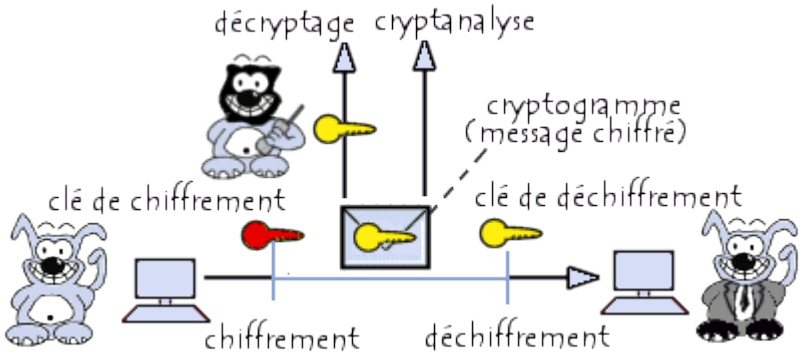

Figure 2.8 – Architecture de la cryptographie

Le chiffrement se fait généralement à l'aide d'une clef de chiffrement, le déchiffrement nécessite quant à lui une clef de déchiffrement. On distingue généralement deux types de clefs :

- Les clés symétriques : il s'agit de clés utilisées pour le chiffrement ainsi que pour le déchiffrement. On parle alors de chiffrement symétrique ou de chiffrement à clé secrète.
- Les clés asymétriques : il s'agit de clés utilisées dans le cas du chiffrement asymétrique (aussi appelé chiffrement à clé publique). Dans ce cas, une clé différente est utilisée pour le chiffrement et pour le déchiffrement.

II.6.5 Secure Shell (SSH)

Le protocole SSH (Secure Shell) a été mis au point en 1995 par le Finlandais Tatu Ylönen.

Il s'agit d'un protocole permettant à un client (un utilisateur ou bien même une machine) d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée :

Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.

Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (spoofing).

SSH est un protocole, c'est-à-dire une méthode standard permettant à des machines d'établir une communication sécurisée. A ce titre, il existe de nombreuses implémentations de clients et de serveurs SSH. Certains sont payants, d'autres sont gratuits ou open source [14].

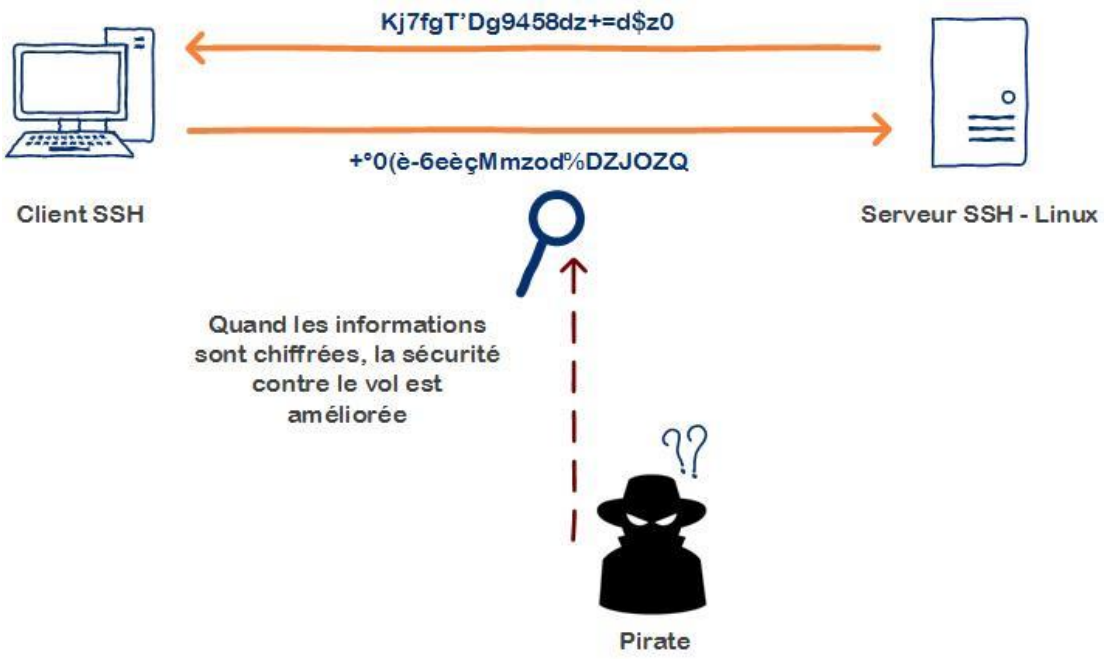

Figure II.9 – Architecture SSH

L'établissement d'une connexion SSH se fait en plusieurs étapes :

- Dans un premier temps le serveur et le client s'identifient mutuellement afin de mettre en place un canal sécurisé (couche de transport sécurisée).
- Dans un second temps le client s'authentifie auprès du serveur pour obtenir une session.

Le protocole SSH s'agit d'un protocole permettant à un client (un utilisateur ou bien même une machine) d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée :

Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.

Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (spoofing).

II.6.6 Réseau Local Virtuel (VLAN)

Un VLAN (Virtual Local Area Network ou Virtual LAN, en français Réseau Local Virtuel) est un réseau local regroupant un ensemble de machines de façon logique et non physique.

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

II.6.6.1 Typologie de VLAN

Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue :

- Un VLAN de niveau 1 (aussi appelés VLAN par port, en anglais Port-Based VLAN) définit un réseau virtuel en fonction des ports de raccordement sur le commutateur ;
- Un VLAN de niveau 2 (également appelé VLAN MAC, VLAN par adresse IEEE ou en anglais MAC Address-Based VLAN) consiste à définir un réseau virtuel en fonction des adresses MAC des stations. Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station ;
- Un VLAN de niveau 3 : on distingue plusieurs types de VLAN de niveau 3 :
- Le VLAN par sous-réseau (en anglais Network Address-Based VLAN) associe des sous-réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifient automatiquement en cas de déplacement d'une station. En contrepartie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.
- Le VLAN par protocole (en anglais Protocol-Based VLAN) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.

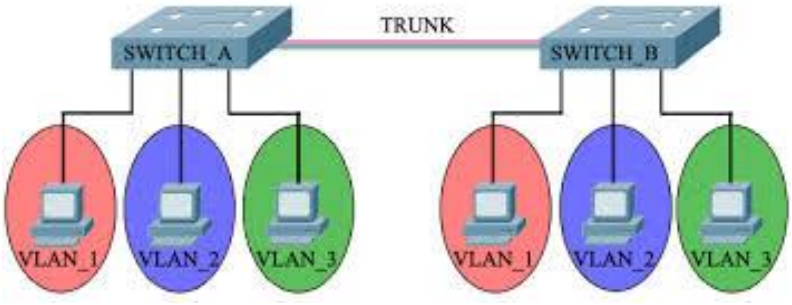

Figure II.10 – Exemple VLAN

II.6.6.2 Les avantages du VLAN

Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants :

- Plus de souplesse pour l'administration et les modifications du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs.
- Gain en sécurité car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées.
- Réduction de la diffusion du trafic sur le réseau

II.7 Conclusion

Dans un monde où le progrès technologique avance à grande vitesse, où les gens, les entreprises, les organismes, les pays et même les objets sont de plus en plus connectés, les attaques informatiques sont de plus en plus fréquentes. La question de la cyber sécurité se pose à tous les niveaux et tend à devenir un enjeu essentiel ces prochaines années.

Il existe au moins des millions de failles dans le monde informatique, et encore plus de manières de les exploiter. Même si certaines sont tellement particulières qu'il est difficile de les qualifier avec des termes génériques, la plupart se rangent dans des catégories précises.

On peut donc en déduire que la sécurité informatique avance grâce au piratage. Les deux sont liés, donc un jour, peut-être que la sécurité contrera le piratage mais pour le moment, le piratage est omniprésent alors que la sécurité l'est peu.

Ce qui nous intéresse le plus c'est les réseaux 4G(LTE), c'est pour cela qu'on va consacrer le chapitre suivant pour présenter notre proposition de la sécurisation d'un réseau 4G

Chapitre III : Simulations et résultats

III.1 Introduction

Dans le chapitre précédent diverses solutions ont été proposées pour la sécurisations du réseau 4G (LTE) contre les attaques. L'objectif principal de ce chapitre est de présenté notre solution pour la sécurisation des données transmises.

Les simulateurs du réseau offrent beaucoup d'économie, de temps et d'argent pour l'accomplissement des tâches de simulation et sont également utilisés pour que les concepteurs des réseaux puissent tester les nouveaux protocoles ou modifier les protocoles déjà existants d'une manière contrôlée et productrice.
Nous présentons dans ce qui suit le déroulement des étapes de simulation que nous avons mené dans ce travail de fin d'études.

III.2 Présentation du simulateur Cisco « Packet Tracer »

Packet Tracer est un logiciel de CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc . . .

Une fois que vous ouvrer CISCO Packet tracer, l'interface suivante s'afficher :

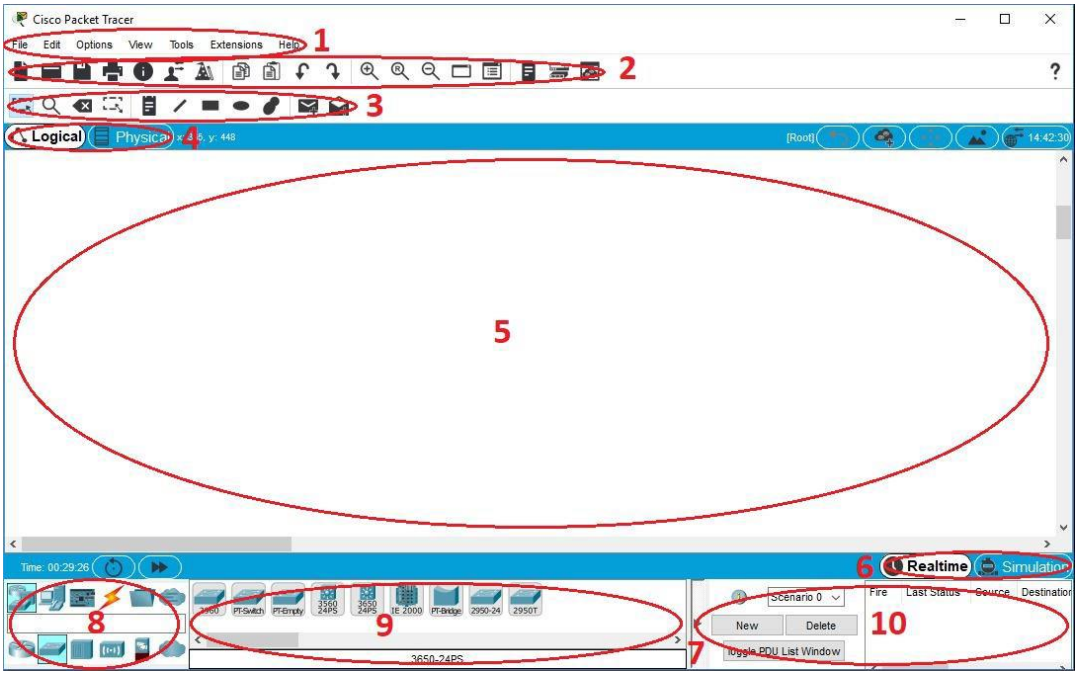

Figure III .1 - La fenêtre de Packet Tracer

(1) : Barre de menu classique

(2) : Barre d'outils principale

(3) : Barre d'outils communs, permet l'accès aux outils d'espace de travail couramment utilisés.

(4) : Espace de travail logique / physique et barre de navigation qui nous a permet de basculer entre l'espace de travail physique et l'espace de travail logique avec les onglets de cette barre. Dans Logical Workspace, cette barre vous permet également de revenir à un niveau précédent dans un cluster, de créer un nouveau cluster, de déplacer l'objet, de définir l'arrière-plan en mosaïque et de la fenêtre d'affichage.

Dans l'espace de travail physique, cette barre vous permet de naviguer dans des emplacements physiques, de créer une nouvelle ville, de créer un nouveau bâtiment, de créer un nouveau placard, de déplacer un objet, d'appliquer une grille à l'arrière-plan, de définir l'arrière-plan et d'accéder au placard de travail.

(5) : Espace de travail qui nous a permet de créer notre réseau, regarder des simulations et afficher de nombreux types d'informations et de statistiques.

(6) : mode réel time /simulation

(7) : Zone des composants réseau, cette zone est l'endroit où vous choisissez les périphériques et les connexions à placer dans l'espace de travail. Elle contient un champ consultable qui vous permet d'entrer un nom d'appareil pour rechercher rapidement cet appareil spécifique. Le nom du périphérique s'affiche lorsque vous passez la souris sur l'icône du périphérique dans la zone spécifique au périphérique.

(8) : Zone de sélection du type de périphérique, cette dernière contient le type de périphériques et les connexions disponibles.

(9) : Zone de sélection spécifique au périphérique

(10) : Fenêtre de paquet permet la gestion des paquets dans les scénarios de simulation.

III.3 Présentation de l'architecture réseau avant la configuration

La figure (Figure **III .2**) illustre notre architecture réseau que nous avons réalisé.

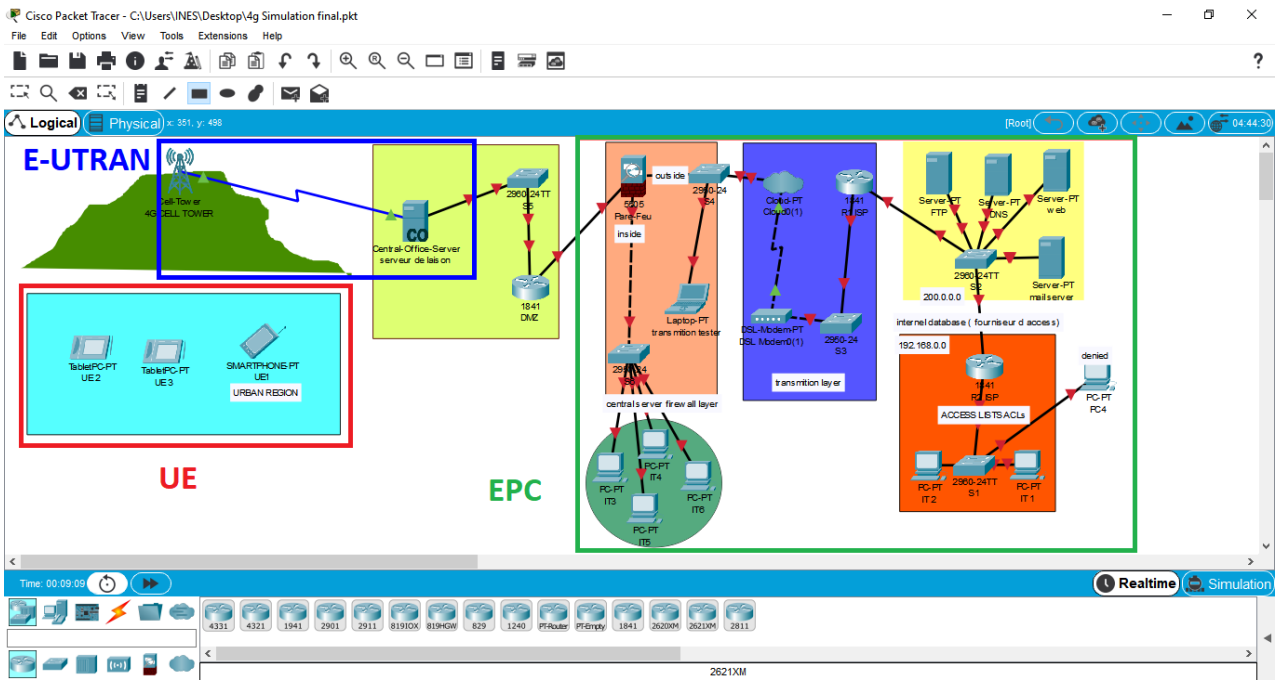

Figure III .2 - L'architecture réseau avant la configuration

1. **UE :** Présente l'équipement utilisateur (Smartphone, Tablette …)
2. **E-UTRAN :** Responsable de la transmission et de la réception radio avec l'UE.
3. **EPC :** présente le réseau local (Le fournisseur d'accès) le réseau extérieur ou tous les échangent ce font par IP.

III.4 Configuration des équipements

La configuration des équipements du réseau sera faite au niveau des commutateurs, et au niveau des routeurs ainsi qu'au niveau des PCs et serveurs. En effet, une série de configuration sera réalisée sur ces équipements, en montrant des exemples de chaque configuration.

III.4.1 Configuration des commutateurs

Pour la configuration des commutateurs on commence par les hostnames et les mots de passe. Le but de cette configuration est de renommer les commutateurs par des noms significatifs comme le montre la (**Figure III .3**). Nous avons choisi "0101IDAM" comme mot de passe via la console.

Nous prendrons comme exemple de configuration le commutateur S1.

Pour protéger les périphériques contre les accès non autorisés aux fichiers de configuration

On utilise la commande « enable secret » pour encodé notre mot de passe, nous avons choisi «2020 » et on chiffre les mots de passes en utilisant la commande « service password-encryption »

Pour rendre notre mot de passe beaucoup plus sécuriser.

La même chose sera faite pour tous les autres switchs.

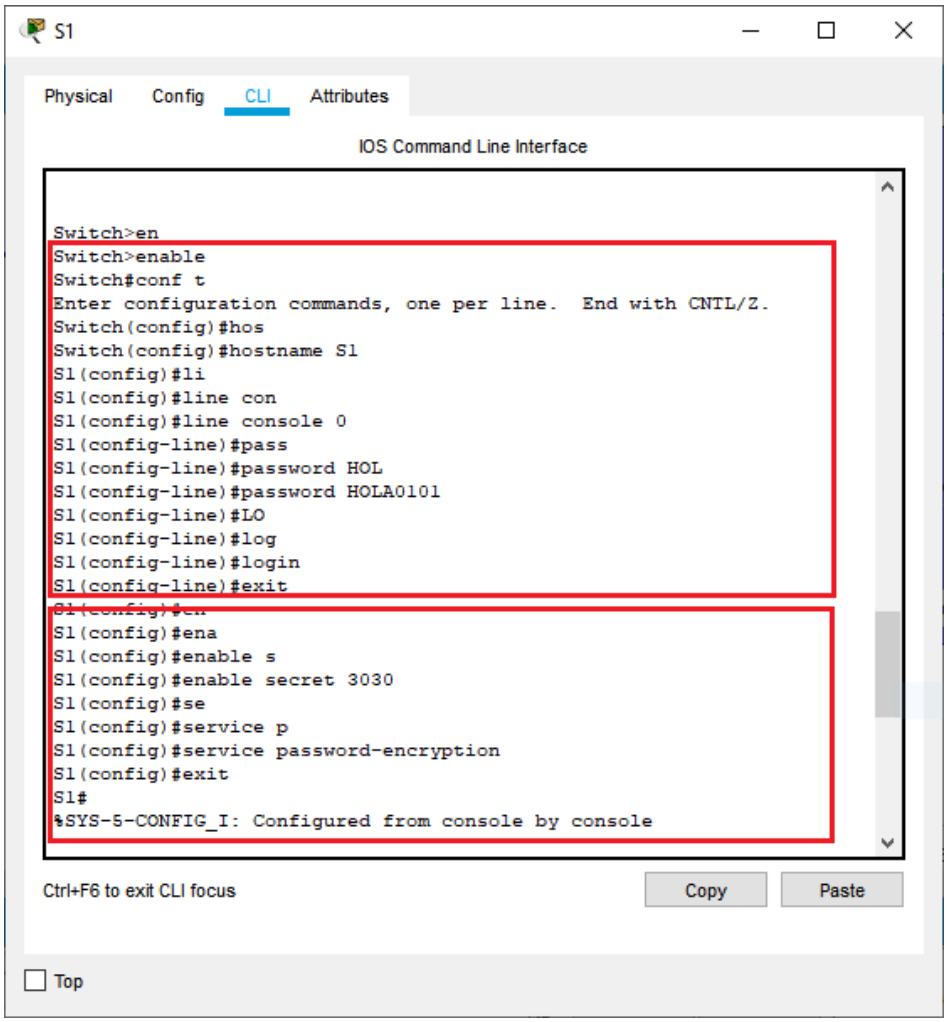

Figure III .3 – Configuration S1 (Nomination, attribution et chiffrement des mots de passe)

III.4.2 Configuration des serveurs et des Pcs

Dans cette étape de configuration, nous allons configurer les serveurs web, les serveurs DNS,les serveurs FTP , les serveurs mail ainsi que les PCs.

III.4.2.1 Configurations des Serveurs

a. Serveur WEB

Un serveur Web est un programme qui utilise le protocole HTTP pour fournir les fichiers qui constituent les pages Web que les utilisateurs ont demandées via des requêtes transmises par les clients HTPP de leurs ordinateurs.

Pour configurer un serveur WEB, nous devons d'abord configurer l'adresse IP puis nous allons l'activer. Les figures (**III .4**) et (**III .5**) montrent les étapes de configuration. D'abord, l'attribution d'une adresse IP Ensuite l'activation du serveur Web avec ses étapes numérotées de 1 jusqu'à 4.

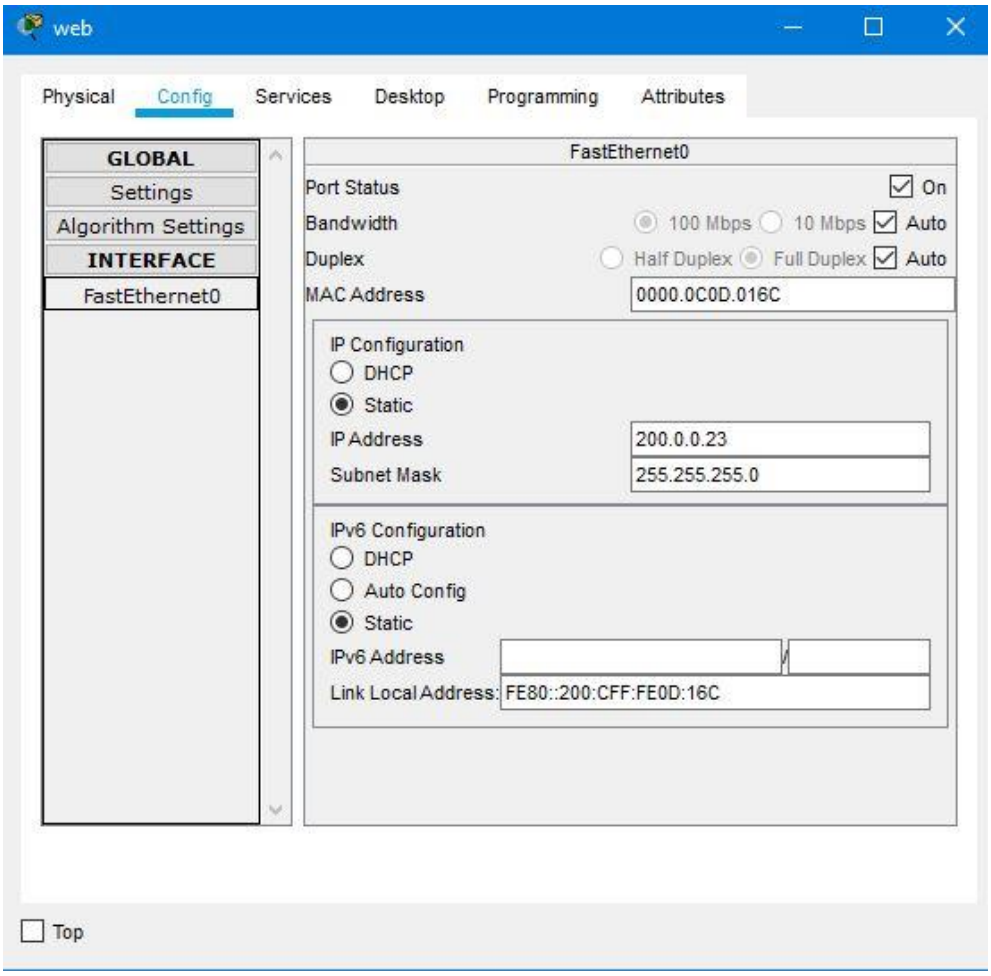

Figure III .4 Attribution d'une adresse IP et l'adresse du serveur DNS au serveur web.

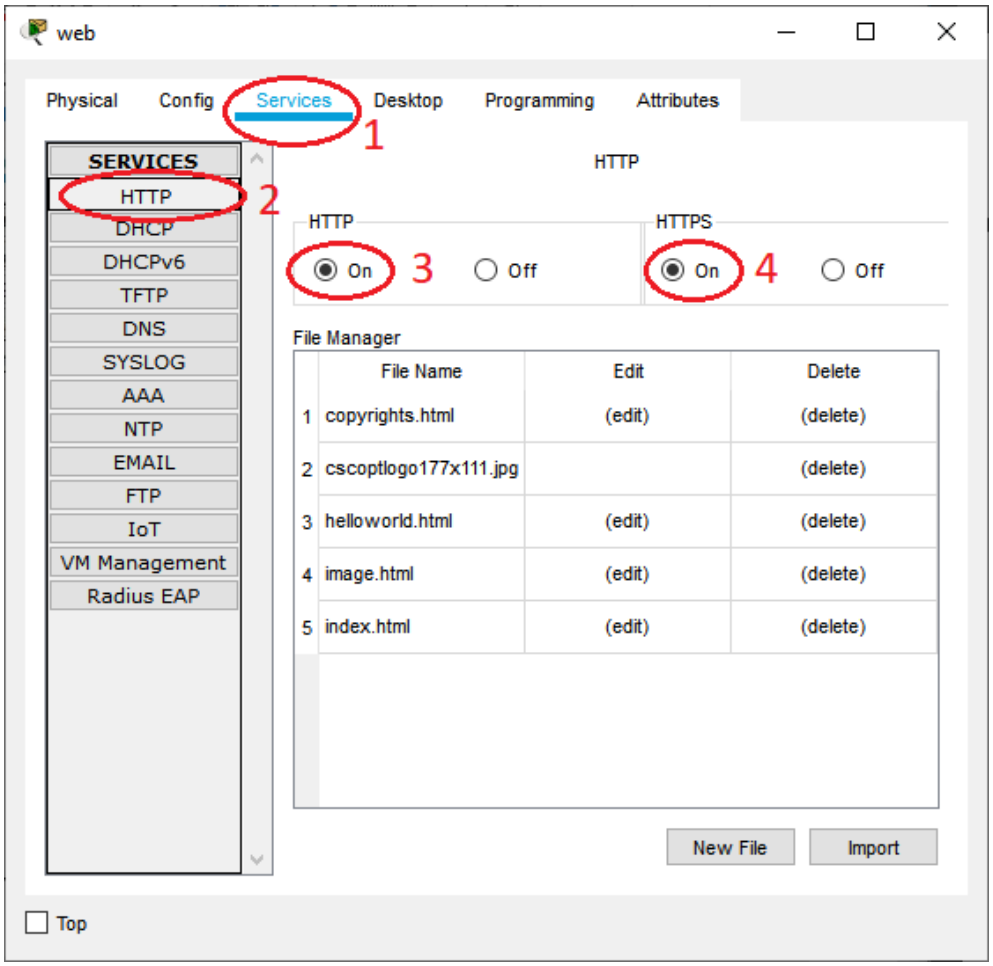

Figure III .5 Activation du serveur web.

b. Serveur DNS

Un serveur DNS assure la résolution de noms des réseaux TCP/IP. En d'autres termes, il permet aux utilisateurs d'ordinateurs clients d'adopter des noms à la place des adresses IP numériques pour identifier les hôtes distants.

Les étapes de configuration de serveur DNS sont illustrées par les figures (**III .6**) et (**III .7**) qui représentent l'attribution d'une adresse au serveur et les étapes de configuration du serveur DNS numérotées de 1 jusqu'à 6 respectivement.

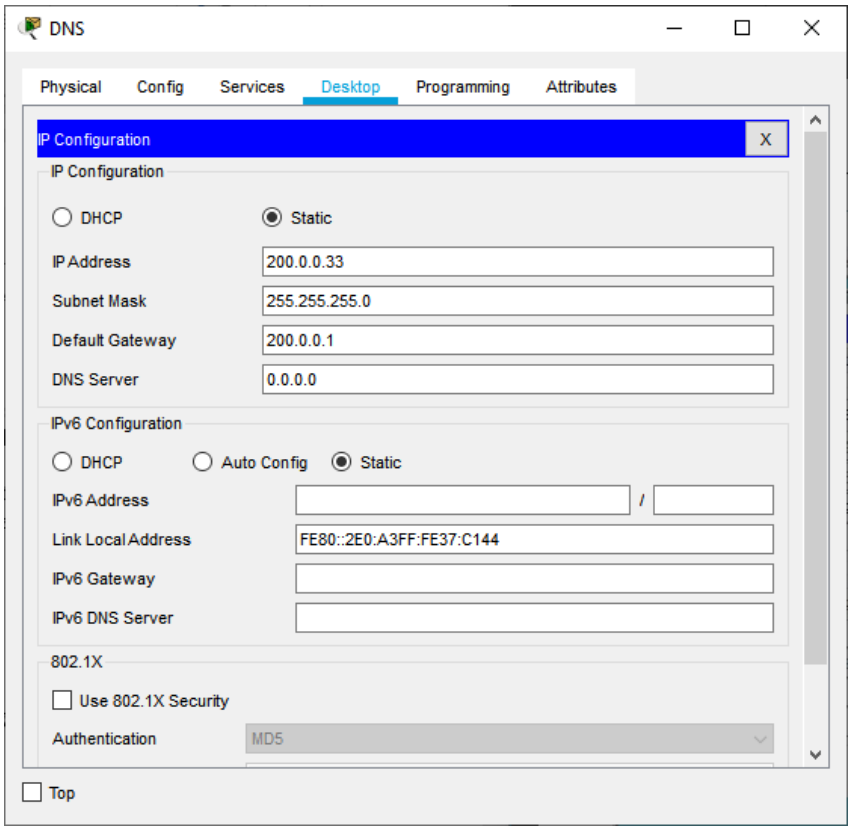

Figure III.6 Attribution d'une adresse au serveur.

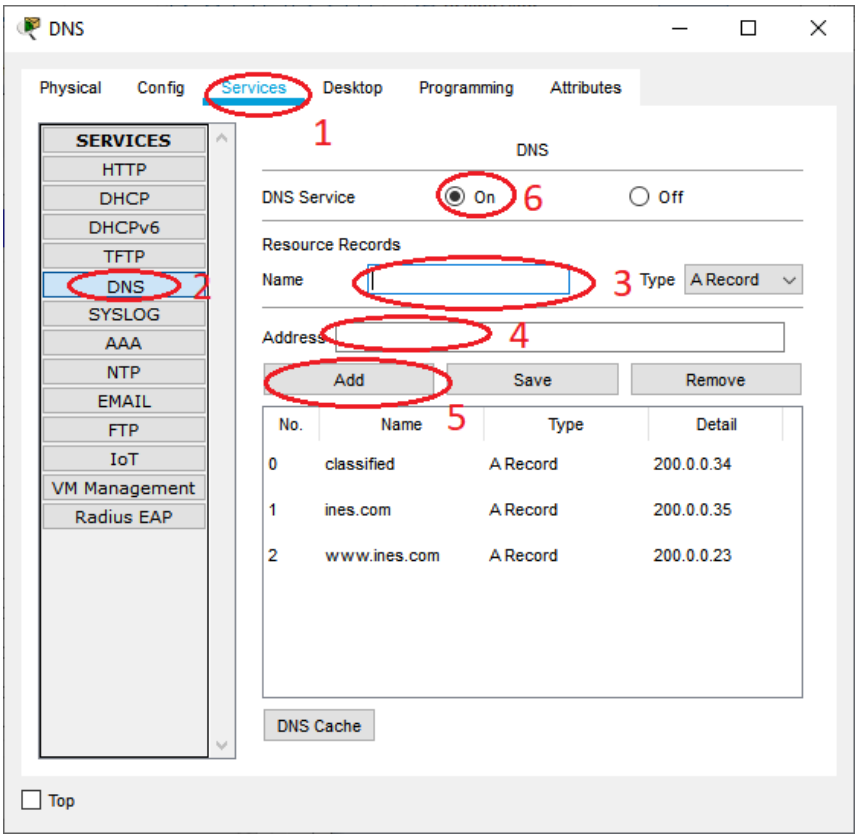

Figure III.7 Configuration du serveur DNS.

c. Serveur FTP

FTP veut dire “File Transfert Protocol” ou Protocole de transfert de Fichier.

C’est donc un langage qui va permettre l’échange de fichiers entre 2 ordinateurs, et plus exactement entre un serveur et un client.

On parle alors de : serveur FTP et client FTP

On a créé les comptes utilisateur suivants :

Nom d’utilisateur	Mot de passe	Autorisations
INES	WHITESUGAR	RWDNL
cisco	cisco	RWDNL

Les étapes de configuration de serveur DNS sont illustrées par les (**Figure III .8**) et (**Figure III .9**) qui représentent l’attribution d’une adresse au serveur et les étapes de configuration du serveur

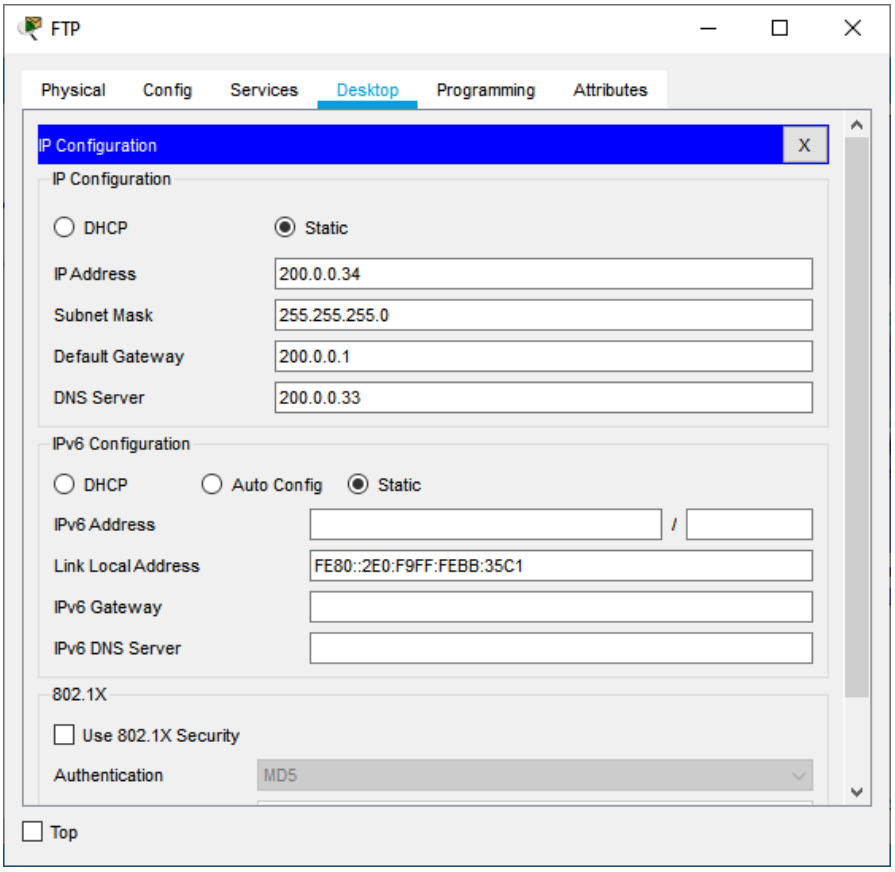

Figure III .8 Attribution d’une adresse au serveur.

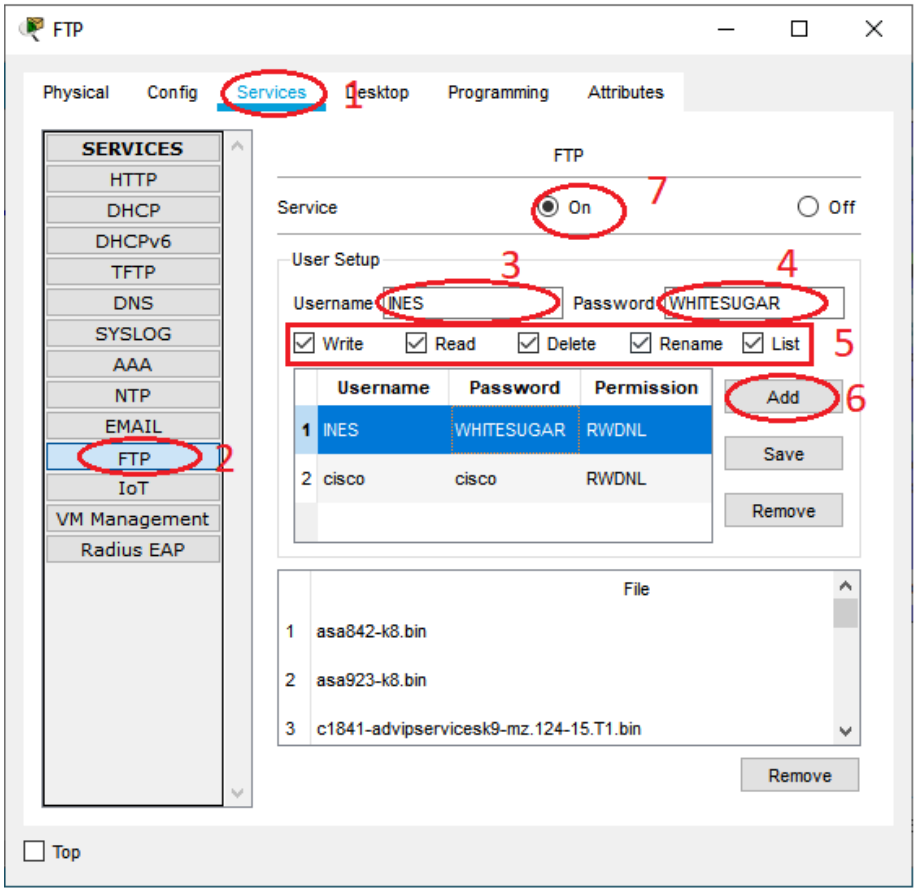

Figure III .9 Configuration du serveur FTP.

d. Serveur MAIL

Pour envoyer correctement des emails il faut configurer un serveur mail qui s'occupera de la transmission de votre message au serveur entrant du destinataire (et de là à son ordinateur). Ce serveur sortant est appelé serveur SMTP comme il utilise le protocole homonyme (SMTP = Simple Mail Transfer Protocol): techniquement, il agit un peu comme le facteur de vos mails: il les ramasse et les livrer aux destinataires

Nom d'utilisateur	Mot de passe
INES	WHITESUGAR
ASMA	BROWNSUGAR

Les étapes de configuration de serveur DNS sont illustrées par les figures (**Figure III .10**) et (**Figure III .11**) qui représentent l'attribution d'une adresse au serveur et les étapes de configuration du serveur

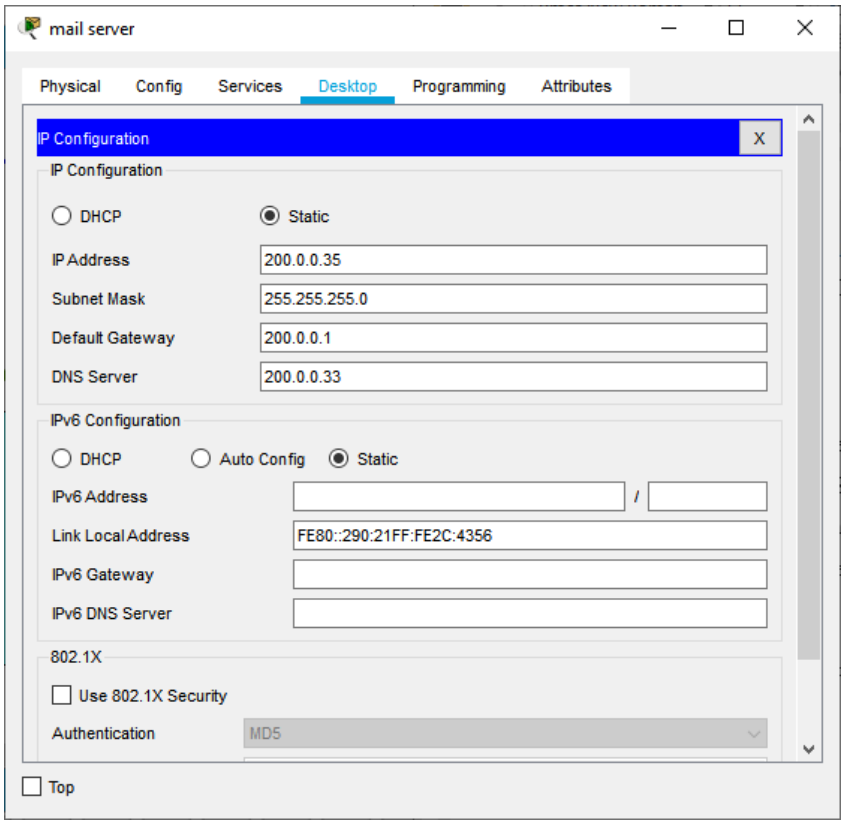

Figure III .10 Attribution d'une adresse au serveur.

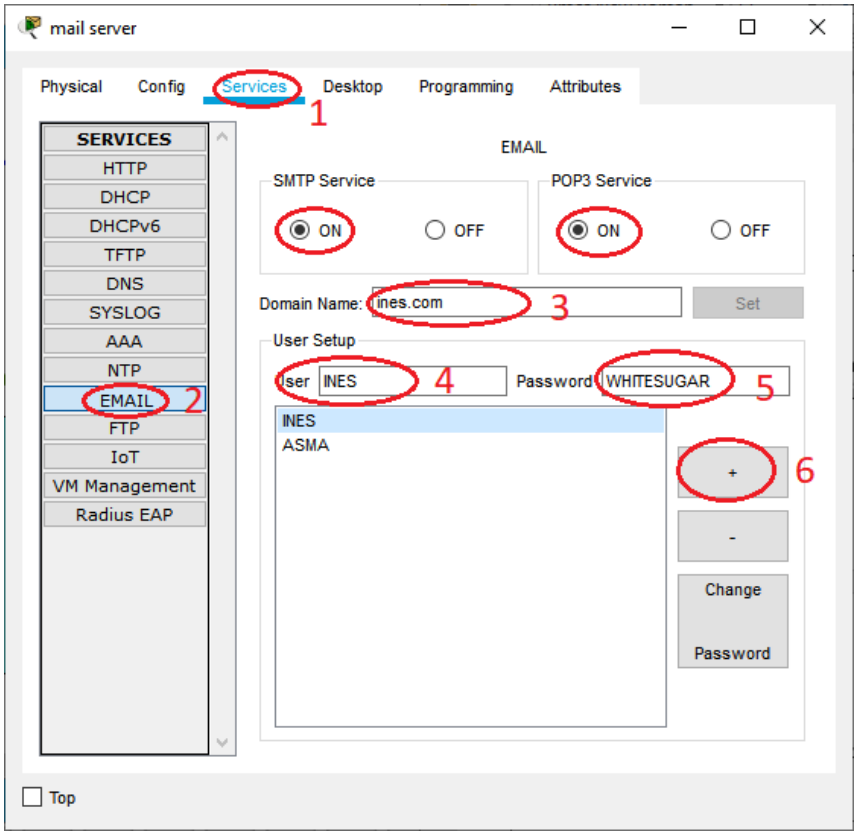

Figure III .11 Configuration du serveur mail

III.4.2.2 Configurations des Pcs

La configuration des PCs se fait par l'attribution des adresses IP, des passerelles ainsi que l'adresse du serveur DNS, la (**Figure III.12**) montre la configuration de pc, Nous prendrons comme exemple de configuration le PC « IT1 » sachant que la même chose sera appliquée pour les PCs « IT1 » « IT2 » et « PC4 »

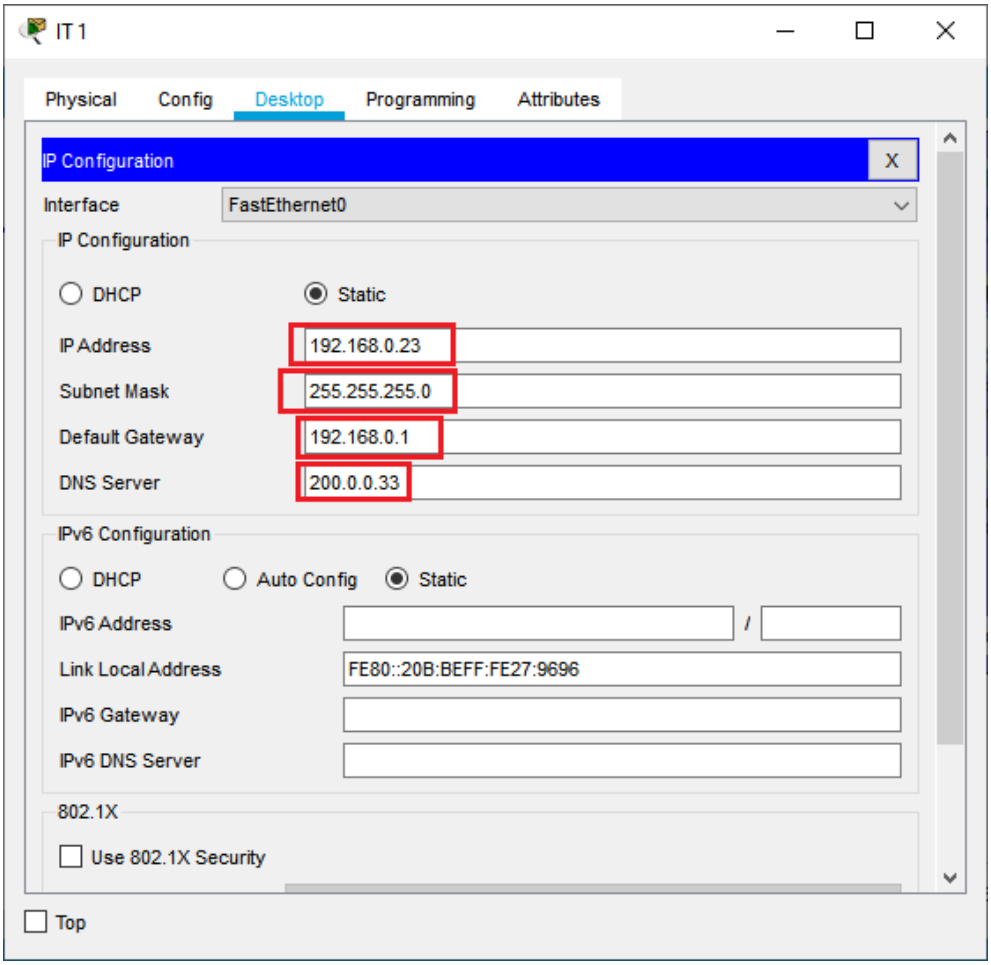

Figure III.12 Configuration PC «IT 1»

III.4.3 Configuration des routeurs

Pour la configuration des routeurs, nous allons commencer par la configuration des hostnames et des mots de passe, Ils sont configurés de la même façon que les commutateurs.

Nous prendrons comme exemple de configuration le commutateur « R2ISP »

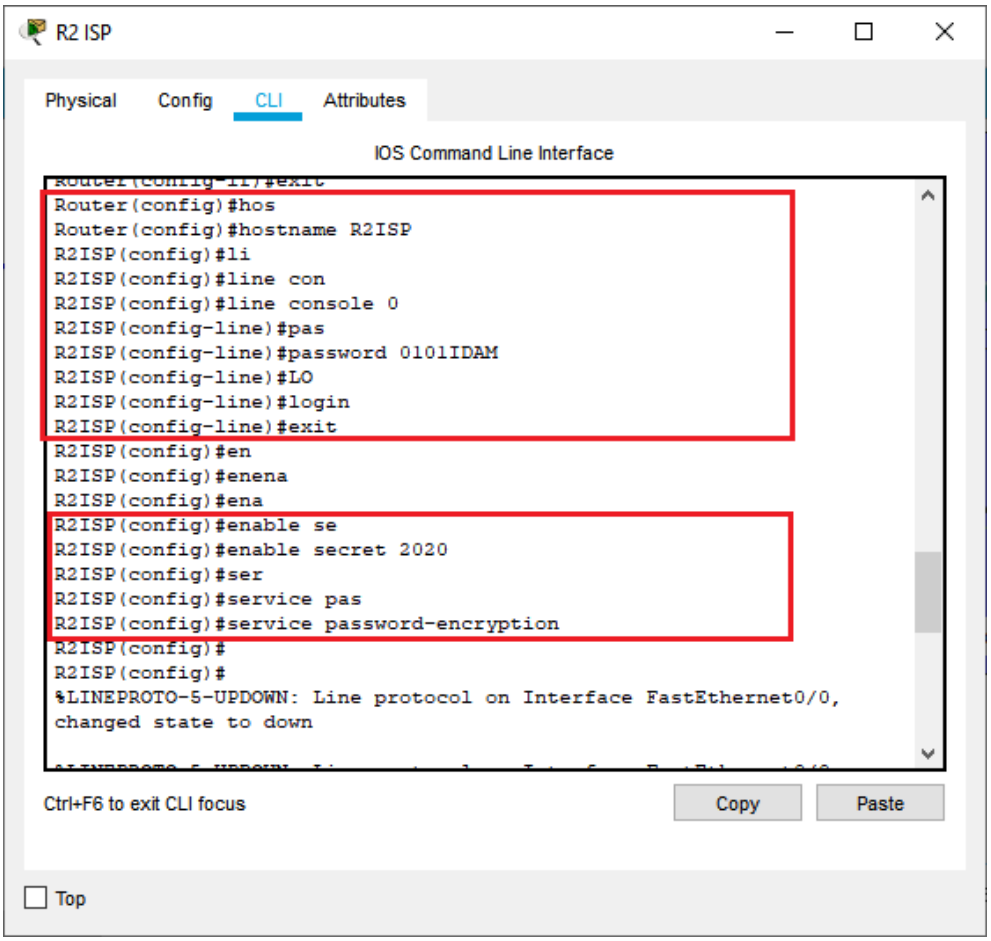

Figure III .13 – Configuration R2 (Routeur)

Configuration des interfaces et de routage statique :

Dans cette étape nous allons attribuer les adresse IP aux interfaces des routeurs et les activer par la suite.

Si on veut que tous les routeurs (tous les réseaux) puissent communiquer entre eux, il va falloir configurer| une route statique.

Les routes statiques sont le moyen de routage le plus sûr. Ils augmenteront également les performances globales du réseau.

Et pour configurer la route statique on a utilisé la commande « ip route »

La (**Figure III .14**) illustre les configurations citées précédemment.

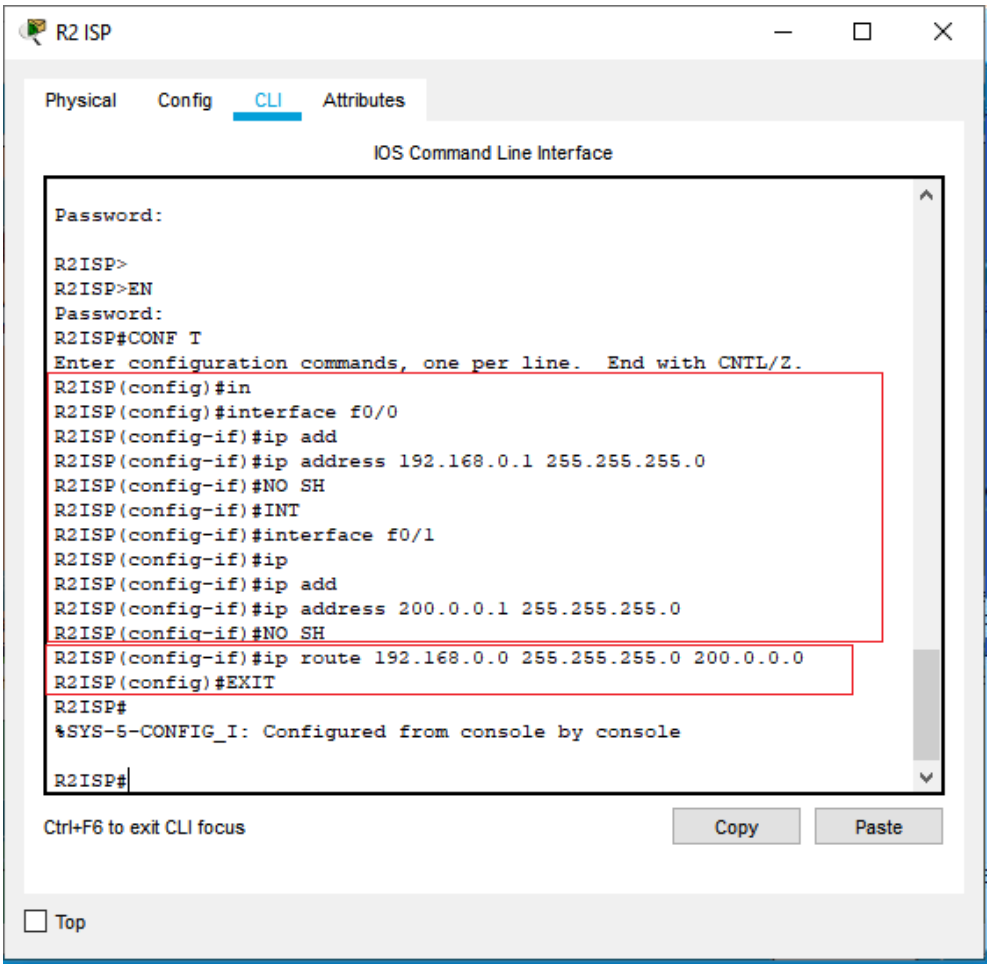

Figure III .14 - Configuration des interfaces et de routage statique

III.5 Configuration de pare feu, liste d'accès et DMZ

Après avoir réalisé l'architecture de notre réseau, nous passons à la configuration de sécurisation

III.5.1 Configuration Pare Feu :

On commence par la configuration des interfaces (INSIDE , OUTSIDE)du pare-feu . En suite nous avons établi un serveur DHCP à même le pare-feu autorisant ainsi la distribution d'adresse IP automatiques depuis cet équipement au Pcs « IT3 » « IT4 » « IT5 » « IT6 »

La «**Figure III.15**» et «**Figure III.16**» montre la configuration des VLANs INSIDE et OUTSIDE.

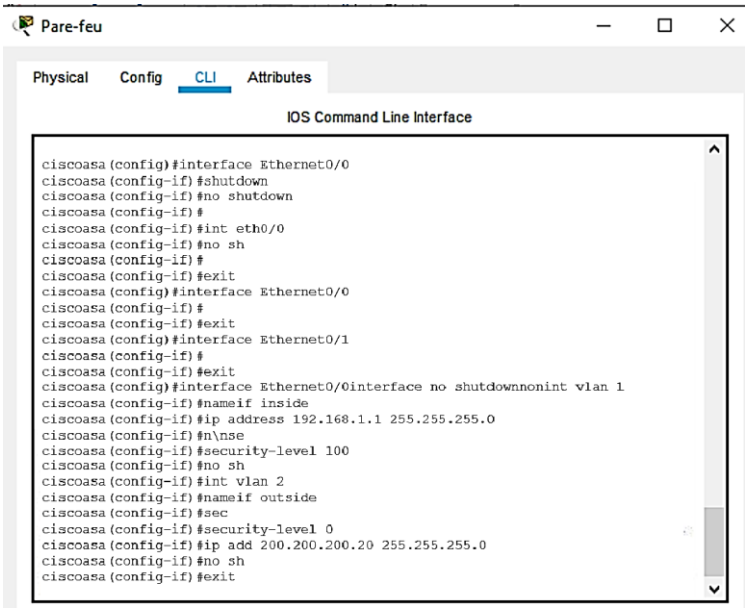

Figure III .15 – Configuration Pare-feu (1)

Dans la Figure III .15, nous remarquons la commande <nameif> qui donne son appellation aux deux interfaces. La commande <security-level> suivie d'une valeur indique son niveau de sécurité. Plus le chiffre est grand plus l'interface est digne de confiance. Il faut retenir que par défaut, le trafic transite uniquement entre deux interfaces du niveau le plus élevé vers le niveau le moins élevé.

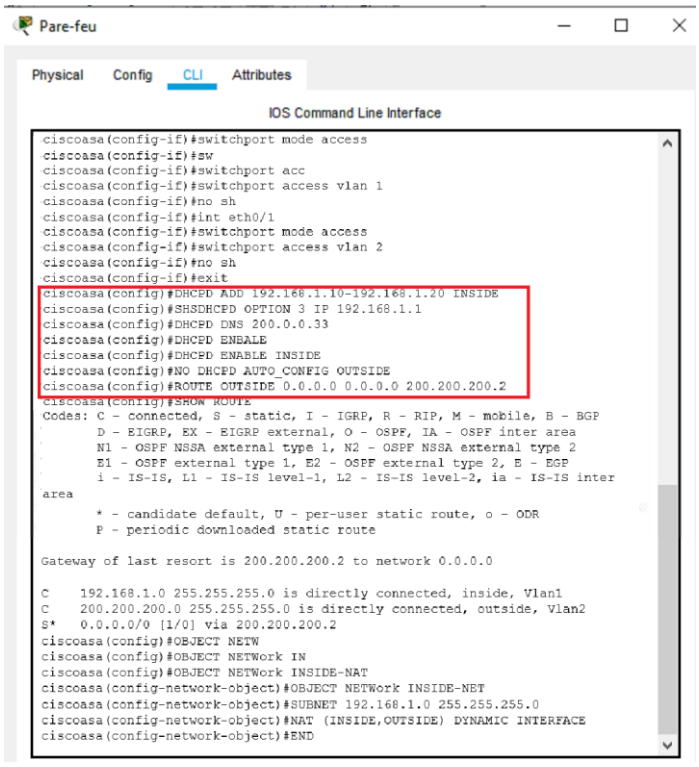

Figure III .16 – Configuration Pare-feu (2)

Dans l'étape suivante, nous allons modifier la politique par défaut MPF inspection d'application de service globale pour permettre aux hôtes du réseau interne pour accéder aux serveurs web sur Internet, on va d'abord créer une classe inspection-default qui correspond à défaut d'inspection du trafic. Ensuite, créer une politique-carte global-policy et l'inspecter avec DNS, FTP, HTTP et ICMP. Enfin, on fixe la carte politique globalement à toutes les interfaces, voir (**Figure III .17).**

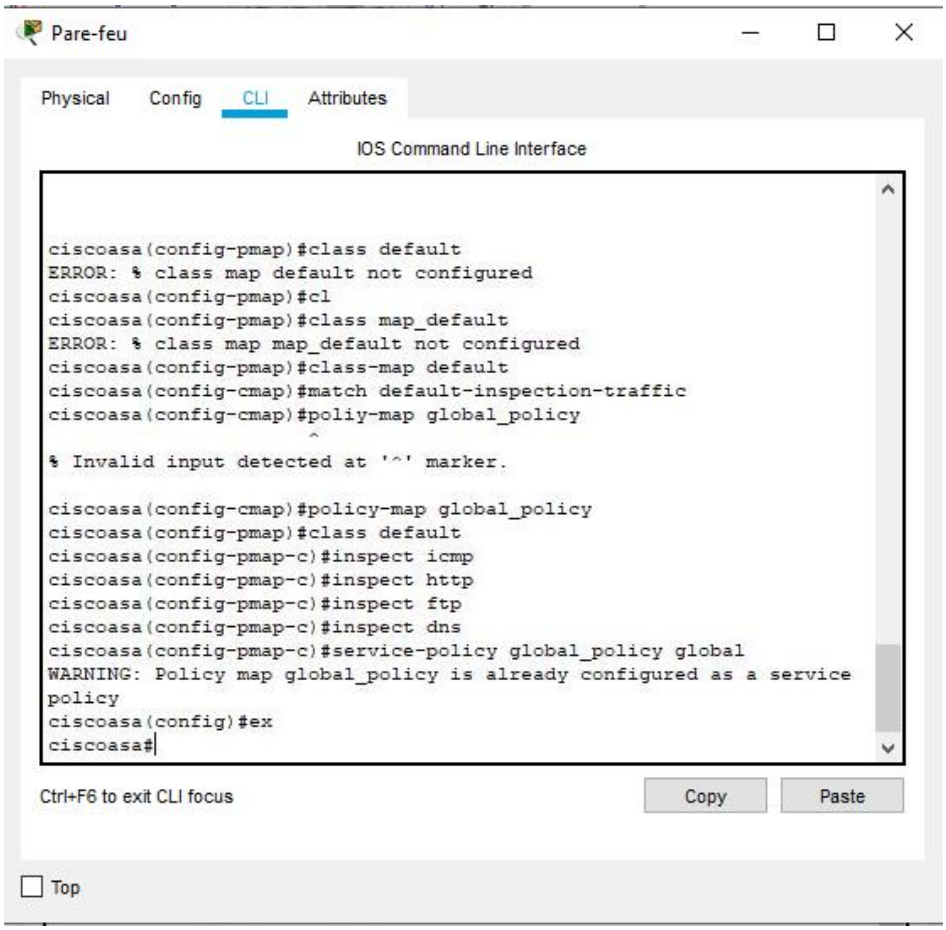

Figure III.17 – Configuration Pare-feu (Filtrage des ports)

III.5.2 Configuration liste d'accès (ACLs)

Les listes d'accès (access list) sont des instructions qui expriment une liste de règle, imposées par l'opérateur, donnant un contrôle supplémentaire sur les paquets reçus et transmis par le routeur mais ne concernant pas ceux générés par le routeur.

Les listes d'accès sont capables d'autoriser ou d'interdire des paquets, que ce soit en entrée ou en sortie vers une destination

On a utilisé la commande « permit » et « deny » pour autorisé seulement les 2 Pcs «IT1» et «IT2» a accéder au serveur

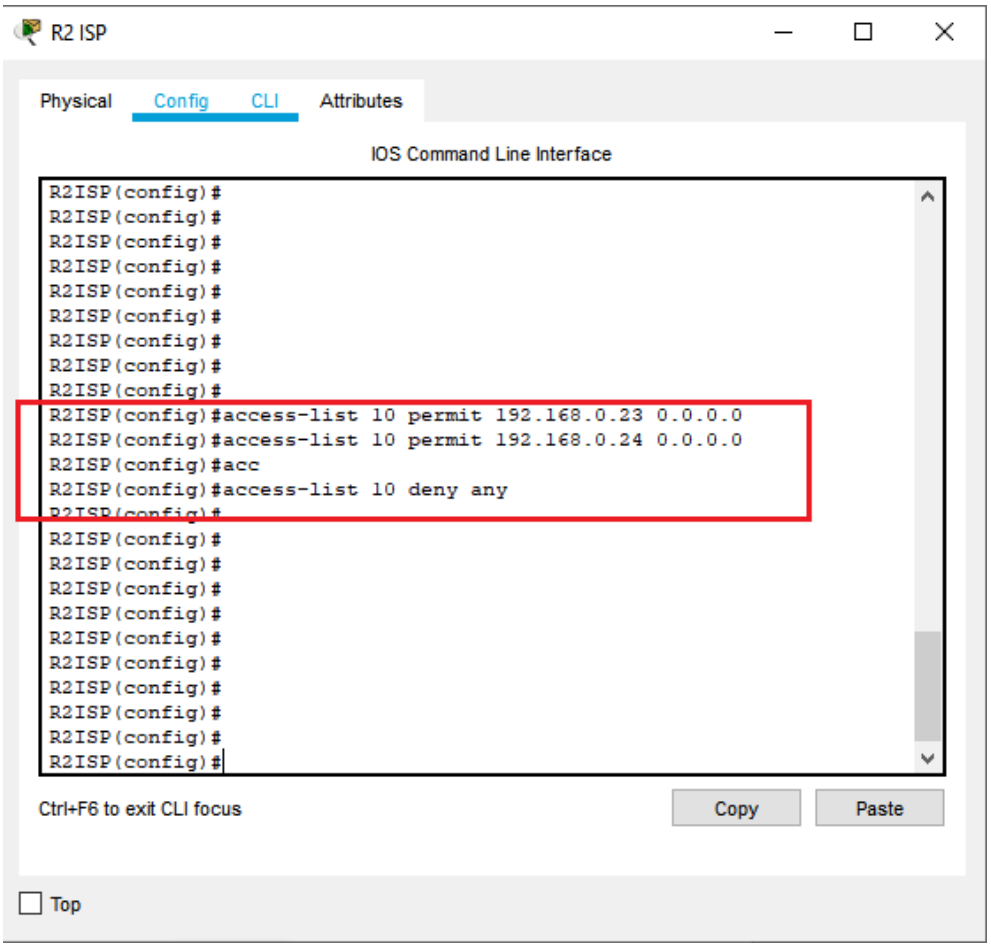

Figure III.18 – Configurations ACLs

III.5.3 Configuration DMZ

Les services offerts au public sont généralement installés sur des zones démilitarisées afin de bénéficier de la protection offerte dans ces espaces. La traduction d'adresse est l'une de ces protections. Il faut que le serveur dans le réseau DMZ soit accessible de l'extérieur par son adresse publique, la configuration de cette traduction d'adresse et illustré dans la «**Figure III .19**»

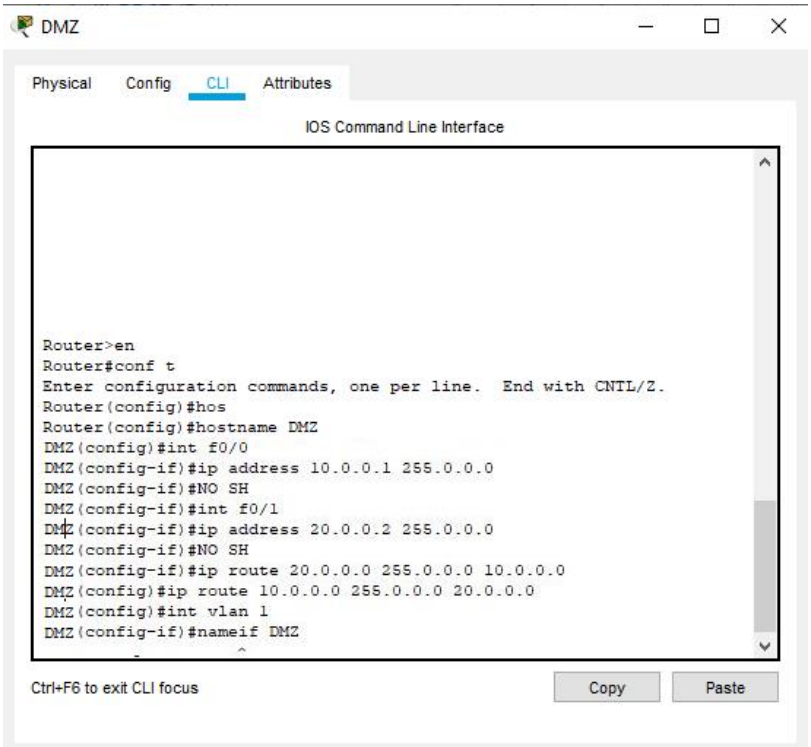

Figure III.19 – Configurations DMZ

III.6 Architecture réalisée

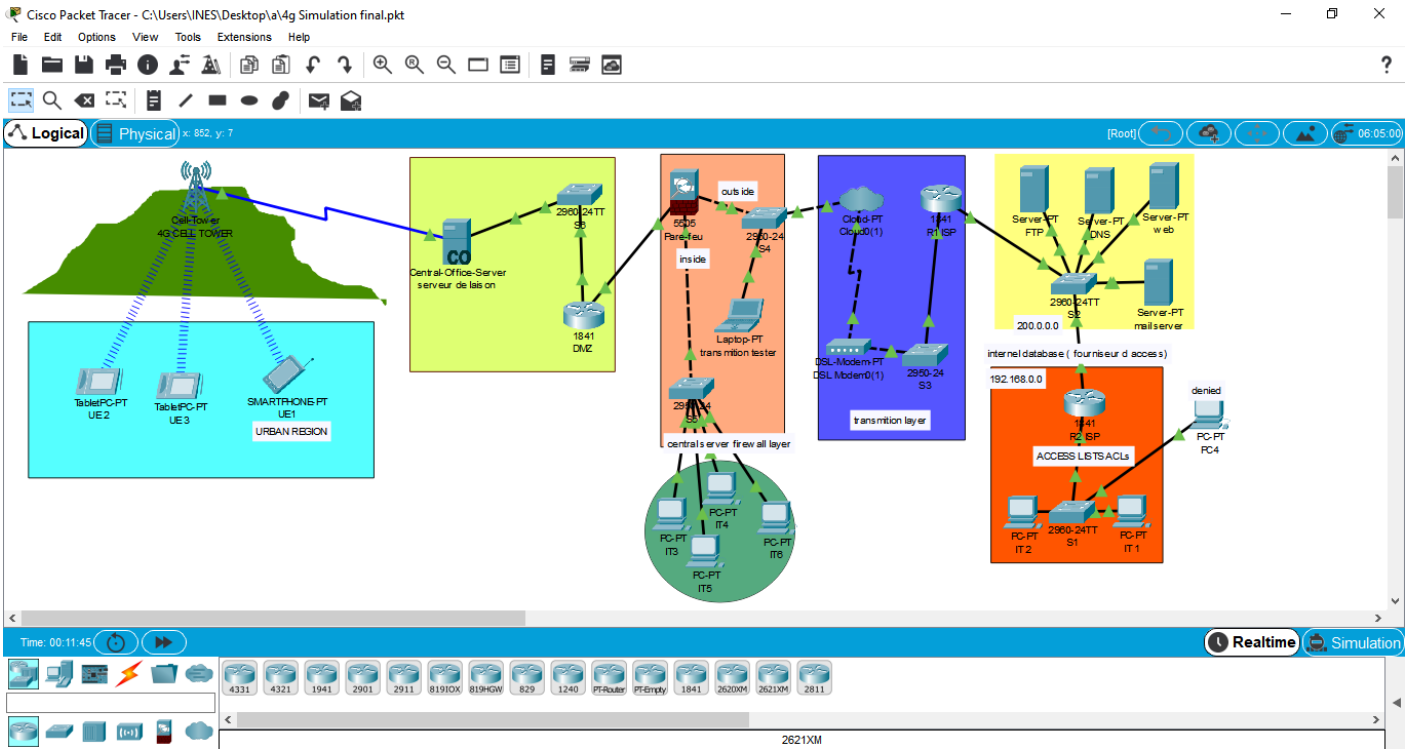

Figure III.20 - L'architecture réalisée après les configurations

III.7 Tests et validation des configurations

Dans cette partie nous allons vérifier d'abord la communication entre les équipements en utilisant la commande Ping. Ensuite, nous allons vérifier l'accès au site web qu'on a crée

a- Teste entre les PCs

Après avoir configuré les différents équipements de l'architecture, nous allons tester le bon fonctionnement des échanges de données et cela grâce à la commande Ping.
Nous avons lancé un Ping entre le PC IT1 ayant l'adresse IP (192.168.0.23) et le PC4 ayant l'adresse (192.168.0.99), ceci illustré par la « **Figure III .21** ».

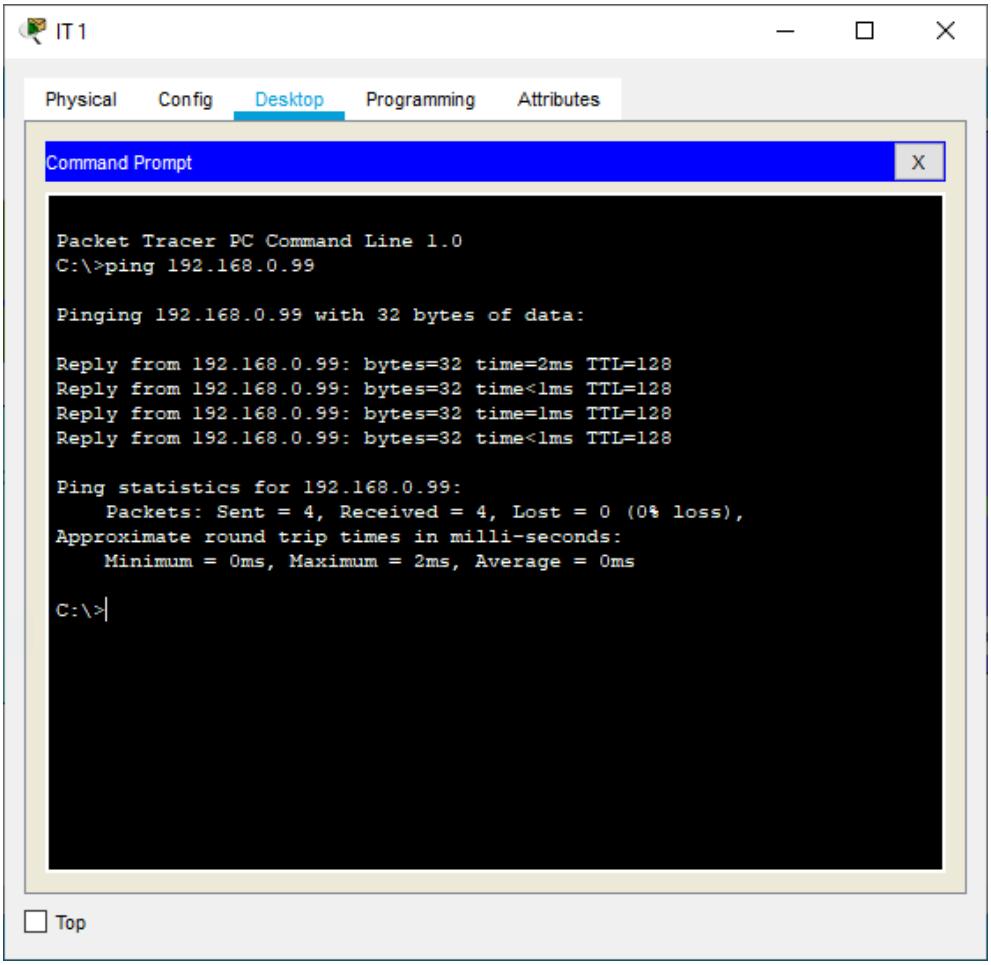

Figure III.21 - Résultat de ping entre IT1 ET PC4

b- Vérification de l'accès au site web

Nous allons tester l'accès au site web à partir d'un laptop (transmission tester) comme nous montre la « **Figure III.22** ».

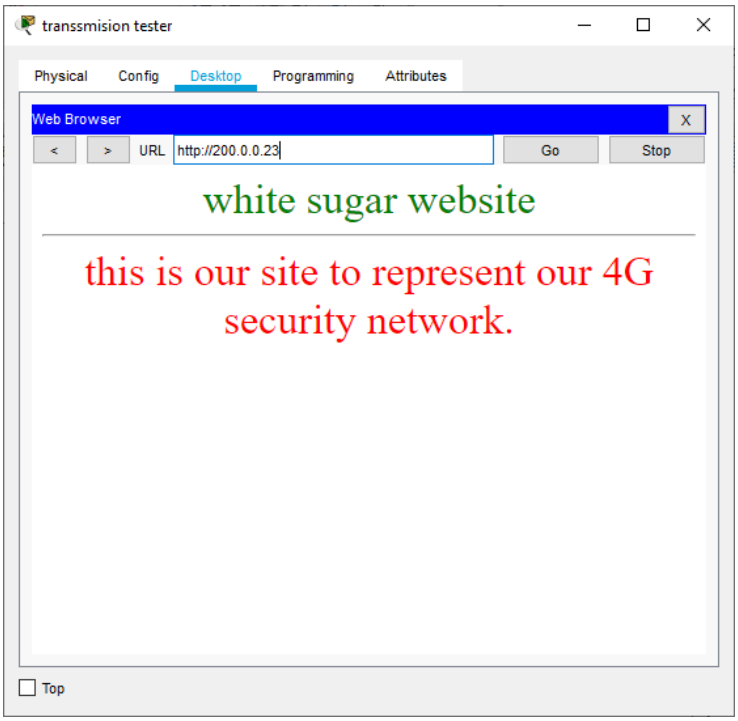

Figure III.22 - Accès au site web

c- Vérification des listes d'accès

Nous avons limité l'accès au serveurs qu'au 2 PC « **IT1** » et « **IT2** ».

On a pris le pc IT1 comme exemple

La figure suivante représente le ping entre le serveur « **FTP** » ayant l'adresse IP (200.0.0.34) et le PC « **IT1** » ayant l'adresse IP (192.168.0.23)

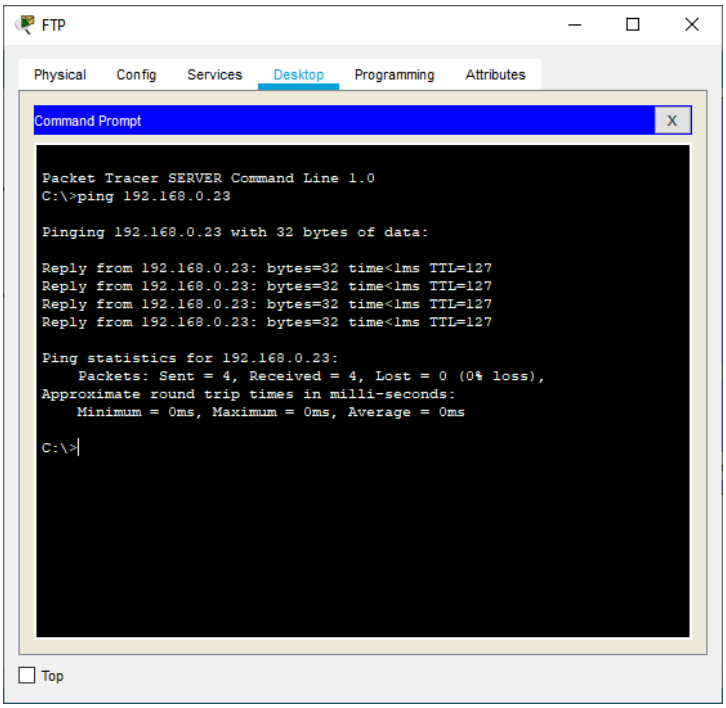

Figure III .23 - Résultat de ping entre serveur FTP et IT1

Et cette figure représente le ping entre le serveur «**FTP**» ayant l'adresse IP(200.0.0.34) et «**PC4**» ayant l'adresse IP(192.168.0.99)

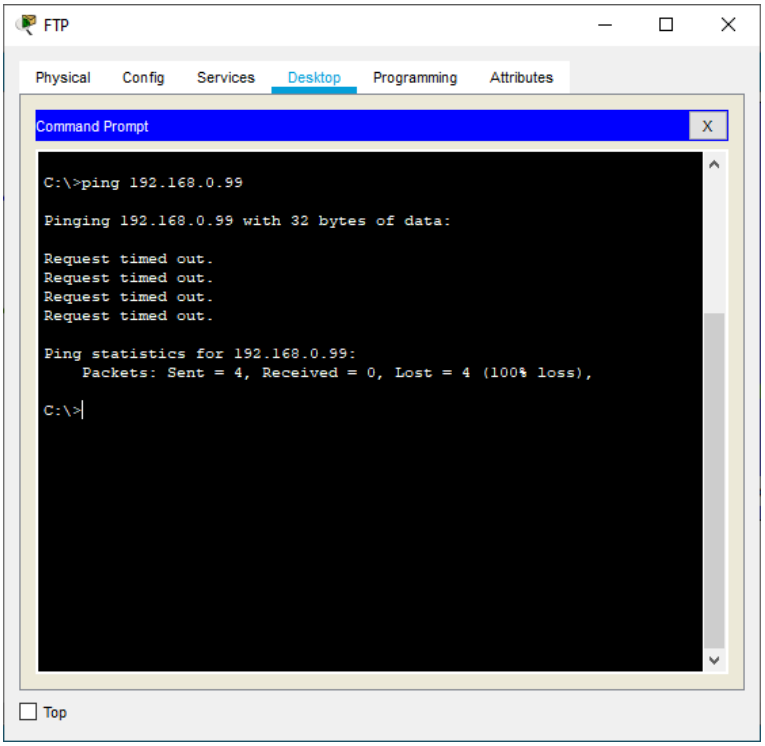

Figure III .24 - Résultat de ping entre serveur FTP et PC4

d- Vérification de la transmission de données entre serveur de liaison et les utilisateurs

La figure suivante représente le ping entre **« serveur de liaison CO »** ayant l'adresse IP(20.0.0.5) et l'utilisateur **«UE1 »**

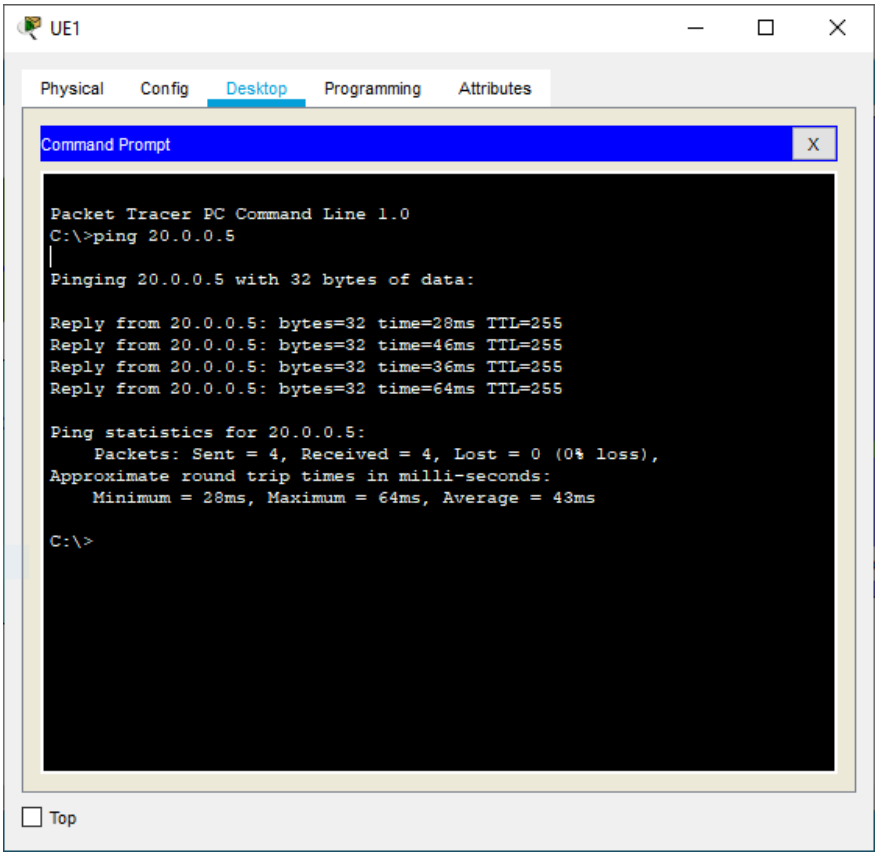

Figure III .25 – Résultat ping entre UE1 et le serveur de liaison CO

III.8 Conclusion

Dans ce chapitre nous avons présenté notre solution pour la sécurisation du réseau.

Par la suite, nous avons décrit la configuration de nos architectures réseaux dans les deux parties. Dans la première, nous avons configuré les réseaux LANs ainsi que des tests de vérification, et dans la deuxième partie nous sommes passé à la configuration du pare-feu, les listes d'accès et DMZ illustré par une présentation des différentes commandes de mise en place.

Conclusion Générale

Ce rapport présente notre travail effectué dans le cadre de notre projet de fin de cycle. Ce dernier consiste à mettre en place et simuler un réseau 4G sécurisé.

Dans ce travail, nous avons pu montrer les failles de la sécurité dans les réseaux de téléphonie mobiles 4G/LTE. Ce qui nous a permis de proposer des solutions contre les différentes vulnérabilités.

Nous avons présenté les différentes normes des réseaux mobiles ainsi que des généralités sur le réseau 4G

Notre démarche consiste à implémenter une solution basée sur les pare-feu les listes d'accès et DMZ pour filtrer les données qui circulent dans le réseau.

Dans ce présent projet, nous n'avons fait qu'une simulation avec le simulateur Cisco Packet-tracer, dans l'avenir, nous souhaitons faire une vraie réalisation sur des équipements réels, afin d'appliquer concrètement ce que nous avons fait au cours de ce mémoire.

Bibliographies

[1] https://bastienbonnard.com/1444-2

[2] Planification d'un réseau 4 G en zone urbaine master Université Abderrahmane Mira Bejaia

[3] https://geeko.lesoir.be/2018/04/10/de-la-2g-a-la-5g-comment-les-reseaux-mobiles-ont-influence-l'évolution-technologique/

[4] Georges RODRIGUEZ, « Introduction aux réseaux cellulaires : Techniques d'accès et de partage de la ressource radio ». Systèmes de Télécommunication Cycle d'harmonisation 2AAST, TEL-COM202, 2011/2012

[5] Tarek Bchini, « Gestion de la Mobilité, de la Qualité de Service et Interconnexion de Réseaux Mobiles de Nouvelle Génération », Thèse de doctorat de l'Université de Toulouse, Le 10/06/2010.

[6] Seide.G, « Planification d'un réseau de quatrième génération à Partir D'un Réseau De Troisième Génération », Mémoire en vue de l'obtention du diplôme de maîtrise des Sciences appliquées (génie informatique), Université de MONTREAL, 2011.

[7] Hiba Mouachi, « Etude et simulation de la norme LTE par 3GPP », Projet de semestre

[8] Eya Jammazi, « Optimisation d'un réseau pilote 4G pour Tunisie Télécom », Mémoire de Projet de Fin d'Etudes en Réseaux et Communications, 21/Juin/2013

[9] « LTE + SAE = EPS, Principes et Architecture », Efort 2009.

[10] AIT ELHADJ Kahina MAKHMOUKHEN Souhila « La sécurité des réseaux mobiles Ad hoc contre l'attaque du trou noir » Mémoire de Fin d'Etudes Pour l'obtention du Diplôme de Master Recherche (Télécommunication) Université Abderahmane MIRA – BEJAIA 2015

[11] https://www.futura-sciences.com/tech/definitions/internet-deni-service-2433/

[12] https://www.commentcamarche.net/contents/68-analyseurs-reseau-sniffers

[13] http://strategique.free.fr/archives/textes/hacking/archives_hacking_05.htm

[14] https://www.ionos.fr/digitalguide