REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE YAHIA FARES DE MEDEA

Faculté de **T**echnologie

Département du **G**énie **E**lectrique

Projet de Fin d'Etudes de Master

Spécialité : Systèmes des télécommunications

Etude et implémentation du système sécurisé pour communication mobile 4G

Présentés par :

BENMERIEM Mohammed Larbi

MOULESMARA Abdelbaki

Proposés et Dirigés par :

Dr. KROBBA Ahmed

Promotion 2024

Remerciements

Tout d'abord, nous remercions « ALLAH », qui nous a guidés sur le chemin du savoir et nous a donné la patience, la volonté et le courage nécessaires à la réalisation de ce projet.

Nous exprimons notre gratitude à notre encadrant, KROBBA Ahmed.

Nous remercions également les membres du jury.

Nos remerciements vont aussi à nos chers parents, frères et sœurs pour tous leurs sacrifices et leur immense soutien.

Enfin, merci à tous nos proches amis, à nos enseignants, ainsi qu'aux membres du département de Génie Électrique de l'université Yahia Farès de Médéa.

Dédicaces

Ce modeste travail est dédié à :

Tous ceux qui nous aiment et que nous aimons.

Nos chers parents, qui nous ont soutenus et encouragés tout au long de notre scolarité.

Nos frères et sœurs.

Nos enseignants.

Nos amis.

Toutes les personnes qui nous ont apporté leur aide.

BENMERIEM Mohammed Larbi & MOULESMARA Abdelbaki

RESUME

La sécurité des réseaux mobiles 4G fait référence aux mesures conçues pour protéger l'information sensible stockée et transmise par les smartphones contre les cyber-attaques. L'objectif de ce travail est de permettre au lecteur, familiarisé avec 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 réseaux 4G/LTE contre les principaux risques de piratage et d'intrusion.

Mot clé : Réseaux mobiles, 4G/LTE, Sécurité, IPSec, Cisco Packet Tracer.

ABSTRACT

4G mobile network security refers to measures designed to protect sensitive information stored and transmitted by smartphones from cyber-attacks. The objective of this work is to enable the reader, familiar with 4G/LET networks, to acquire a body of security knowledge that will allow them to better understand the various mechanisms for protecting 4G/LTE networks against the main risks of hacking and intrusion.

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

ملخص

يشير أمان شبكة الهاتف المحمول 4G إلى التدابير المصممة لحماية المعلومات الحساسة المخزنة والمرسلة بواسطة الهواتف الذكية من الهجمات السيبرانية. تم تصميم المتناقضات لخداع الاتصالات المتنقلة عن طريق إضافة ضوضاء غير محسوسة إلى الإشارات الصوتية. تمثل هذه العملية تهديدًا خطيرًا لأمن أنظمة الاتصالات المتنقلة. ولذلك يصبح من الضروري دراسة نقاط الضعف لديهم. الهدف من هذا العمل هو دراسة الحلول التي تضمن أمن أنظمة الاتصالات المتنقلة، من خلال اقتراح خوارزميات فعالة تعتمد على نهج الذكاء الاصطناعي باستخدام الشبكات العصبية العميقة.

الكلمة الرئيسية: شبكات الهاتف المحمول، 4G/LTE، الأمان، IPSec، Cisco Packet Tracer.

Liste des figures

Figure 1 L'évolution des réseaux mobile (2) 4
Figure 2 Architecture du réseau GSM 5
Figure 3 Architecture du réseau GPRS 7
Figure 4 Architecture du réseau EDGE 8
Figure 5 Architecture globale du réseau UMTS 10
Figure 6 Architecture LTE (14) 16
Figure 7 Architecture de l'E-UTRAN (15) 17
Figure 8 Architecture EPC (16) 19
Figure 9 Les types de porteur. (19) 24
Figure 10 Architecture de sécurité du LTE (20) 28
Figure 11 Menaces contre l'identité de l'utilisateur (21) 29
Figure 12 Classifications des attaques dans les réseaux 31
Figure 13 Sécurité EPS (19) 35
Figure 14 Architecture de la cryptographie (25) 38
Figure 15 Architecture pare-feu (Firewall) (27) 38
Figure 16 Architecture d'un VPN 39
Figure 17 Architecture proposée pour un réseau 4G/LTE 41
Figure 18 L'architecture du réseau 4G/LTE sous Packet Tracer 42
Figure 19 Configuration des routes sur FAI 44
Figure 20 Configuration des routes sur PGW-MEDEA 46
Figure 21 Configuration des switch sur MME-MEDEA 47
Figure 22 Configuration de l'adresse IP sur l'ordinateur de la direction-MEDEA 48
Figure 23 Le réseau 4G/LTE en mode simulation 49
Figure 24 Connectivité réussie entre les entreprises 50
Figure 25 Configuration des routes sur PGW-MEDEA 51
Figure 26 L'activation de ISKAMP et protocole IPSec 53
Figure 27 Le CRYPTO MAP sur le routeur PGW-MEDEA ET PGW-OUARGLA 54
Figure 28 Réalisation du ping 55

Abréviations

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

AS: Access Stratum

BSC: Base Station Controlers

BSS: Base Station Sub-system (access list)

BTS: Base Transceiver System

CDMA: Code Division Multiple Access

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

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

FDD: Frequency Division Duplex VII

GGSN: Gateway GPRS Support Node

GPRS: General Packet Radio Service

GSM: Global System for Mobile

HSS: Home Subscriber Server

IMS: IP Multimedia Subsystem

IPSCE: Internet Protocol Security

ISAKMP: Internet Security Association and Key Management Protocol

LTE: Long Term Evolution

MAC: Medium Access Control

MME: Mobility Manager Entity

MMS: Multimedia Message Service

MSC: Mobile Switching Center

NAS: Non-Access Stratum

NMT : Nordic Mobile Téléphone

OFDMA: Orthogonal Frequency Division Multiple Access

OSI: Open Systems Interconnection

PC: Personnel Computer

PCU: Packet Control Unit

PCRF: Policy and Charging Rules Function

PDNGW: Packet Data Network Gateway

P-GW: Packet Data Network Gateway

PS : Packet Switched

RLC: Radio Link Control

RNC: Radio Network Controller

RRC: Radio Resource Control

SGSN: Serving GPRS Support Node

SGW: Serving Gateway

SMS: Short Message Service

TACS : Total Access Communications System

TCP: Transmission Control Protocol

TDD: Time Division Duplex

TDMA: Time Division Multiple Access

UE: User équipement

UMTS: Universal Mobile Telecommunications System

USIM: Universal Subscriber Identity Module

VPN: Virtual Private Network

Table des matières

Remerciements I
Dédicaces II
RESUME III
Liste des figures V
Abréviations VI
Table des matières IX
Introduction Générale 1
Chapitre I Généralité sur les réseaux mobiles 2
I.1. Introduction : 3
I.2.Evolution des réseaux mobiles : 3
I.3. Les différentes normes téléphoniques mobiles sans fil : 4
I.3.1. La première génération des téléphones mobile (1G) : 4
I.3.2 La deuxième génération des téléphones mobiles (2G) : 5
I.3.3 La troisième génération des téléphones mobiles (3G) : 9
I.3.4 La quatrième génération des téléphones mobiles (4G/LTE) : 11
I.3.5 La cinquième génération des téléphones mobiles (5G) : 12
I.4. Conclusion : 13
Chapitre II Réseau mobile 4G /LTE 14
II.1. Introduction : 15
II.2. Définition de la 4G/LTE : 15
II.3. Objectifs de la 4G/LTE : 15
II.4. Architecture de la 4G/LTE : 16
II.4.1 Équipement Utilisateur (UE) : 16
II.4.2 Réseau d'accès E-UTRAN : 17
II.4.3 Réseau Cœur EPC (Evolved Packet Core) : 18
II.5. Les couche du modèle LTE : 21
II.6. Performances et caractéristiques des réseaux LTE : 22
II.6.1. Les Débits : 22
II.6.2. La latence : 22
II.6.3 L'agilité en fréquence : 23

II.6.4 Codage : 23
II.6.5 Le multiplexage : 23
II.6.6 Qualité de service dans le réseau 4G/LTE : 24
II.7. Conclusion : 25
Chapitre III La sécurité dans le réseau mobile 4G/LTE 26
III.1. Introduction : 27
III.2. Les objectifs de la sécurité : 27
III.3. Architecture de la sécurité : 27
III.4. Vulnerabilities et menaces dans 4G/LTE : 28
III.4.1. Menaces contre l'identité de l'utilisateur (IMSI catcher) : 29
III.4.2. Menaces de suivi d'UE (Threats of UE tracking) : 30
III.4.3. Menaces pour l'eNB : 30
III.4.4. Menaces pour la passerelle MME /SAE : 30
III.4.5. Les attaques dans les réseaux 4G/LTE : 30
III.5. Mécanismes de sécurité dans 4G/LTE : 34
III.5.1. La sécurité de l'eNB : 34
III.5.2. La Sécurité dans EPS : 35
III.5.3. La Sécurité dans l'IMS : 36
III.5.4. La Sécurité NAS : 37
III.5.5. La Sécurité AS : 37
III.5.6. Développement des procédures adaptées : 37
III.7. Conclusion : 39
Chapitre IV 40
Chapitre IV Simulations et amélioration de la sécurité pour signaux mobile 4G/LTE 40
IV.1. Introduction : 41
IV.2. Méthode développée pour l'amélioration de la sécurité LTE : 41
IV.2.1. Réalisation du réseau : 42
IV.3. Les résultats des configurations de bases : 48
IV.3.1. Vérification en mode SIMULATION : 49
IV.3.2 Vérification de la connectivité entre les 2 entreprises : 49
IV.4. La mise en œuvre de la solution de sécurité Configuration du VPN-IPSec : 50
IV.5. Simulation et Résultats des configurations : 52
IV.5.1 En mode simulation : 52

IV.5.2 Vérification du MAP du VPN : 53
IV.5.3 Réalisation d'un ping : 54
IV.6. Conclusion : 55
Conclusion Générale 56
Références 57

Introduction Générale

En seulement deux décennies, les réseaux mobiles et sans fil ont connu une évolution spectaculaire. Initialement, ces réseaux étaient exclusivement dédiés à la téléphonie (2G, GSM), avant de s'orienter vers le multimédia (3G, UMTS). Les réseaux locaux sans fil, tels que le Wifi et le Bluetooth, sont devenus courants dans la vie quotidienne. La quatrième génération de réseaux mobiles, ou 4G, représente un tournant majeur en intégrant des solutions plus diversifiées. Les réseaux LTE (Long Term Evolution) sont déployés mondialement, utilisant la commutation de paquets et le protocole IP. Contrairement aux générations précédentes basées sur la commutation de circuit, cette transition vers la commutation de paquets expose à de nouvelles formes d'attaques.

Certaines implémentations de réseaux LTE et d'applications mobiles présentent actuellement des vulnérabilités, pouvant entraîner des pertes de confidentialité, des facturations incorrectes et des falsifications de données. Cela soulève la question de comment sécuriser les réseaux LTE à l'aide de mécanismes de sécurité tels que l'authentification, le chiffrement et la confidentialité pour protéger les systèmes d'information et les réseaux 4G/LTE contre les risques de piratage et d'intrusion, Cette problématique engendre plusieurs questions :

- Quelles sont les différentes générations de téléphonie mobile ?
- Quelles sont les spécificités et technologies des réseaux 4G/LTE ?
- Quelles menaces pèsent sur la sécurité des réseaux 4G/LTE ?
- Comment améliorer et protéger la sécurité des réseaux 4G/LTE ?

Pour répondre à ces questions, notre travail est structuré en quatre chapitres. Le premier chapitre introduit les Généralité sur les réseaux mobiles pour mieux comprendre le contexte. Le deuxième chapitre est consacré à la présentation de la 4G/LTE. Le troisième chapitre se focalise sur les La sécurité dans le réseau mobile 4G/LTE, étant donné que notre projet met l'accent sur la sécurité de cette génération de réseau, Le quatrième chapitre présente l'architecture du réseau 4G/LTE lors de la connexion au réseau TCP/IP et les attaques potentiellement dévastatrices pour les entreprises connectées à ce réseau. Pour y remédier, nous avons simulé notre solution en utilisant le simulateur PACKETTRACER, qui nous a permis de mettre en place un VPN utilisant le protocole IPSec (VPN est une connexion permettant une transmission de données sécurisée entre deux sites distants via le réseau IP, grâce au principe de tunneling. Divers protocoles de sécurité peuvent être utilisés pour mettre en œuvre un VPN, mais nous nous concentrons sur le protocole IPSecurity).

Nous concluons par une conclusion générale et des perspectives.

Chapitre I

Généralité sur les réseaux mobiles

I.1. Introduction :

Les réseaux hertziens englobent tous les systèmes de communication exploitant les ondes radio. Ces réseaux se manifestent sous la forme de réseaux cellulaires, constitués de zones géographiques distinctes appelées cellules, dotées d'antennes situées au centre.

Les réseaux mobiles font partie de la catégorie des réseaux hertziens cellulaires, permettant aux utilisateurs de passer d'une cellule à une autre sans interruption de communication. Les échanges entre utilisateurs mobiles connaissent une croissance rapide et représentent un marché considérable pour cette décennie.

Cinq générations de réseaux mobiles se sont succédées, qui se distinguent par la nature de la communication transportée :

- **1G:** communication analogique.
- **2G:** communication numérique sous forme de circuit.
- **3G:** communication sous forme de paquet; sauf pour la parole.
- **4G:** communication multimédia sous forme de paquet de haut debit.
- **5G:** communication multimédia et service du Cloud (1)

Dans ce chapitre, nous expliquerons brièvement les caractéristiques de chaque générations et éventuellement leurs architectures.

I.2.Evolution des réseaux mobiles :

L'évolution des réseaux mobiles a connu plusieurs étapes importantes, marquées par l'introduction de nouvelles technologies et normes. Voici un aperçu de cette évolution:

- **1G (Première génération) :** Lancée dans les années 1980, la 1G était basée sur la technologie analogique et permettait uniquement les appels vocaux. Les réseaux 1G étaient limités en termes de capacité et de qualité sonore.
- **2G (Deuxième génération) :** Introduite dans les années 1990, la 2G a marqué la transition vers la communication numérique. Les technologies telles que le GSM (Global System for Mobile Communications) et le CDMA (Code Division Multiple Access) ont été déployées, offrant des services vocaux améliorés ainsi que des fonctionnalités de messagerie texte.
- **3G (Troisième génération) :** Déployée à la fin des années 1990 et au début des années 2000, la 3G a introduit des vitesses de données plus élevées, permettant l'accès à Internet sur les téléphones mobiles. Les normes telles que l'UMTS (Universal Mobile Télécommunications System) et le CDMA2000 ont été utilisées pour offrir une connectivité à large bande passante.
- **4G (Quatrième génération) :** Lancée dans les années 200, la 4G a représenté une avancée majeure en termes de vitesse, de capacité et de performances. Les normes LTE (Long Term Evolution) et WiMax ont permis des vitesses de téléchargement plus rapides, une latence réduite et une meilleure prise en charge des applications multimédias gourmandes en données.

- **5G (Cinquième génération) :** Actuellement en cours de déploiement, la 5G promet des performances révolutionnaires, avec des vitesses de données ultra-rapides, une latence ultra-faible et une capacité massive pour prendre en charge un grand nombre d'appareils connectés simultanément. La 5G ouvre la voie à de nouvelles applications et services innovants, tels que l'Internet des objets (IoT), les véhicules autonomes et la réalité augmentée.

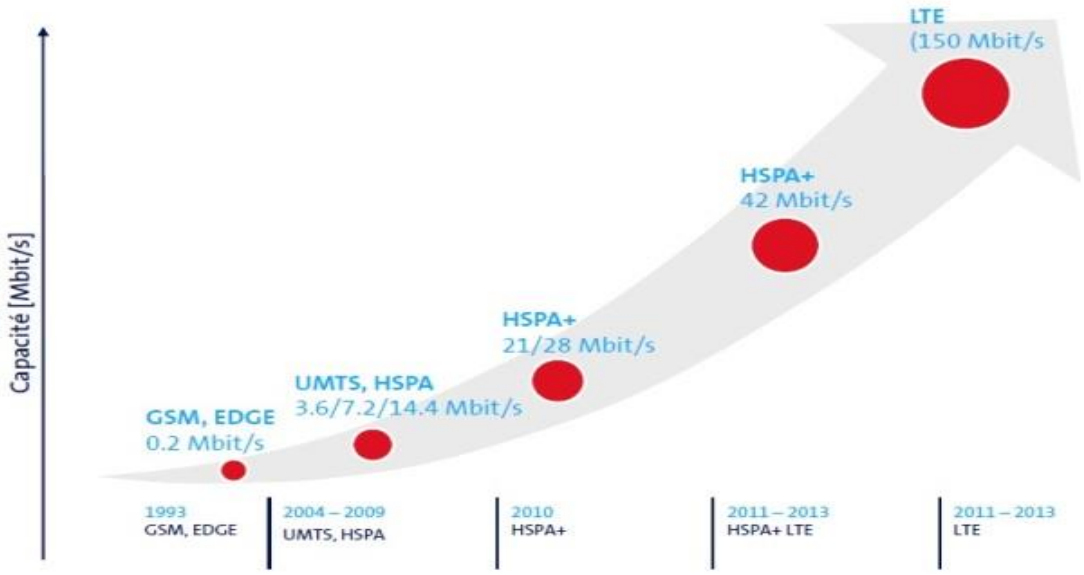


Figure 1 L'évolution des réseaux mobile (2)

I.3. Les différentes normes téléphoniques mobiles sans fil :

Afin de comprendre la technologie actuellement utilisée, il est essentiel de retracer l'évolution des techniques employées. Cette démarche nous permettra de mieux appréhender nos origines et de nous situer de manière plus précise dans le contexte 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 (3).

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.

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 :

I.3.2.1 GSM (Global System for Mobile(2G)):

GSM est la première norme de la téléphonie cellulaire qui est pleinement numérique (1). C'est la référence mondiale pour les systèmes radio mobiles. Le réseau GSM o re à ses abonnés des services qui permettent la communication de stations mobiles de bout en bout à travers le réseau. La téléphonie numérique améliore également la sécurité des transmissions de la voix qui est le service le plus important du GSM et des données à faibles débits. Le système GSM fait appel à la technique TDMA et fonctionne dans les bandes de fréquences des 900, 1800 et 1900 MHz (5).

La structure du reseau GSM : L'architecture du réseau GSM (cf.Figure 2)se décompose en quatre sous-ensembles :

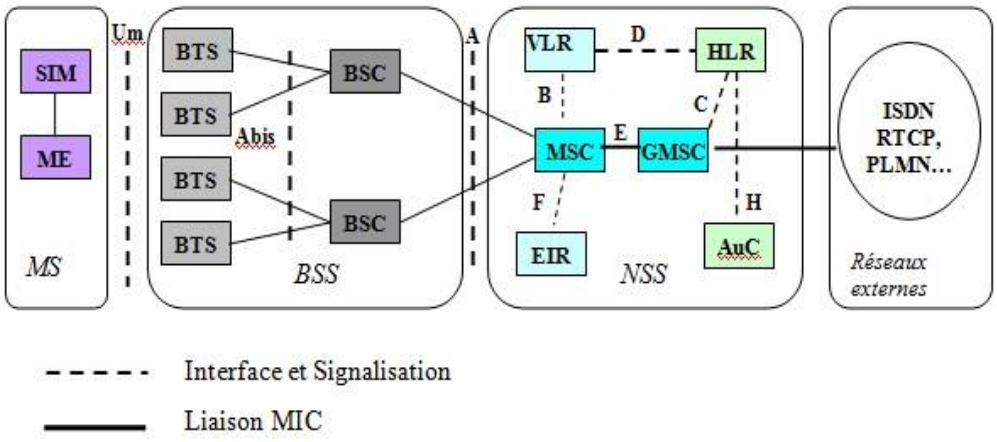


Figure 2 Architecture du réseau GSM

✓ **MS (La station Mobile):**

La station mobile (SM) se compose de l'équipement physique utilisé par un abonné pour se connecter au réseau. Il comprend l'équipement mobile et le module d'identité d'abonné (une puce SIM). A chaque mobile GSM est attribué un unique numéro IMEI (International Mobile Equipement Identity) codé sur au plus 15 chiffres, mis dans la mémoire du mobile lors de sa fabrication qui dépend :

- Du fabricant,
- du modèle,
- du numéro desérie.

✓ **Le sous-système radio BSS (Base Station Sub-system) :**

C'est l'ensemble des constituants du réseau d'accès qui gère l'échange et la transmission des données par voie hertzienne.Le BSS est principalement constitué de deux éléments (6):

- **La station de base BTS :** c'est l'équipement de transmission radio du réseau GSM.
- **Le contrôleur de stations de base BSC :** c'est un équipement qui peut contrôler une ou plusieurs BTS.

✓ **Le Sous-système réseau NSS (Network Sub-System) :**

Le NSS (Network Switching Sub-System) assure les fonctions de commutation et de routage, facilitant l'accès au réseau public RTCP. En plus des fonctions de base de commutation, il intègre des fonctions de gestion de la mobilité, de la sécurité et de la confidentialité conformes à la norme GSM.

Le NSS (Network Sub-System) est composé de commutateurs et de bases de données utilisateura qui sont :

- **MSC** (Mobile services Switching Centre) : Ce commutateur gère la gestion des appels ainsi que tous les aspects liés à l'identité des abonnés, leur enregistrement et leur localisation.
- **GMSC** (Gateway MSC) : Sa fonction principale est d'assurer le routage des appels vers d'autres opérateurs téléphoniques (**exemple** appel de mobilis vers djezzy, ou l'inverse).
- **HLR** (Home Location Register) : C'est une base de données opérée par l'opérateur, contenant des informations relatives aux abonnés.
- **VLR** (Visitor Location Register) : C'est une base de données temporaire contenant des informations sur les abonnés visiteurs.
- **EIR** (Equipment IdentityRegister) : C'est une base de données auxiliaire contenant les identités des terminaux, notamment les numéros IMEI.

- **UC** (AuthenticationCenter) : Mémorise la clé secrète IMSI de chaque abonné pour authentifier les demandes de services et assurer le chiffrement des communications.

✓ **Le Sous-système OMC (Operations and Maintenance Center):**

L'OMC (Operation and Maintenance Center) est responsable de la gestion et de l'exploitation du réseau, combinant la gestion administrative des abonnés et la gestion technique des équipements. La gestion administrative et commerciale implique des actions telles que la création, la modification et la suppression d'abonnements, ainsi que la facturation, nécessitant une interaction avec la base de données HLR. La gestion technique se concentre sur la disponibilité et la configuration matérielle optimale des équipements, incluant la supervision des alarmes, la résolution de dysfonctionnements, la gestion des versions logicielles, la performance et la sécurité.

I.3.2.2 GPRS (General Packet Radio Service (2.5G)):

Le GPRS représente une évolution majeure du GSM. Par l'utilisation de la com mutation de paquets et l'augmentation des débits (7). Il ouvre la porte aux applications mobiles multimédias et il permet la transition en douceur vers la troisième génération. Le GPRS a la possibilité d'allouer 8 times slots d'une porteuse GSM à un instant donné à un utilisateur, ce qui lui permet d'a cher un débit crête de $8\ x\ 21.4\ kbit/s\ soit\ 171.2\ kbit/s$ (8), moyennant l'utilisation d'un codage canal dé ni spécialement pour ce service.

La structure du reseau GPRS :

Le réseau GPRS et le réseau GSM fonctionnent en parallèle (cf.Figure 3), le premier est utilisé pour le transport des données, et le second pour les services de la voix. Tous les deux utilisent les mêmes équipements BSS.

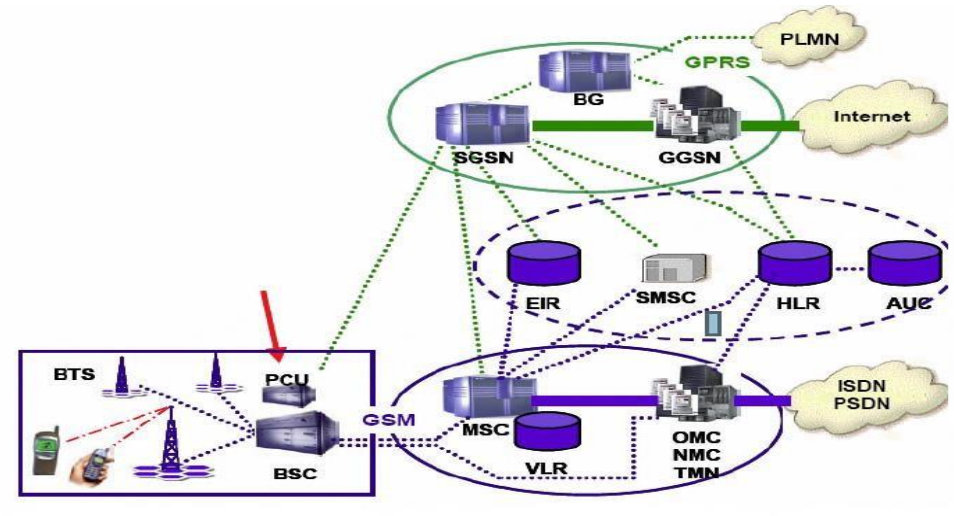


Figure 3 Architecture du réseau GPRS

Les éléments propres au GPRS sont :

Le réseau GPRS comprend les mêmes entités dans le reseau GSM, avec l'ajout de quelques Nouvelle (Les entités sont : PCU dans le sous système BSS, et le SGSN et GGSN dans le sous système NSS).

- ✓ **PCU (Packet Control Unit):** cet équipement gère les fonctions de couches basses, c'est a-dire les protocoles RLC (Radio Link Control), MAC (Medium Acces Control),contrôle de puissance, adaptation des débits, … pour envoyer sur le réseau «GPRS ». Il gère les fonctions de transmissions et d'acquittements.
- ✓ **SGSN** (**Serving GPRS Support Node):** serveur d'accès au service GPRS (equivalent au MSC), et qui gère les MS présentes dans une zone donnée. Son rôle est de délivrer des paquets aux MS.
- ✓ **GGSN** (**Gateway GPRS Support Node):** routeur connectant le réseau GPRS et un réseau externe de commutation par paquets (IP). Il sert de passerelle entre les SGSN du réseau GPRS et les autres réseaux de données.

I.3.2.3 EDGE (Enhanced Data rate for GSM Evolution (2.75G)):

l'introduction d'une nouvelle modulation $(8PSK)$ (9), de nouveaux schémas de codage et la généralisation du principe de l'adaptation de lien (link adaptation). La norme EDGE propose des débits presque trois fois plus important que le GPRS, allant jusqu'à $43.2\ kbit/s$ par time slot GSM (6).

EDGE et le GPRS (cf.Figure 4) permettent ensemble de doper le réseau GSM/GPRS a n d'o rir à l'utilisateur les moyens de transmettre des données à des débits très loin des $9{,}6\ kbit/s$ du GSM (jusqu'à $384\ Kbit/s$)

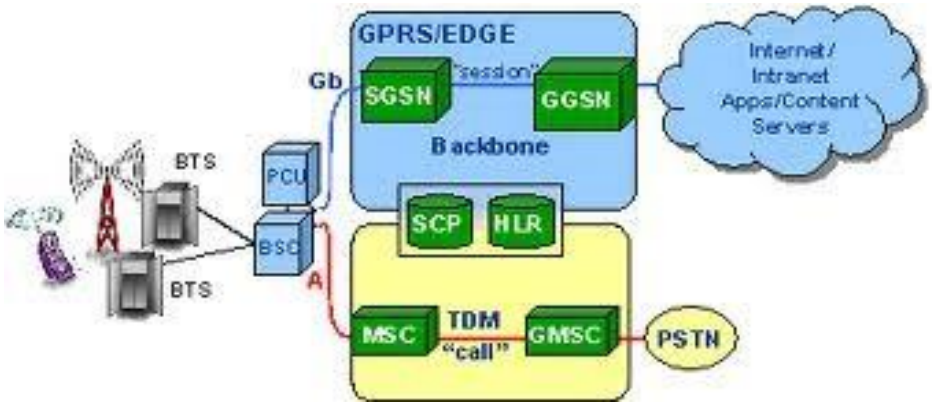


Figure 4 Architecture du réseau EDGE

Le déploiement de L'EDGE nécessite :

- ✓ La mise à jour du BSC et de la BTS.

- ✓ L'ajout d'un émetteur et 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) :

Les réseaux de télécommunications mobiles de troisième génération offrent une gamme complète de services de communication aux utilisateurs fixes et mobiles, présents dans divers environnements autour de la bande de fréquences de 2 GHz. Ils améliorent les infrastructures précédentes en garantissant une qualité de service au moins équivalente à celle des réseaux fixe.

Un autre objectif des réseaux de troisième génération est de rendre les services fixes et mobiles compatibles pour former un service transparent de bout en bout pour les utilisateurs.

I.3.3.1 Réseau UMTS (Universal Mobile Télécommunications System) :

L'UMTS représente une évolution dans les services et les vitesses de transfert de la deuxième génération à la troisième génération (10). Elle représente une voie privilégiée pour le développement de produits et services multimédias.

En parallèle avec l'évolution d'Internet qui propose désormais une gamme diversifiée de services spécialisés tels que la banque en ligne, les achats en ligne, les jeux, et les informations variées, les opérateurs, motivés par cette tendance, déploient des services permettant d'accéder à ce nouveau média via la téléphonie mobile.

Cependant de nouveaux protocoles plus performants sont indispensables pour proposer une nouvelle gamme de services à haut débit allant de l'Internet au téléchargement de musique ou de lm. C'est ce qu'apporte l'UMTS.

La structure du réseaux UMTS :

L'architecture générale d'un réseau UMTS est composée de quatre domaines qui sont reliés par des interfaces tel que Uu et Iu (cf. Figure 7) (8).

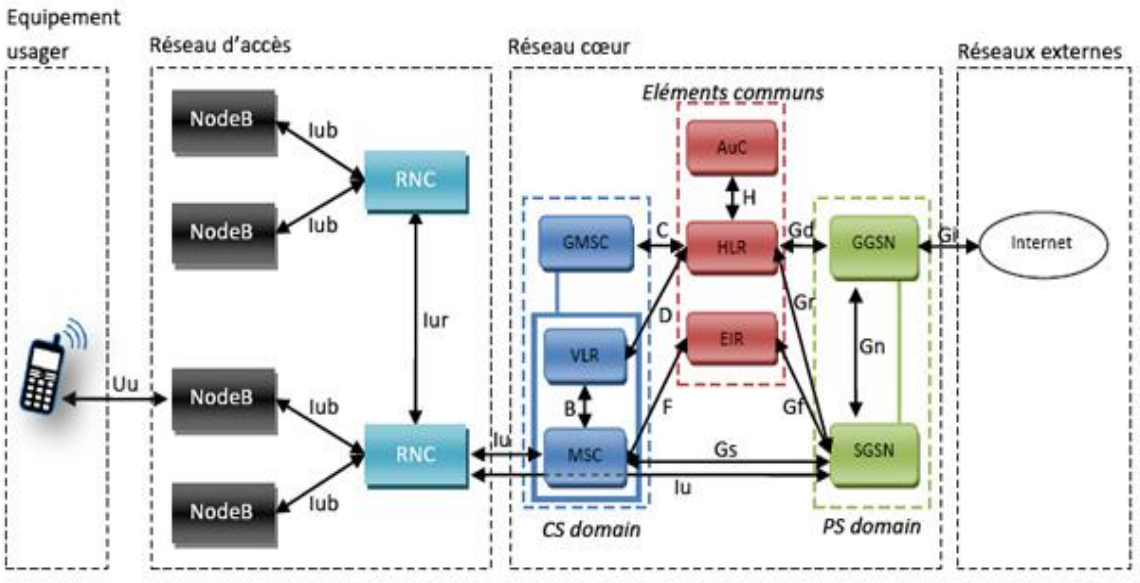


Figure 5 Architecture globale du réseau UMTS

Les trois domaines sont dé nits comme suit :

1. **Domaine de l'équipement de l'usager UE :**

Ce domaine est composé de :

- ✓ **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.
- ✓ **La carte USIM** : La carte USIM assure la sécurité du terminal et la confidentialité des **communications.**

2. **Domaine du réseau d'accès UTRAN :**

Le réseau d'accès radio de l'UMTS est complètement différent de celui du GSM. Il comporte des éléments tels que les NodeB (équivalent des BTS en GSM) et les RNC (Radio Network Controller) quicorrespondent aux BSC dans le cas du GSM.

- ✓ **Le « Node B » :** Les NodeB convertissent les flux de données entre les interfaces Iub et Uu et en même temps ils participent à la gestion des ressources radio.
- ✓ **Le « RNC » :** Quant au RNC il gère les ressources radio de la zone dont il a le contrôle, c'est le point d'accès pour tous les services fournis par l'UTRAN au réseau cœur.

3. Domaine du réseau cœur:

Le réseau cœur de l'UMTS est quant à lui scinder en deux parties, une partie s'occupe de la commutation en mode circuit **CS (Circuit Switched)** et la deuxième partie est un réseau à commutation de paquet **PS (Packet Switched)**.

Le réseau à commutation de circuit **CS (Circuit Switched)** est conçu à l'image du réseau cœur GSM et contient, les éléments tels que le **MSC/VLR** et le **GMSC** comme le cas d'un GSM. Les fonctions de ces éléments restent les mêmes que pour les réseaux de 2G. Le réseau à commutation paquet **PS (Packet Switched)**. lui aussi est conçu à l'image du réseau cœur GPRS avec des éléments comme le SGSN et le GGSN. Ce réseau paquet peut être relié à un réseau paquet public ou a un autre réseau paquet d'un autre opérateur. Le réseau entre le GGSN et le SGSN est généralement un réseau IP. en plus des éléments communs aux domaines CS et PS (**AUC/ EIR /HLR**) Les fonctions de ces éléments restent les mêmes que pour les réseaux de 2G.

A cette architecture sont appliquées des strates fonctionnelles permettant de séparer les différentes fonctions en groupes indépendants.

Les interfaces de communication : Plusieurs types d'interfaces de communication coexistent au sein du réseau UMTS (11):

- ✓ **Uu:** Interface entre un équipement usager et le réseau d'accès UTRAN. Elle permet la communication avec l'UTRAN via la technologie CDMA.
- ✓ **Iu**: Interface entre le réseau d'accès UTRAN et le réseau cœur de l'UMTS. Elle permet au contrôleur radio RNC de communiquer avec le SGSN.
- ✓ **Iur:** Interface qui permet à deux contrôleurs radio RNC de communiquer.
- ✓ **Iub:** Interface qui permet la communication entre un NodeB et un contrôleur radio RNC

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

La norme LTE (Long Term Evolution) permet le déploiement du "très haut débit mobile", ce qui implique des transmissions de données à des débits théoriques dépassant les 100 Mbit/s, voire dépassant 1 Gbit/s selon les spécifications IMT-Advanced pour la norme LTE Advanced définies par l'UIT. En pratique, les débits varient généralement de quelques dizaines de Mbit/s en fonction du nombre d'utilisateurs, car la bande passante est partagée entre les terminaux actifs des utilisateurs dans une même cellule radio.

Une caractéristique majeure de la 4G est l'utilisation d'un "cœur de réseau" basé sur IP, sans mode commuté pour les communications téléphoniques, ce qui signifie que la voix sur IP (VoIP) est utilisée pour les appels vocaux, fonctionnant en mode paquet.

Avec la 4G, il y a une transition vers la transmission de toutes les informations, qu'il s'agisse de voix ou de données, via IP, le même protocole utilisé sur Internet. Pour les fournisseurs, cela

représente une gestion plus simple et moins coûteuse, tout en facilitant le développement d'applications multimédias. Cette technologie offre des vitesses de téléchargement plus rapides et des temps de latence plus courts.

Tableau 1 Différents Paramètres du LTE / LTE-Advanced (12)

		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	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

I.3.5 La cinquième génération des téléphones mobiles (5G) :

Ces derniers temps,on entend parler de la cinquième génération. Cette technologie de base a un but pas di érente de la quatrième génération mais les di érences sont architecturales qui sont dé nit comme suit (1):

L'introduction de Cloud : Il joue un rôle important pour prendre en charge le contrôles des réseaux mobiles. Il apporte une puissance de calculer et de récupérer l'information. Il permet aussi de prendre des décisions tenant compte d'un très grand nombre de paramètres. On peut parler du Cloud distribué ou local.

Utilisation fort de la virtualisation : L'idée principale de la virtualisation est de partager des équipements du réseau entre plusieurs opérateurs et plus généralement entre les utilisateurs. Elle peut permettre la coexistence de réseaux hétérogène puisque les réseaux sont isolés les uns des autres.

Les plates formes d'altitude : C'est la partie la plus visible de cette génération, car il utilise deux plates forme d'altitude :

- les plates forme à haute altitude, où on la trouve dans une position stratosphérique de l'ordre de 18 à 22 km dont la couverture se compte en centaine de kilomètre carrés.

- les plates formes de basse altitude peuvent se positionner de quelque dizaines de mètre de hauteur jusqu'à plusieurs kilomètres, la couverture étant de quelque kilomètres carrés.

L'avantage de ces plates-formes provient d'une capacité de communication pouvant couvrir un million de personnes avec un haut débit et un matériel de l'ordre de 20.

L'architecture 5G offre des débits de données élevés, pouvant atteindre plusieurs gigabits par seconde, et une latence réduite à moins d'une milliseconde. Elle gère également intelligemment le trafic pour maintenir une expérience utilisateur de haute qualité même en période de pointe. La 5G supporte également une grande densité d'appareils connectés, qui communiquent entre des milliards d'objets intelligents.

I.4. Conclusion :

Dans ce chapitre, nous avons examiné de manière générale les différentes phases de l'évolution de la téléphonie mobile et les caractéristiques principales des réseaux cellulaires. Nous avons débuté avec la 1G, apparue dans les années 80, qui a servi de point de départ pour toutes les générations suivantes. Cependant, ses limites ont nécessité le développement de la 2G, qui est toujours en usage aujourd'hui, mais avec des améliorations par rapport à la précédente. La 3G, quant à elle, a apporté de nouvelles fonctionnalités telles qu'un haut débit pour l'accès à Internet et le transfert de données. Passage par la quatrième generation(4G), puis suivie par la cinquième generation(5G).

Étant donné que notre projet se concentre davantage sur la sécurisation du réseau de la quatrième génération (4G/LTE), nous allons approfondir l'étude des réseaux 4G/LTE dans le chapitre à venir.

Chapitre II

Réseau mobile 4G /LTE

II.1. Introduction :

La 4G LTE, abréviation de "Long Term Evolution", est une technologie de communication sans fil qui offre des performances améliorées par rapport à ses prédécesseurs, comme la 3G. Elle a révolutionné la connectivité mobile en offrant des vitesses de téléchargement et de téléversement beaucoup plus rapides, une latence réduite et une capacité accrue pour prendre en charge un plus grand nombre d'appareils connectés simultanément.

Ce chapitre a pour objectif de présenter la 4G/LTE, les différents éléments importants de notre projet tels que: la stratégie de mise en place par le réseau radio mobile LTE, les spécificités et aussi les technologies de transmission de la qualité de services dans le réseau 4G.

II.2. Définition de la 4G/LTE :

LTE (Long Term Evolutionof UMTS) est un projet mené par la 3GPP (3G) et a été considéré comme une norme de 3éme génération (3,9G) proche de la 4G. Elle permet d'atteindre des débits théoriquesde 100 Mbit/s en voie descendante et 50 Mbit/s en voie montante pour une largeur de bande de 20Mhz, avec une très grande portée, un grand nombre d'appels simultanés, une faible latence et une capacité élevée.

En réalité, l'ensemble de ce réseau s'appelle EPS (Evolved Packet System), et il est composé d'UE (User Equipment), l'EPC (Evolved PacketCore) et l'E-UTRAN (Evolved UTRAN).

II.3. Objectifs de la 4G/LTE :

La 4G cherche à accroître la capacité de gestion du nombre de téléphones mobiles dans une seule zone. Elle efforce également de proposer des débits élevés lors de déplacements et de garantir une mobilité totale à l'utilisateur en permettant l'interopérabilité entre différentes technologies existantes. Elle vise à rendre la transition entre réseaux fluide pour l'utilisateur, à éviter toute interruption de service pendant les transferts intercellulaires et à migrer vers une utilisation entièrement basée sur IP.Les réseaux de 4e génération ont pour principaux objectifs: (13)

- Assurer la continuité de la session en cours.
- Réduire les délais et le trafic de signalisation.
- Fournir une meilleure qualité de service.
- Minimiser le cout de signalisation.
- Optimiser l'utilisation des ressources.
- Réduire le délai de relève, le délai de bout en bout, la perte des paquets.

II.4. Architecture de la 4G/LTE :

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.

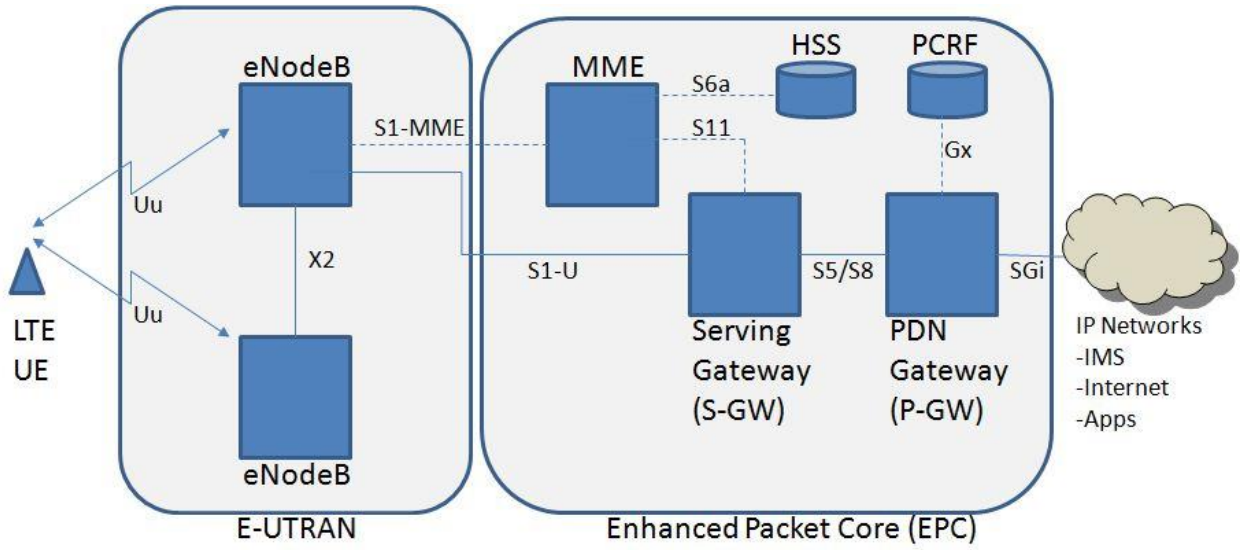


Figure 6 Architecture LTE (14)

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.

II.4.1 Équipement Utilisateur (UE) :

C'est l'équipement utilisé par l'utilisateur pour accéder à divers services fournis par l'UMTS via l'interface radio UTRA.

Le 3GPP (3rd Generation Partnership Project), qui supervise cette norme, l'améliore continuellement, notamment pour augmenter les vitesses et accueillir un plus grand nombre d'abonnés. Les normes associées à cette génération incluent :

- La norme HSDPA (High Speed Downlink Packet Access) : elle offre des performances dix fois supérieures à la 3G, uniquement sur le flux descendant.
- La norme HSUPA (High Speed Uplink Packet 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 ; elle est une évolution de la norme HSPA permettant d'atteindre des vitesses de : 42 Mb/s (montant) et 11 Mb/s (descendant).

II.4.2 Réseau d'accès E-UTRAN :

Le Réseau d'Accès Terrestre UMTS Évolué :

La partie radio du réseau, connue sous le nom de "e-UTRAN", est simplifiée par rapport aux réseaux 2G et 3G en raison de l'intégration des fonctions de contrôle dans les stations de base "eNodeB". Ces fonctions 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, des antennes locales ou distantes, des liaisons en fibres optiques vers les antennes distantes et des liens IP reliant les eNodeB entre eux (liens X2) et avec le réseau cœur.

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

Cette figure décrit l'architecture de l'e-UTRAN avec ses eNodeB, les interfaces X2 (entre les eNodeB) et S1 (entre

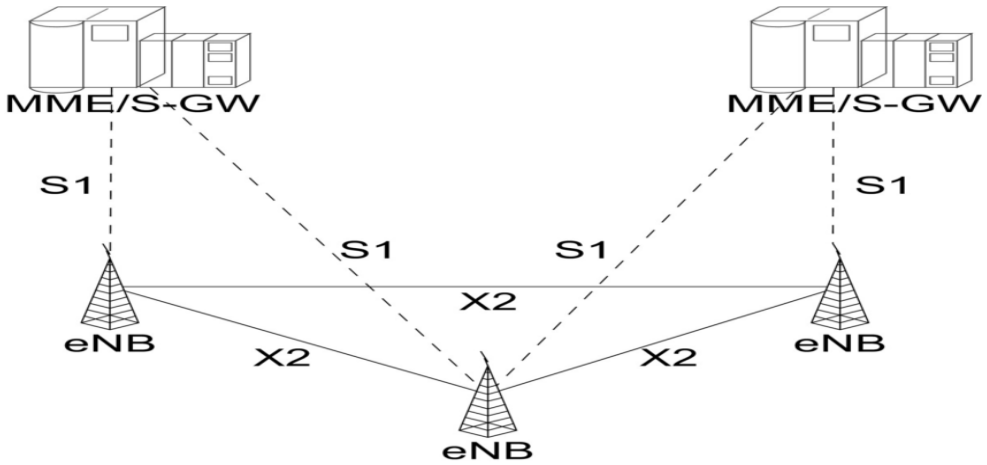


Figure 7 Architecture de l'E-UTRAN (15)

- **L'eNodeB :**

L'eNodeB est l'équivalent de la BTS dans le réseau GSM et du NodeB dans l'UMTS. La fonctionnalité de transfert intercellulaire est plus robuste dans LTE. Ce sont des antennes qui connectent les UE (équipements utilisateur) avec le réseau cœur LTE via l'interface radio RF (Radio Fréquence). La fonctionnalité du contrôleur radio réside dans l'eNodeB, ce qui rend le réseau plus efficace et moins latent, par exemple, la mobilité est déterminée par l'eNodeB plutôt que par le BSC ou le RNC des réseaux GSM et UMTS. Les eNodeB sont reliés entre eux par une interface X2.

- **L'interface S1:**

C'est l'interface intermédiaire entre le réseau d'accès et le réseau cœur, et 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.

- **L'interface X2 :**

Il s'agit d'une interface logique, introduite dans le but de permettre aux eNodeB d'échanger des informations de signalisation lors d'un transfert intercellulaire (Handover) ou de la signalisation, sans impliquer le réseau cœur. Lorsque l'utilisateur 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 ; toutefois, le réseau continue de transmettre ses données à l'ancien eNodeB tant qu'il n'a pas été informé du changement. Pour minimiser la perte de ses paquets de données, l'ancien eNodeB relaie les paquets entrants sur l'interface X2 vers le nouvel eNodeB qui les délivre à l'UE. L'eNodeB est connecté au cœur du réseau via l'interface S1.

II.4.3 Réseau Cœur EPC (Evolved Packet Core) :

Le cœur de réseau, appelé EPC (Evolved Packet Core), utilise des technologies entièrement basées sur le protocole IP, c'est-à-dire les protocoles Internet, pour la signalisation ainsi que pour le transport de la voix et des données. Ce cœur de réseau permet l'interconnexion, via des routeurs, avec d'autres eNodeB, les réseaux d'autres opérateurs mobiles, les réseaux de téléphonie fixe et l'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 grâce à des équipements comme le MME, le SGW, le PDN-GW (Packet Data Network Gateway) et le PCRF (Policy and Charging Rules Function) (16).

L'utilisation du protocole IP de bout en bout dans le cœur du réseau permet de réduire les temps de latence pour l'accès à Internet et les appels vocaux LTE. Son architecture est simplifiée, comme le montre la figure, en comparaison avec celle des réseaux 2G/3G.

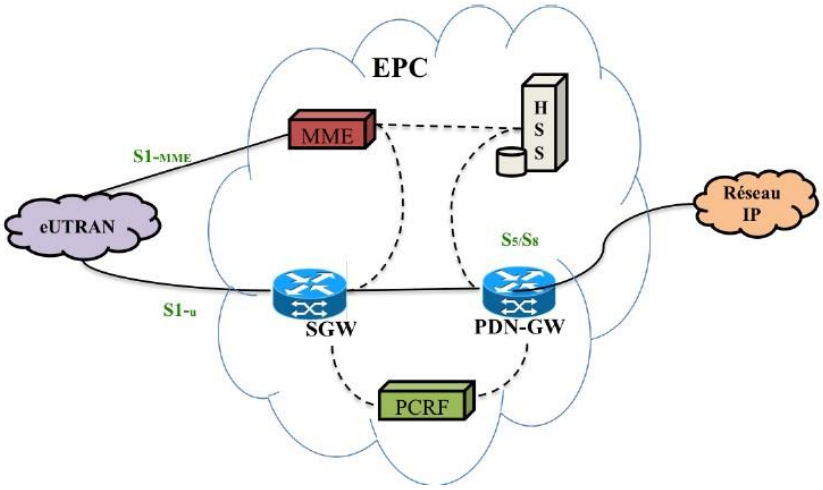


Figure 8 Architecture EPC (16)

Le réseau cœur EPC est décomposé en :

- **Signalisation EMM et ESM avec l'UE :** Les terminaux LTE utilisent les protocoles EMM (EPS Mobility Management) et ESM (EPS Session Management) pour gérer leur mobilité (attachement, détachement, mise à jour de localisation) et leurs sessions de données (établissement et libération). Ces protocoles sont échangés entre l'UE et le MME.
    1. **Authentification :** Le MME est responsable de l'authentification des UE en utilisant les informations recueillies auprès du HSS.
    2. **Joignabilité de l'UE en état ECM-IDLE (incluant le paging) :** Le MME est responsable du paging lorsque l'UE est en état IDLE et que des paquets destinés à l'UE sont reçus et mis en mémoire par le Serving GW.
    3. **Gestion de la liste de Tracking Area (localisation) :** Le MME informe l'UE des zones de localisation prises en charge, appelées Tracking Areas. L'UE met à jour sa localisation lorsqu'il entre dans une Tracking Area non prise en charge par son MME.
    4. **Sélection du Serving GW et du PDN GW :** Le MME est responsable de sélectionner le Serving GW et le PDN GW.
    5. **Sélection de MME lors du handover avec changement de MME**: Lorsque l'utilisateur est en état ACTIF et qu'il se déplace d'une zone contrôlée par un MME à une autre zone sous le contrôle d'un autre MME, le handover doit impliquer à la fois l'ancien et le nouveau MME.
    6. **Sélection du SGSN lors du handover avec les réseaux 2G et 3G**: Si l'utilisateur passe d'une zone LTE à une zone 2G/3G, le MME est responsable de sélectionner le SGSN.
    7. **Roaming avec interaction avec le HSS nominal** : Lorsqu'un utilisateur se connecte au réseau, le MME interagit avec le HSS nominal pour mettre à jour la localisation du mobile et obtenir le profil de l'utilisateur.
    8. **Interception légale du trafic de signalisation :** Le MME reçoit toute la signalisation émise par l'UE et peut l'archiver à des fins de traçabilité.

- **Serving-GW (Serving Gateway):** Les fonctions de l'entité Serving GW incluent :

1. **Point d'ancrage pour le handover inter-eNodeB :** Lors d'un handover entre eNodeB, le trafic de l'utilisateur, précédemment échangé entre l'ancien eNodeB et le Serving GW, doit maintenant être relayé du nouvel eNodeB vers le Serving GW.
2. **Point d'ancrage pour le handover entre LTE et les réseaux 2G/3G :** Le Serving GW relaye les paquets entre les systèmes 2G/3G et le PDN-GW. Lors d'une mobilité entre LTE et les réseaux 2G/3G, le SGSN du réseau 2G/3G s'interface avec le Serving GW pour assurer la continuité du service de données.
3. **Routage et relais des paquets :** Le Serving GW route les paquets sortants vers le PDN-GW approprié et relaie les paquets entrants vers l'eNodeB qui dessert l'UE.
4. **Comptabilité par usager pour la taxation inter-opérateurs :** Le Serving GW comptabilise le nombre d'octets envoyés et reçus, permettant l'échange de tickets de taxation entre opérateurs pour les reversements.

- **PDN-GW (Packet Data Network Gateway):**

Les fonctions de l'entité PDN GW incluent :

1. **Interface vers les réseaux externes (Internet et intranet) :** Le PDN GW termine le réseau mobile EPS et assure l'interface avec les réseaux externes IPv4 ou IPv6.
2. **Allocation de l'adresse IP de l'UE :** Le PDN GW attribue une adresse IP à l'UE dès son attachement au réseau, lorsque le "default bearer" permanent est établi. Il peut assigner une adresse IPv4 ou IPv6.
3. **Interception légale :** Le PDN GW, étant sur le chemin de signalisation pour l'établissement et la libération des bearers ainsi que sur le chemin des paquets de données échangés par l'UE, est un point stratégique pour l'interception légale des flux de données et de contrôle.
4. **Marquage des paquets** dans les sens montant et descendant, e.g., positionnant le DiffServ Code Point (different Service code point: champ dans l'entete d'un paquet IP) sur la base du QCI (QoS Class Identifier) du bearer EPS associé. Cela permet d'associer des priorités aux flux de données au sens DiffServ pour permettre une diversité des services offerts.
5. **Taxation des flux de service montants et descendants :** Le PDN GW s'occupe de la taxation des flux de données, basée sur les règles fournies par le PCRF ou sur l'inspection des paquets définie par des politiques locales.

- **HSS (Home Subscriber Server):** Le HSS est une version avancée du HLR, permettant de stocker des informations d'abonnement utilisées pour le contrôle des appels et la gestion des sessions par le MME. Il conserve les données d'identification des utilisateurs, incluant leur 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 d'autres réseaux tels que le GSM, le GPRS, la 3G, le LTE et l'IMS.

- **PCRF (Policy and Charging Rules Function):** La PCRF remplit principalement deux fonctions importantes :
  - ✓ Elle gère la qualité de service (QoS) requise par le réseau et attribue les porteuses (bearers) adéquates en conséquence.
  - ✓ Elle s'occupe de la tarification en régissant les politiques de facturation que le PDN-GW doit appliquer en fonction des actions de l'utilisateur.

II.5. Les couche du modèle LTE :

Les couches principales de cette technologie :

1) **Couche NAS (Non Access Stratum):** Cette couche gère plusieurs fonctions de contrôle, telles que :
   - ✓ La gestion des accès au réseau.
   - ✓ L'authentification.
   - ✓ La gestion de la mobilité.
   - ✓ La mise en place du porteur de données (data bearer).

2) **Couche AS (Access Stratum):** Cette couche assure la connexion directe entre nous et les eNodeBs, comprenant tous les messages, c'est-à-dire les données utilisateur échangées sur la couche radio pour accéder physiquement à un réseau LTE.

3) **Couche RRC (Radio Resource Control) :** Présente au niveau de l'eNodeB, cette couche effectue plusieurs opérations, dont :
   - ✓ La diffusion des informations du système.
   - ✓ La gestion de la pagination.
   - ✓ L'allocation des identificateurs temporaires aux UE.
   - ✓ La gestion du transfert de la connexion (« handover ») entre deux eNodeB pour l'UE. (17)

4) **Couche PDCP (Packet Data Convergence Protocol) :** Cette couche prend en charge au niveau utilisateur la compression et la décompression des en-têtes IP des données utilisateurs. Les messages de la couche NAS sont chiffrés deux fois, au niveau du MME et de l'eNodeB, car ils traversent la couche RRC.

5) **Couche RLC (Radio Link Control) :** Située sous la couche PDCP, elle formate et transporte les données entre l'eNodeB et l'UE.

6) **Couche MAC (Medium Access Control) de LTE :** C'est l'une des couches les plus importantes du modèle. Elle assure le mappage des données entre les canaux logiques et les canaux de transport en utilisant une fonction de multiplexage de RLC.

7) **Couche physique de LTE (PHY) :** Cette couche utilise la technique OFDMA (Orthogonal Frequency Division Multiple Access) pour le flux descendant (de l'eNodeB vers l'UE) et la technique SC-FDMA (Single Carrier-Frequency Division Multiple Access) pour le flux ascendant. Elle permet aussi d'utiliser trois modes de transmission : Full Duplex FDD (Frequency Division Duplex), Half-Duplex FDD, et TDD (Time Division Duplex). (17)

Remarque:
En comparant l'architecture du réseau LTE avec les réseaux antérieurs, nous pouvons observer que : ✓ L'entité MME remplace le dispositif MSC ce qui offre une architecture simplifiée. ✓ L'entité SGW remplace le dispositif SGSN. ✓ L'entité e-NodeB remplace la BTS/NodeB. ✓ L'entité PGW remplace GGSN.

II.6. Performances et caractéristiques des réseaux LTE :

II.6.1. Les Débits :

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

Tableau 2 débit maximale

débit maximale		
300Mb/s	en voie descendante	pour une largeur de bande allouée de20Mhz
75Mbit/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.

II.6.2. La latence :

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

- **Latence du plan de contrôle :** L'objectif est d'optimiser la latence du plan de contrôle parrapport à l'UMTS, en visant un temps de transition inférieur à 100 ms.

- **Latence du plan utilisateur :** Il s'agit du temps de transmission d'un paquet IP dans leréseau d'accès. L'objectif du réseau LTE est d'avoir une latence du plan utilisateur inférieure à 5 ms.

II.6.3 L'agilité en fréquence :

LTE doit fonctionner sur des porteuses de différentes largeurs de bande afin de s'adapter à diverses allocations de spectre. Les largeurs de bande initialement requises ont été mises à jour pour inclure 1,4 MHz, 3 MHz, 5 MHz, 10 MHz, 15 MHz et 20 MHz.

II.6.4 Codage :

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 le WiFi). Cependant, contrairement à l'OFDM, l'OFDMA est optimisé pour l'accès multiple, permettant le partage simultané de la ressource spectrale (bande de fréquence) entre plusieurs utilisateurs distants les uns des autres.

II.6.5 Le multiplexage :

Il existe deux modes du multiplexage de fréquences :

Tableau 3 Le multiplexage

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

II.6.6 Qualité de service dans le réseau 4G/LTE :

La qualité de service (QDS) ou Quality of service (QoS) est la capacité de transmission dans de bonnes conditions un certain nombre de paquet dans une connexion entre un émetteur et un récepteur.

Les nouveaux besoins en termes de mobilité des utilisateurs et la croissance des réseaux permettant le nomadisme des utilisateurs ont fait migrer le problème vers la des réseaux sans fil. (18)

II.6.6.1 Le porteur EPS (the bearer) :

Le porteur EPS est un tuyau (tunnel) construit entre l'UE et le P-GW selon les caractéristiques contenues dans l'EPS session. Le premier bearer EPS construit, nommé default bearer EPS est mis en place lors de la procédure d'enregistrement.

Un bearer EPS est un tuyau caractérisé par des paramètres de QoS car les applications n'ont pas les mêmes besoins : Certaines applications comme le streaming, la vision et la phonie nécessitent un débit garanti (GBR) alors que le browsing et le téléchargement se suffisent de Best Effort (Débit Non Garanti). (19)

Il existe deux types de porteurs EPS :

- ✓ Le Default bearer, le premier porteur établi lorsque le terminal se connecte un PDN, il reste actif durant toute la connexion.
- ✓ Les Dedicated bearer, tous les porteurs additionnels établis avec le même PDN.

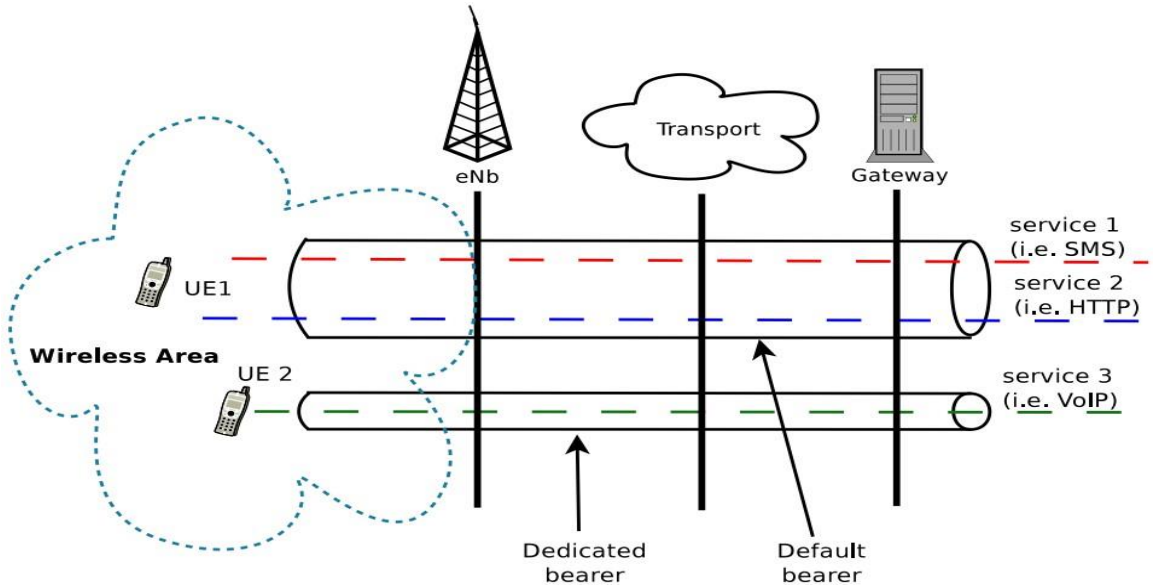


Figure 9 Les types de porteur. (19)

II.7. Conclusion :

L'émergence de la 4G, successeur avancé de la 3G, illustre clairement l'augmentation considérable du développement des réseaux. Il est également évident que l'architecture du réseau 4G/LTE facilite l'évolution en intégrant des technologies plus performantes, permettant ainsi de fournir des services de haute qualité.

Étant donné que notre projet se concentre principalement sur la sécurité des réseaux de quatrième génération 4G/LTE, nous examinerons en détail la sécurité dans les réseaux 4G/LTE dans le chapitre suivant.

Chapitre III

La sécurité dans le réseau mobile 4G/LTE

III.1. Introduction :

Les avancées des réseaux mobiles LTE (Long Term Evolution) ouvrent de nouvelles perspectives pour la croissance et le développement commercial à l'échelle mondiale. En passant de la commutation de circuit à la commutation de paquets et en adoptant le protocole IP, ces réseaux offrent des possibilités inédites. Toutefois, cette transition entraîne également de nouveaux défis en matière de sécurité. Certaines implémentations de réseaux LTE et d'applications mobiles présentent des vulnérabilités à divers niveaux, entraînant des risques tels que la perte de confidentialité, la facturation incorrecte et la falsification de données.

III.2. Les objectifs de la sécurité :

En générale, la sécurité implique de garantir que les ressources matérielles ou logicielles d'une organisation ne sont utilisées que conformément à leur usage prévu.

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

- ✓ 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.

III.3. Architecture de la sécurité :

L'architecture 4G LTE a été développée par le 3GPP en tenant compte des principes de sécurité dès sa création et la conception basée sur cinq groupes de fonctions de sécurité:

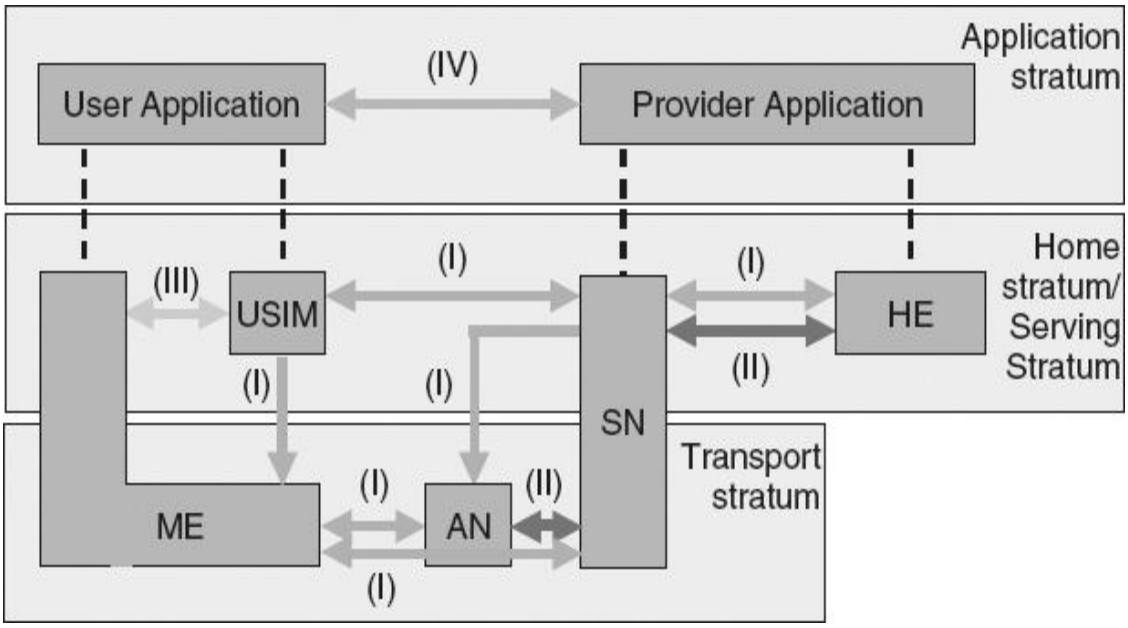


Figure 10 Architecture de sécurité du LTE *(20)*

Comme le montre la figure, le 3GPP définit cinq ensembles de fonctionnalités de sécurité:

(I) **Sécurité d'accès au réseau :** L'ensemble des éléments de sécurité qui permettent aux utilisateurs d'accéder de manière sécurisée aux services, et qui protègent notamment contre les attaques sur la liaison d'accès (radio).

(II) **La sécurité du domaine réseau :** fournit des fonctions de sécurité pour permettre un échange sécurisé des données de signalisation entre les nœuds (entre le réseau d'accès (AN) et le réseau de desserte (SN) et au sein de l'AN) et protège contre les attaques sur le réseau câblé fixe,

(III) **Sécurité du domaine utilisateur :** ensemble de fonctionnalités de sécurité qui sécurisent l'accès aux stations mobiles.

(IV) **Sécurité du domaine d'application :** ensemble de fonctionnalités de sécurité qui permettent aux applications du domaine de l'utilisateur et du fournisseur d'échanger des messages en toute sécurité. (20)

III.4. Vulnerabilities et menaces dans 4G/LTE :

En raison de l'introduction de nouvelles technologies d'accès radio et la transition vers une architecture basée sur IP ont engendré de nouvelles failles dans l'infrastructure réseau, exposant ainsi les réseaux mobiles à diverses menaces. Ces menaces visent les piles de protocoles, les mécanismes de sécurité et les interfaces réseau. Une vulnérabilité dans un réseau mobile désigne une faiblesse intrinsèque de son architecture et de ses composants, pouvant être exploitée par des acteurs malveillants pour mener des attaques.

Par conséquent, une menace est caractérisée par la volonté délibérée d'accéder sans autorisation à des informations, de les manipuler, ou de rendre un système instable ou inoperant. Les menaces auxquelles sont confrontés les réseaux LTE, décrits dans les spécifications du système, peuvent être classées comme suit :

III.4.1. Menaces contre l'identité de l'utilisateur (IMSI catcher) :

Les IMSI Catchers, également connus sous le nom de (Sting rays), sont des appareils de surveillance électronique qui permettent de capturer des informations sur les téléphones portables et sont utilisés pour intercepter les données de télécommunication. Un des premiers points faibles identifié de la sécurité de LTE, et hérité de l'UMTS, est l'envoie de l'identité permanente IMSI en claire.

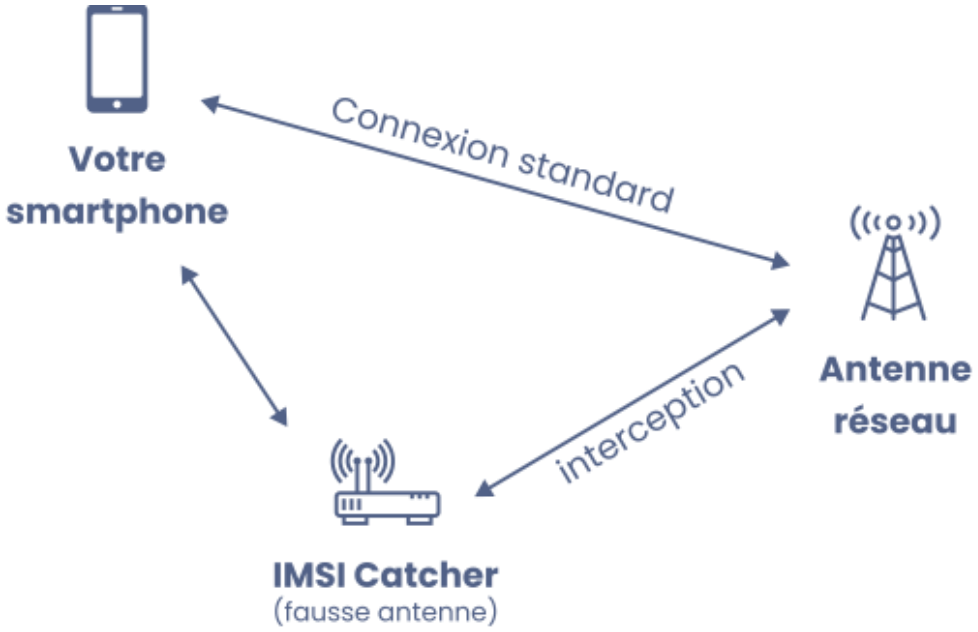


Figure 11 Menaces contre l'identité de l'utilisateur (21)

Les IMSI Catchers fonctionnent en exploitant les vulnérabilités des réseaux de téléphonie mobile, en particulier celles présentes dans le protocole 2G. Ils agissent comme une fausse antenne opérateur, ce qui permet de tromper les téléphones portables à proximité pour qu'ils se connectent au dispositif. Les IMSI Catchers interceptent ensuite les signaux entre le téléphone portable et la véritable antenne, et collectent les informations de communication.

L'IMSI Catcher nécessite un certain niveau de sophistication technique pour être efficace. Il doit être en mesure de générer un signal suffisamment puissant pour attirer les téléphones mobiles à proximité et les convaincre de se connecter à leur réseau plutôt qu'à celui des opérateurs de téléphonie mobile (par exemple : Djezzy, Mobilis….).

Une fois que le téléphone portable est connecté à l'IMSI catcher, l'appareil peut capturer toutes sortes de données sur le téléphone, y compris le numéro IMSI (International Mobile Subscriber Identity) qui identifie le téléphone portable et le numéro de téléphone : les IMSI catchers peuvent intercepter les communications téléphoniques, les SMS et les données Internet échangées par le téléphone portable. Ils peuvent également utiliser la localisation GPS pour suivre la position du smartphone. (21)

III.4.2. Menaces de suivi d'UE (Threats of UE tracking) :

Pour ce type de menaces on peut imaginer le suivi d'un utilisateur en se basant sur l'adresse IP liée à l'identité de l'utilisateur (IMSI ou TMSI), ou bien le suivi d'un utilisateur en se basant sur les messages de signalisation du transfert intercellulaire (handover).

III.4.3. Menaces pour l'eNB :

L'intrusion physique dans l'eNB ou son détournement peut permettre l'injection ou la modification de paquets. Cela donne à l'attaquant la capacité d'injecter des données vers le réseau en amont et vers l'unité de qualité d'accès en aval, ce qui peut dégrader le service. De plus, les attaques physiques sur l'eNB peuvent entraîner l'extraction de données clés et non chiffrées, et lorsqu'elles sont combinées à des attaques par déni de service (DoS), elles peuvent compromettre l'intégrité du système.

III.4.4. Menaces pour la passerelle MME / SAE :

De telles attaques peuvent inclure des attaques par déni de service (DoS) contre le MME, en utilisant des messages de signalisation provenant du RAN. Cela peut impliquer diverses procédures système, comme l'authentification lors de l'accès initial.

III.4.5. Les attaques dans les réseaux 4G/LTE :

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.

III.4.5.1. Les scénarios d'attaques :

Les attaques peuvent être classés en deux grandes catégories: les attaques actives et les attaques passives.

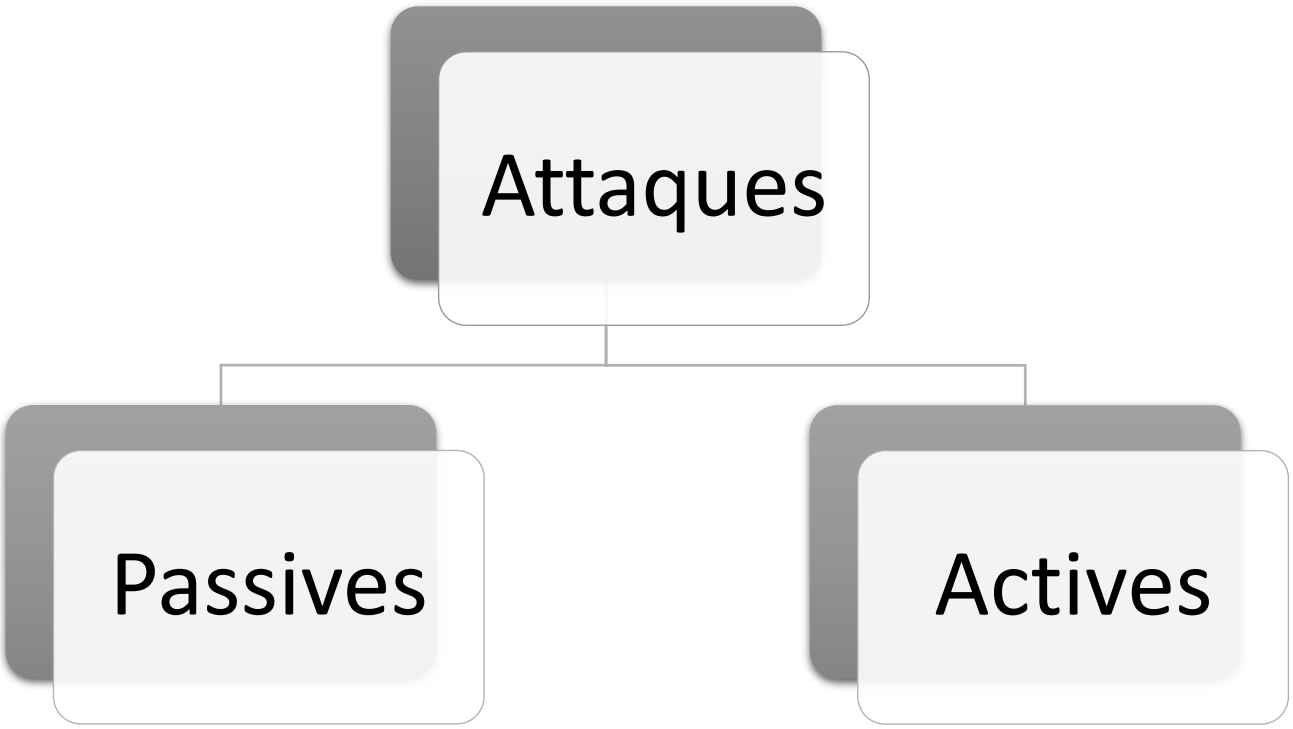


Figure 12 Classifications des attaques dans les réseaux

III.4.5.1.1. Attaque Passive :

Visent à intercepter des informations ou des données sans altérer leur contenu. Cela peut inclure des activités telles que l'écoute de conversations sur un réseau, la surveillance des connexions réseau, la collecte d'informations d'identification ou la recherche de vulnérabilités dans les systèmes cibles.

Elles sont souvent difficiles à détecter, car elles ne perturbent pas les opérations normales du système cible.

III.4.5.1.2. Attaque Active :

Quant à elles, impliquent une altération ou une perturbation du contenu ou du fonctionnement normal du système cible. Cela peut inclure des activités telles que l'injection de code malveillant, la modification de données, la suppression de données, le déni de service ou la prise de contrôle de systèmes.

Les attaques actives sont généralement plus faciles à détecter que les attaques passives, car elles ont un impact direct sur le système cible.

Type des attaques actives :

Les attaques actives peuvent être classées en attaque Interne ou attaque externe.

- **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. 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:**

Les attaques provenant de plusieurs nœuds dispersés à divers emplacements du réseau sont généralement plus sophistiquées et risquées. De plus, la participation de nombreux nœuds intermédiaires complique leur détection et rend l'identification de leur source exacte plus difficile.

III.4.5.2. Description de quelques attaques :

La prolifération des vulnérabilités et des outils d'attaque a considérablement accru le risque pour les réseaux. Les attaques ciblent généralement trois éléments principaux d'un système : la couche réseau, le système d'exploitation et la couche applicative.

De plus, beaucoup d'attaques peuvent infecter le réseau, On cite quelques-unes :

III.4.5.2.1. 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 réseau 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. (22)

Quelques vulnérabilités connues pour les attaques (DoS) :

a. Attaque par débordement de tampon (Buffer overflow attack) :

Il s'agit du type de vulnérabilité le plus courant. L'attaque Buffer Overflow dépend de l'envoi d'un grand nombre de visites sur le site, et le nombre de visites est supérieur au nombre spécifié par les développeurs du site, de sorte que le site ne peut pas accueillir le volume de visites, ce qui permet à l'attaquant de contrôler le ciblez-le ou même désactivez-le.

b. Inondation SYN (SYN Flood):

Une attaque par inondation SYN envoie une demande de connexion à un serveur Web mais n'authentifie jamais complètement la connexion, puis cible tous les ports ouverts restants sur le serveur Web jusqu'à ce qu'elle force le serveur à planter.

III.4.5.2.2. 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

Plus inquiétant encore, un tel logiciel a la capacité de créer délibérément une faille dans la sécurité interne de votre réseau, permettant ainsi à des individus externes de contourner les protections et d'accéder à des zones sensibles du réseau.

Pour contrer ce type d'intrusion, il est recommandé d'installer un pare-feu, un programme qui filtre les communications entrantes et sortantes de votre système, afin de restreindre au maximum l'accès à votre machine. De plus, maintenir un antivirus régulièrement mis à jour est crucial. Un utilitaire spécifique pour éliminer les chevaux de Troie peut également être d'une grande aide dans cette démarche de protection.

III.4.5.2.3. L'attaque IP spoofing :

L'IP spoofing représente une technique de piratage où les paquets de données TCP/IP ou UDP/IP sont envoyés avec une adresse expéditeur falsifiée. De cette manière, l'attaquant peut accéder et utiliser l'adresse d'un système légitime et de confiance. Cela lui permet d'injecter ses propres paquets de données dans un autre système, contournant ainsi les mesures de filtrage qui auraient normalement bloqué ces données. Dans la plupart des cas, cette usurpation d'adresse IP est exploitée pour mener des attaques de type DoS (Déni de Service) et DDoS (Déni de Service Distribué).

Dans certaines situations, un attaquant disposant d'une adresse IP usurpée ou falsifiée peut même intercepter le trafic entre deux ou plusieurs systèmes informatiques.

III.5. Mécanismes de sécurité dans 4G/LTE :

Sur les couches AS et NAS, différentes mesures de sécurité sont déployées afin de se prémunir contre les attaques malveillantes. Pour illustrer, la couche AS est chargée de garantir la sécurité des données utilisateur ainsi que des données de gestion radio, tandis que la couche NAS supervise la sécurité des messages relatifs à la gestion de la mobilité.

III.5.1. La sécurité de l'eNB :

La sécurité de l'eNB revêt une importance cruciale du fait qu'il constitue un point d'achèvement pour les principales mécanismes de sécurité de l'EPS. Souvent installé dans des endroits exposés en dehors du périmètre de sécurité de l'opérateur, tels que les toits d'immeubles ou les lieux publics extérieurs, l'eNB peut être difficile à contrôler en termes

d'accès. De même, les liaisons physiques reliant l'eNB à l'EPC, comme la fibre optique enfouie ou les liaisons hertziennes, peuvent être vulnérables.

Pour répondre à ces défis, la norme 3GPP a établi des exigences de sécurité strictes pour l'eNB et ses interfaces, ce qui représente une première pour un nœud de réseau de téléphonie mobile. Ces exigences couvrent à la fois les aspects logiciels de sécurité tels que le démarrage, la configuration, la gestion des clés et le traitement des données, ainsi que les interfaces de l'eNB.

En garantissant le respect de ces exigences, l'eNB peut bénéficier d'une sécurité optimale.

III.5.2. La Sécurité dans EPS :

Le niveau élevé de sécurité offert par EPS est assuré par l'introduction de nouveaux mécanismes, en particulier dans le domaine de l'accès au réseau. Parmi ces mécanismes, on cite :

L'authentification du réseau de service introduit dans la procédure EPS-AKA, une nouvelle hiérarchie des clés ; et l'introduction de deux niveaux de sécurité. (23)

Authentification mutuelle entre le MME et l'utilisateur :

Le but de cette procédure est de réaliser une authentification mutuelle entre l'utilisateur (UE) et le réseau LTE.

Les paramètres présents dans le vecteur d'authentification (quadruplé) sont : (19)

- **RAND :** le challenge (non aléatoire généré par le HSS) qui sert en tant qu'un des paramètres d'entrée pour générer les autres paramètres de l'AV.
- **XRES :** Le résultat attendu, utilisé par le réseau pour l'authentification de l 'USIM de l'UE.
- **AUTN :** Le jeton d'authentification utilisé par l 'USIM pour l'authentification réseau.
- **KASME :** (Access Security Management Entity) est une clé maîtresse de session de 256 bits ou appelé aussi, clé de base MME, c'est une clé dérivée des clés de chiffrement et d'intégrité.

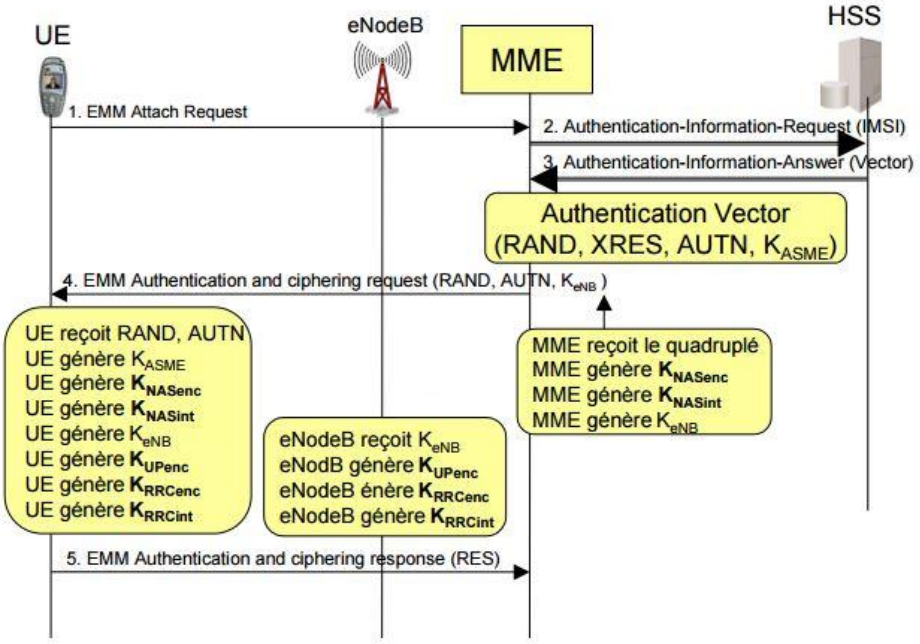


Figure 13 Sécurité EPS (19)

- **KNASenc** est une clé de chiffrement de 128 bits.Il est utilisé pour la protection du trafic NAS avec un algorithme de chiffrement particulier.
- **KNASint** est une clé utilisée pour la protection du trafic NAS (Non Access Stratum) avec un algorithme d'intégrité particulier. Cette touche est dérivée de KASME par l'équipement utilisateur et le MME.
- **KeNB** est une clé dérivée de KASME par l'UE et le MME ou par l'UE et l'eNB.
- **KUPenc** est une clé de chiffrement de 128 bits. Il est utilisé pour la protection du trafic usager avec un algorithme de chiffrement particulier.
- **KRRCenc** est une clé de chiffrement de 128.Il est utilisé pour la protection du trafic de signalisation RRC avec un algorithme de chiffrement particulier.
- **KRRCint** est une clé utilisée pour la protection du trafic RRC (Radio Ressource Control) avec un algorithme d'intégrité particulier, cette clé est dérivée par l'équipement utilisateur et l'eNodeB à partir de KeNB.

L'authentification EPS est réalisée lorsque :

- Le mobile se connecte au réseau.
- Le mobile établit un canal par défaut.
- Le mobile établit un canal dédié.
- Le mobile met à jour sa localisation (Tracking Area)

L'authentification est réalisée entre le mobile et MME:

Le chiffrement a lieu à deux niveaux:

- entre le mobile et l'eNodeB (trafic usager et trafic de signalisation)
- entre le mobile et le MME (trafic de signalisation)

III.5.3. La Sécurité dans l'IMS :

IMS (IP Multimedia Subsystem) est élaboré par le 3GPP et propose une structure qui favorise la convergence des données, de la voix et de la technologie. Fondé sur le standard de connectivité IP, il constitue une architecture pour la gestion des services. (23)

Les usagers (UE) désirant établir une session doivent entrer en communication avec le noyau du réseau IMS en utilisant des messages du protocole SIP (Session Initiation Protocol). Une fois les paramètres de la session et le protocole de transport RTP (Real-time Transport Protocol) négociés, la session multimédia est mise en place. Un exemple courant de cette session est la Voix sur IP (VoIP). Les principaux éléments architecturaux de l'IMS sont les serveurs mandataires SIP, également connus sous le nom de CSCF (Call Session Control Functions), qui assurent le contrôle des appels de service. Toute la signalisation de session SIP peut être gérée par les CSCF, qui se divisent en trois entités : P-CSCF, I-CSCF et S-CSCF. Lorsqu'un usager de messagerie instantanée souhaite communiquer avec l'IMS, la S-CSCF joue le rôle de HSS pour authentifier l'usager et assure le contrôle de session du service multimédia pour celui-ci. Les services

multimédias ne seront accessibles qu'une fois que l'UE aura établi une association sécurisée avec le réseau.

III.5.4. La Sécurité NAS :

NAS est l'abréviation de (Non Access Stratum) :

Le but principal de la sécurité NAS est de transmettre les messages de signalisation entre le MME et l'équipement usager en toute sécurité, donc chiffrés, au niveau du plan de commande. Les clés de sécurité NAS sont générées à partir de la 10 clé KASME. Après avoir établi la sécurité NAS, le MME et le UE partagent une clé de chiffrement (KNASenc) et une clé d'intégrité (KNASint) utilisées pour le chiffrement et la protection de l'intégrité de la signalisation entre l'UE et le MME. (23)

III.5.5. La Sécurité AS :

AS est l'abréviation de « Access Stratum ». Les clés de sécurité AS sont utilisées pour transmettre en toute sécurité des paquets IP et des messages Radio Resource Control (RRC) entre le point d'accès (ENodeB) et le UE. Elles sont générées à partir de la clé KeNB. Après avoir établi la sécurité AS, l'eNodeB et l'équipement usager partagent une clé d'intégrité RRC (KRRCint), une clé de cryptage RRC (KRRCenc) et la clé de cryptage du plan d'usager (KUP enc). Ces clés servent au chiffrement et à la protection de l'intégrité. (24)

III.5.6. Développement des procédures adaptées :

III.5.6.1. La cryptographie :

Le terme cryptographie englobe l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire de les rendre incompréhensibles sans une action spécifique. Bien que le verbe "crypter" soit parfois utilisé, le terme "chiffrer" est préféré. La cryptologie repose principalement sur l'arithmétique. Pour un texte, il s'agit de transformer les lettres du message en une série de chiffres (représentés sous forme de bits en informatique, car les ordinateurs fonctionnent en binaire), puis d'effectuer 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.

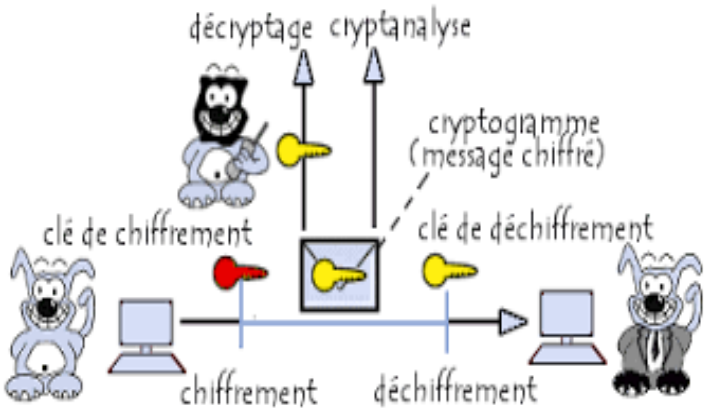


Figure 14 Architecture de la cryptographie *(25)*

Le chiffrement se fait généralement à l'aide d'une clé de chiffrement, tandis que le déchiffrement nécessite une clé de déchiffrement. Il existe deux types de clés :

- ✓ Les clés symétriques : Utilisées à la fois pour le chiffrement et le déchiffrement. Ce procédé est appelé chiffrement symétrique ou chiffrement à clé secrète.
- ✓ Les clés asymétriques : Employées dans le cas du chiffrement asymétrique (également appelé chiffrement à clé publique). Dans ce cas, une clé différente est utilisée pour le chiffrement et pour le déchiffrement. (25)

III.5.6.2. Un pare-feu :

Un pare-feu est un appareil de sécurité des réseaux qui contrôle le trafic réseau entrant et sortant et décide s'il bloque ou autorise le trafic selon un ensemble défini de règles de sécurité. Ils établissent une barrière entre les réseaux internes sécurisés et contrôlés auxquels il est possible de se fier et les réseaux externes qui n'ont pas de contenu de confiance, comme Internet.

Un pare-feu peut être matériel, logiciel, en nuage public ou en nuage privé (virtuel). (26)

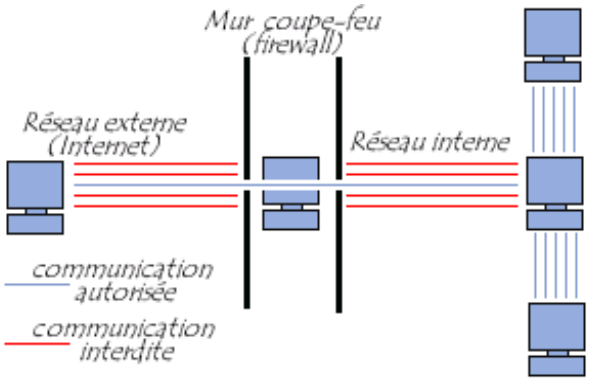


Figure 15 Architecture pare-feu (Firewall) (27)

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).

III.5.6.3. Réseau privé virtuel (VPN) :

Un réseau privé virtuel, ou VPN, est une connexion Internet chiffrée liant un appareil à un réseau. La connexion chiffrée permet de s'assurer que les données sensibles sont transmises en toute sécurité. Il empêche les personnes non autorisées d'espionner le trafic et permet à l'utilisateur d'effectuer du travail à distance. La technologie VPN est très utilisée dans les environnements professionnels. (26)

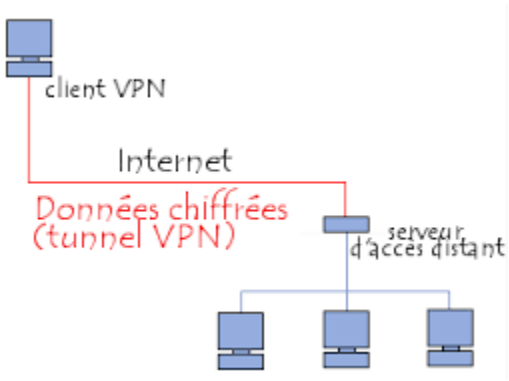


Figure 16 Architecture d'un VPN

Fonctionnement d'un système VPN :

Un VPN permet d'étendre un réseau d'entreprise via des connexions chiffrées établies sur Internet. Le trafic entre l'appareil et le réseau étant chiffré, il reste privé. Un employé peut donc travailler hors du bureau et se connecter en toute sécurité au réseau d'entreprise. Même les téléphones intelligents et les tablettes peuvent se connecter via un VPN. (26)

III.7. Conclusion :

Dans ce chapitre, nous avons examiné les mécanismes de sécurité des réseaux de quatrième génération. Cela inclut la migration progressive des protocoles de la troisième génération et l'authentification mutuelle, ainsi que l'utilisation d'algorithmes de chiffrement robustes qui améliorent significativement la sécurité des échanges. Actuellement, le piratage reste très présent tandis que la sécurité est insuffisante. Notre principal intérêt étant les réseaux 4G (LTE), nous consacrerons le prochain chapitre à présenter notre proposition d'amélioration de la sécurité de la 4G/LTE.

Chapitre IV

Simulations et amélioration de la sécurité pour signaux mobile 4G/LTE

IV.1. Introduction :

Comme nous avons vu dans le chapitre précédent diverses solutions ont été proposées pour la sécurisation du réseau 4G/LTE contre les attaques. L'objectif principal de ce chapitre est de présenté notre solution pour la sécurisation des données transmises de réseau 4G/LTE. en destination des réseaux extérieures.

Nous commençons d'abord par une suggestion de la topologie utilisée, ensuite nous discutrons de l'environnement du simulateur utilisé pour l'implémentation de la solution de sécurité proposée qui consiste à créer un réseau privé virtuel basé sur le protocole IPSec.

Enfin, nous analyserons la performance de notre topologie avec les différentes simulations.

IV.2. Méthode développée pour l'amélioration de la sécurité LTE :

An de répondre aux objectifs de sécurités , nous proposons une nouvelle structure du réseau (cf. Figure 17), qui consiste à créer un réseau privé virtuel basé sur le protocole IP Security entre deux PGWs sur deux sites différents. L'avantage de cette solution est qu'elle est totalement transparente pour les utilisateurs, puisqu'elle donne l'impression d'avoir un réseau en continu.

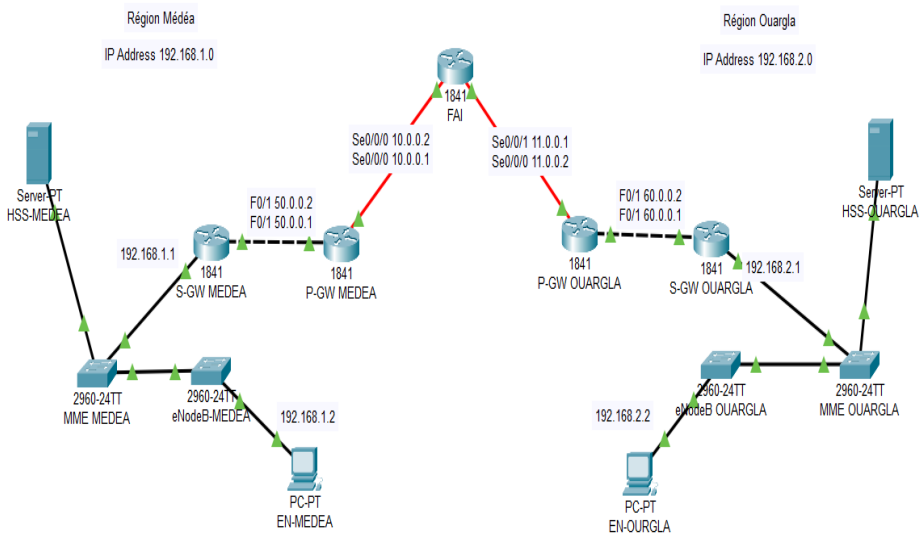


Figure 17 Architecture proposée pour un réseau 4G/LTE

IV.2.1. Réalisation du réseau :

An de réaliser notre solution de sécurité, on doit d'abord réaliser une architecture du réseau LTE Pour cela, on doit faire les étapes suivantes :

1. Création de la topologie.
2. Etude de l'adressage IP et de la configurée sur chaque équipement.
3. Configurations des routeurs et switches.
4. Configurations des paramètres de base de la sécurité (les mots de passes et les modes d'accès) sur les équipements.

1. La topologie utilisée :

L'architecture du réseau LTE présentée sur la figure 18, est inspirée de l'architecture réel du réseau LTE.

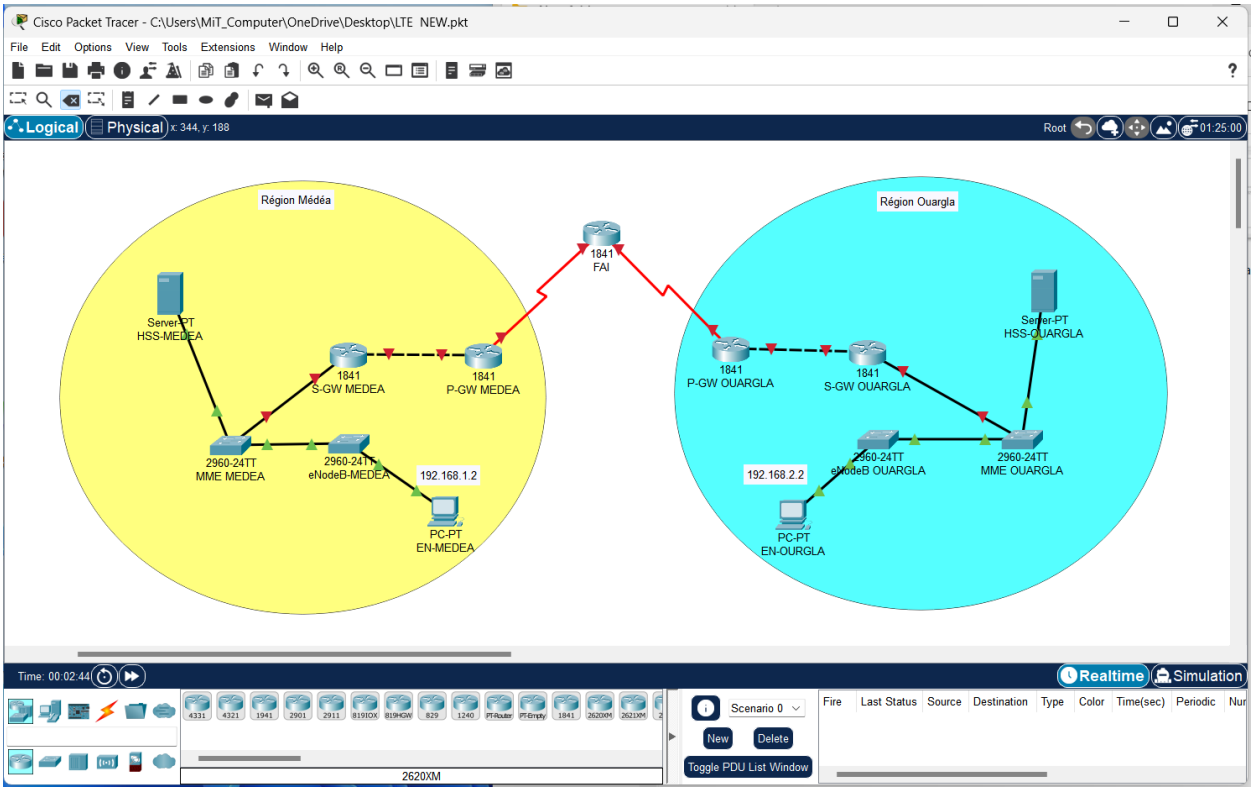


Figure 18 L'architecture du réseau 4G/LTE sous Packet Tracer

Table d'adressage IP:

Tableau 4 Table d'adressage IP

Périphériques	Interface	Adresse	IP Masque	Passerelle
FAI	Se0/0/0 Se0/0/1	10.0.0.2 11.0.0.1	255.0.0.0 255.0.0.0	
PGW-MEDEA	Se0/0/0 F0/1	10.0.0.1 50.0.0.2	255.0.0.0 255.0.0.0	
SGW-MEDEA	F0/1 F0/0	50.0.0.1 192.168.1.1	255.0.0.0 255.255.255.0	
PGW-OURAGLA	Se0/0/0 F0/1	11.0.0.2 60.0.0.2	255.0.0.0 255.0.0.0	
PGW-OURAGLA	F0/1 F0/0	60.0.0.1 192.168.2.1	255.0.0.0 255.255.255.0	
HSS-MEDEA		192.168.1.3		192.168.1.1
HSS-OURAGLA		192.168.2.3		192.168.2.1
EN-MEDEA		192.168.1.2	255.255.255.0	192.168.1.1
EN-OUARGLA		192.168.2.2	255.255.255.0	192.168.2.1

2. Configuration de base du réseau :

An que notre réseau fonctionne comme un cas réel et permet le transfert des données à des distances lointaines, il faut procéder à des configurations et la mise en service des équipements utilisés (routeurs, commutateurs, les serveurs, les ordinateurs et configurations des routes d'échange de paquets).

1) Configuration des routeurs :

- **Configuration de base des routeurs :**

Je dois suivre les étapes décrites dans la figure 19 pour le processus de configuration.

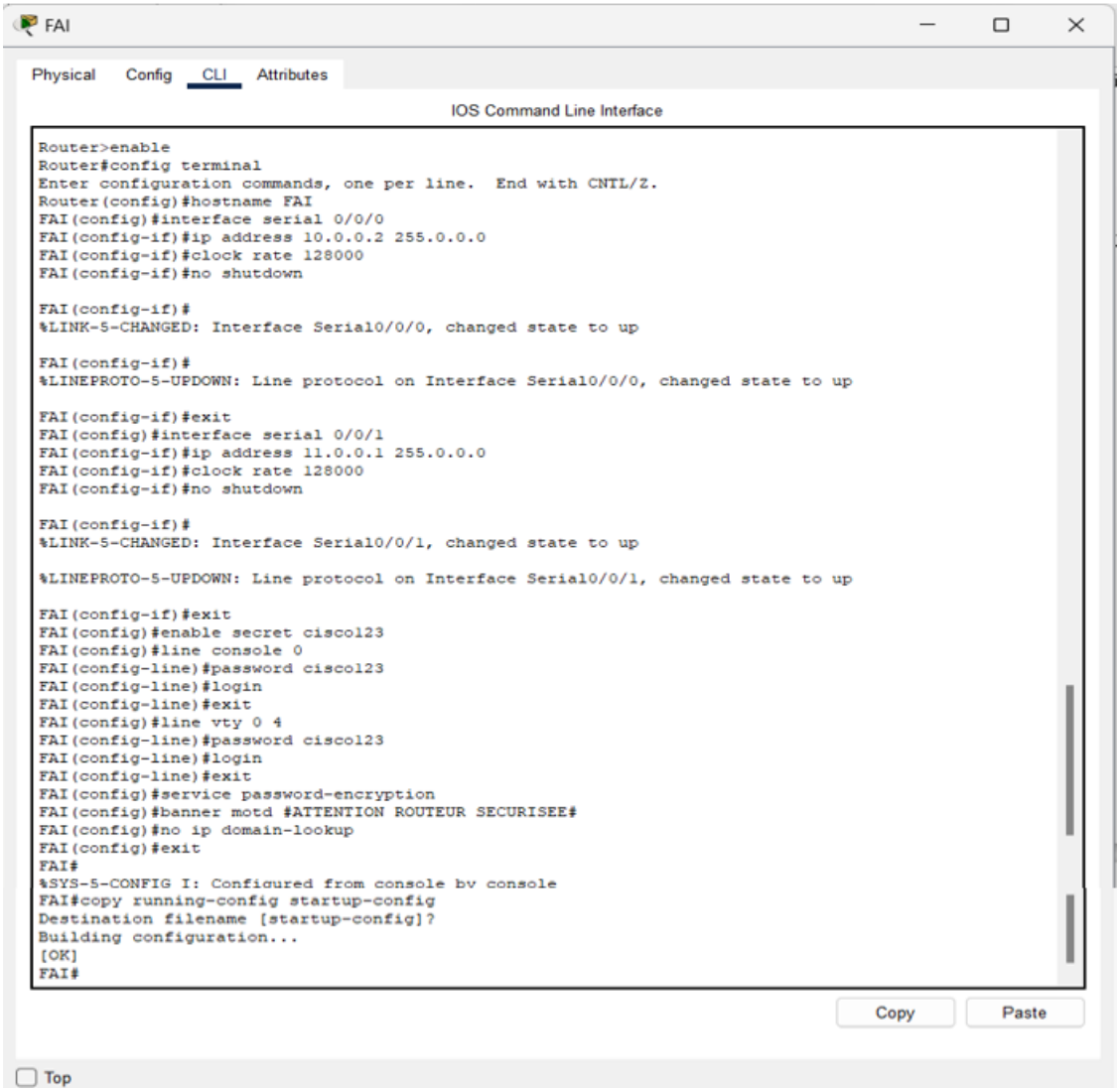


Figure 19 Configuration des routes sur FAI

Explication les étapes :

- **Etape 01 :** Mode privilégié et Mode de configuration terminal.
- **Etape 02 :** Nom du routeur : Il permet de donner un nom à un routeur.
- **Etape 03 :** Adressage IPv4 d'une interface : Configuration des interfaces du routeur (serial/ fast Ethernet) : Cette configuration permet d'attribuer à chaque interface de l'équipement des adresses IP.
- **Etape 04 :** Configuration du mot de passe enable : Les mots de passe enable secret sont utilisés pour empêcher l'accès au mode privilégié. Il est crypté en utilisant un puissant algorithme MD5.

- **Etape 05 :** Configuration du mot de passe de l'accès console : Les commandes suivantes permettent de définir un mot de passe facultatif mais recommandé sur la ligne console.
- **Etape 06 :** Configuration de mot de passe des lignes VTY : Pour qu'un utilisateur puisse accéder à un routeur à distance via telnet. Un mot de passe doit être défini sur une ou plusieurs lignes du terminal virtuel (vty).
- **Etape 07 :** Chiffrer les mots de passes :
- Il est parfois préférable que les mots de passe ne soient pas aches en texte clair dans les résultats des commandes show running-config ou show startup-config, La commande suivante permet de crypter les mots de passes.
- **Etape 08 :** Configurez une bannière MOTD : La bannière MOTD affiche tous les terminaux connectés à la connexion et permet de transmettre des messages destinés à tous les utilisateurs du réseau (pour les avertir, par exemple, d'un arrêt imminent du système), La bannière MOTD apparaît avant la configuration de la bannière de connexion.
- **Etape 09 :** Désactiver la recherche DNS : Désactivation de la résolution DNS empêche la conversion du nom d'hôte de type DNS en adresse. Cette commande est activée par défaut.
- **Etape 10 :** Enregistrer la configuration en cours dans le fichier de configuration initial : Après la configuration des équipements, on doit enregistrer les configurations effectuées.
-

Remarque : La configuration des quatre routeurs se fait de la même façon, sauf au niveau de la configuration des interfaces qui vont être configurés selon le tableau 5.

- ✓ **Configuration du routage dynamique sur les routeurs :**

Les protocoles de routage (Voir l'Annexe) déterminent le meilleur chemin, ou la meilleure route, vers chaque réseau (28). Cette route est alors ajoutée à la table de routage. L'un des principaux avantages des protocoles de routage dynamique est l'échange d'informations de routage entre les routeurs lors de la modification de la topologie.

Tableau 5 Les routes statiques des routeurs utilisées

Les Routeurs	Les Routes Statiques
FAI	10.0.0.0 11.0.0.0
PGW-MEDEA	10.0.0.0 50.0.0.0
SGW-MEDEA	50.0.0.0 192.168.1.0
PGW-OUARGLA	11.0.0.0 60.0.0.0
SGW-OUARGLA	60.0.0.0 192.168.2.0

Exemple d'une configuration du routage dynamique sur le routeur PGW-MEDEA (cf, Figure 20)

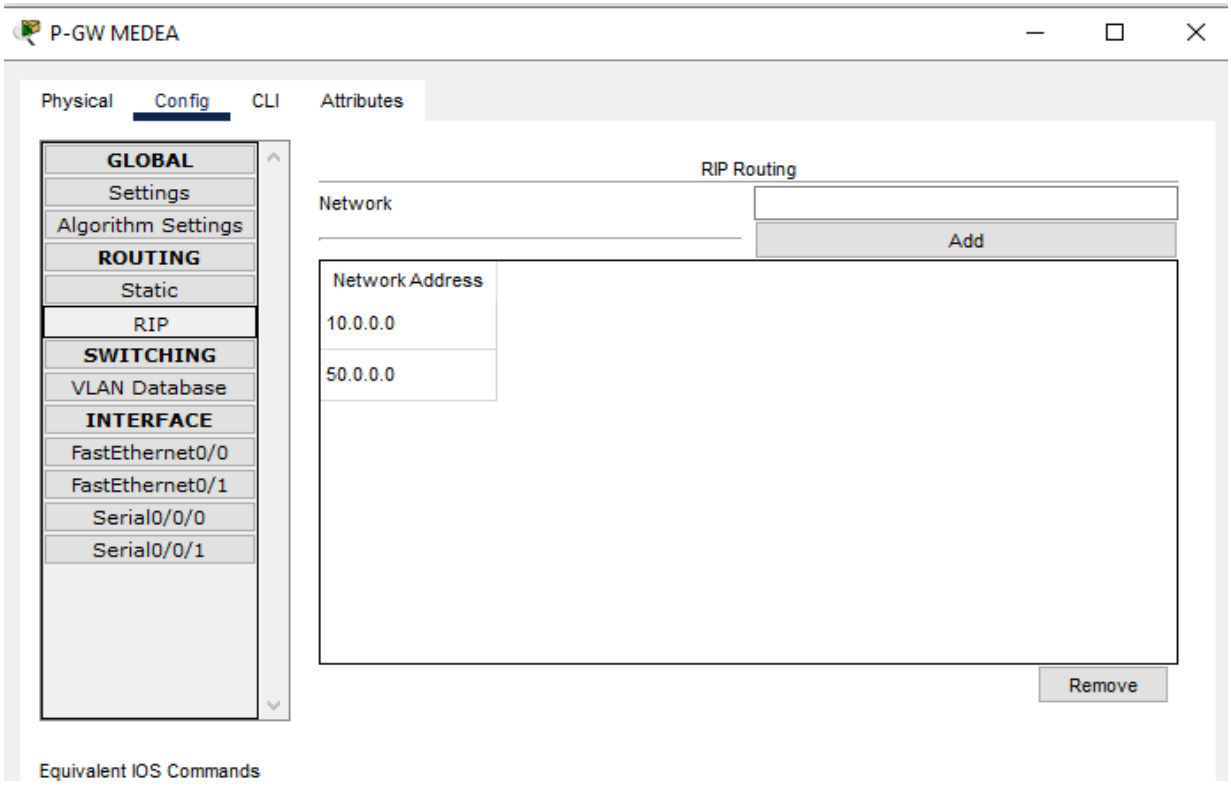


Figure 20 Configuration des routes sur PGW-MEDEA

2) Configuration des commutateurs :

Pour une configuration de base des commutateurs ; elle se fait de la même façon que les routeurs on procède à faire toutes les étapes citées précédemment (des hostnames et des mots de passe, ...) pour une configuration de base.

Nous prendrons comme exemple de configuration le commutateur « MME-MEDEA»

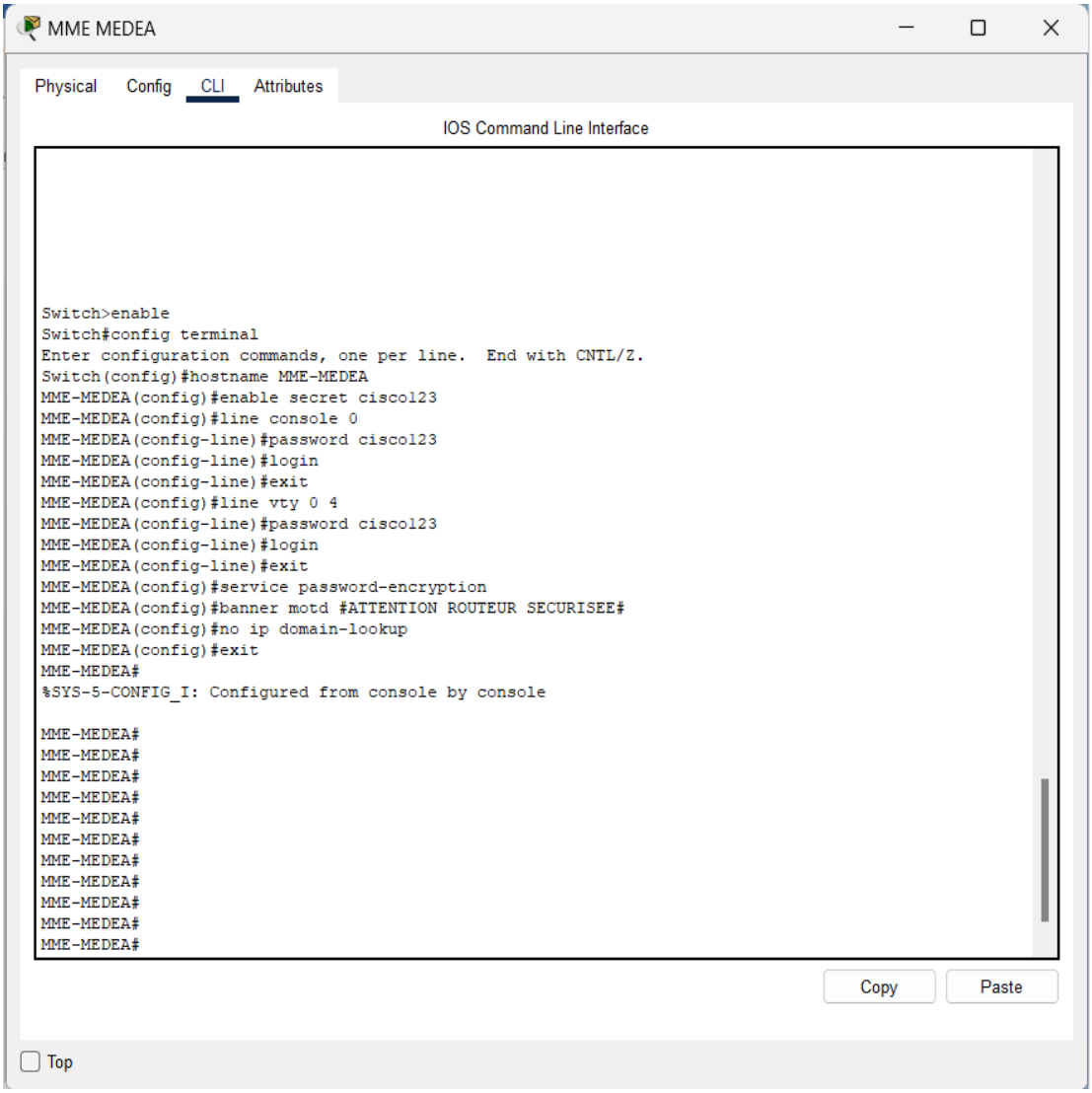


Figure 21 Configuration des switches sur MME-MEDEA

Remarque : La configuration des deux commutateurs se fait de la même façon.

3) Configuration de bases des ordinateurs et serveurs :

Dans cette configuration, on a attribué à chaque ordinateur une adresse IP, un masque sous réseau, et une adresse passerelle selon le tableau 4.

Exemple d'une configuration des adresses IP sur l'ordinateur de la direction à MÉDÉA (cf. Figure 22) : sachant que la même chose sera appliquée pour le PC « Direction OUARGLA »

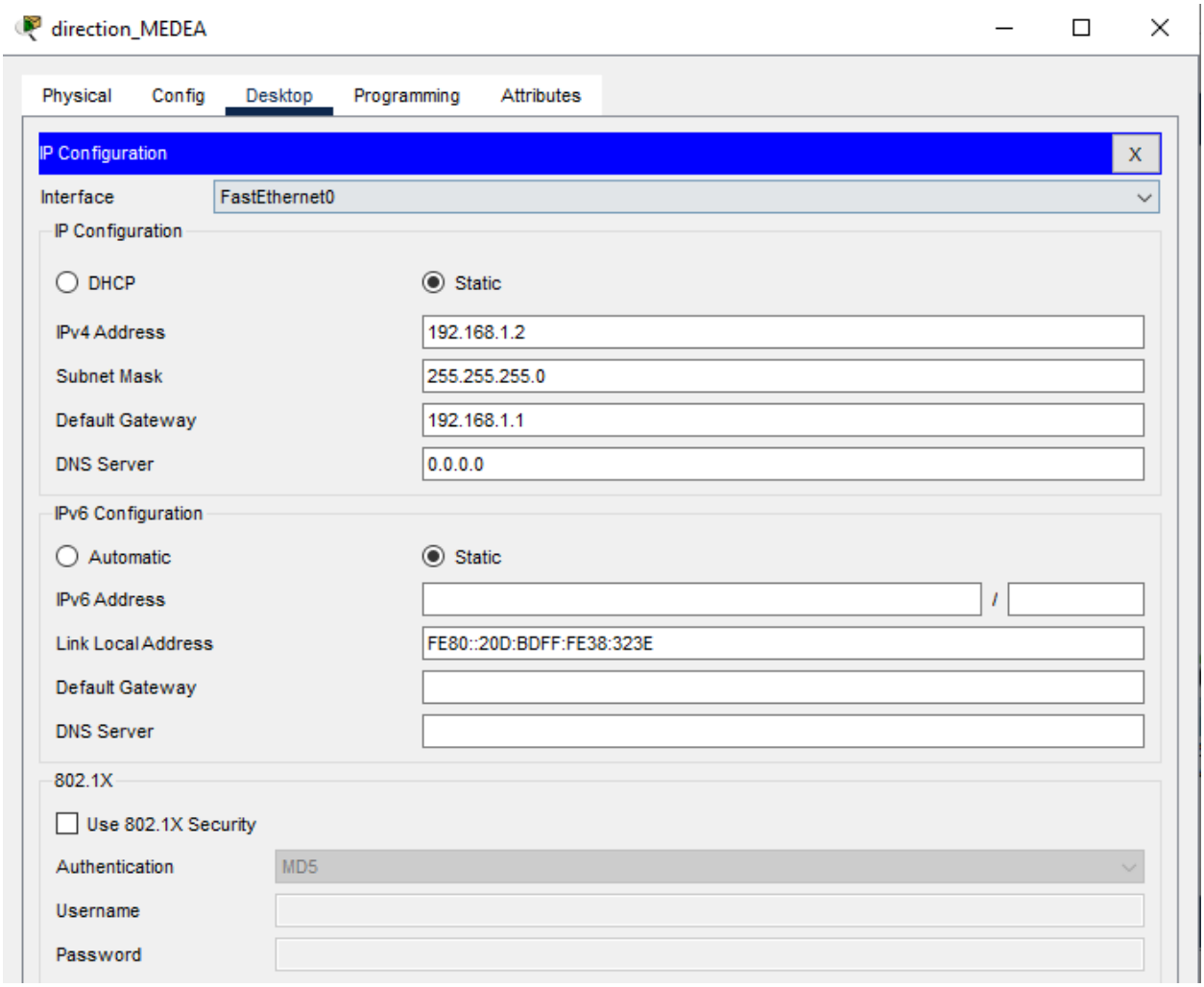


Figure 22 Configuration de l'adresse IP sur l'ordinateur de la direction-MEDEA

IV.3. Les résultats des configurations de bases :

Apres avoir configuré notre réseau, on vérifie la connectivité entre les différents équipements du réseau.

IV.3.1. Vérification en mode SIMULATION :

Dans cette partie, on visualise sur la figure 23 que les paquets sont échangés entre les équipements du réseau, ce qui signifie que les routes et les équipements ont été bien configurés. On remarque aussi que les protocoles de routage sont activés comme le cas du protocole RIPv1, ainsi que le cache ARP.

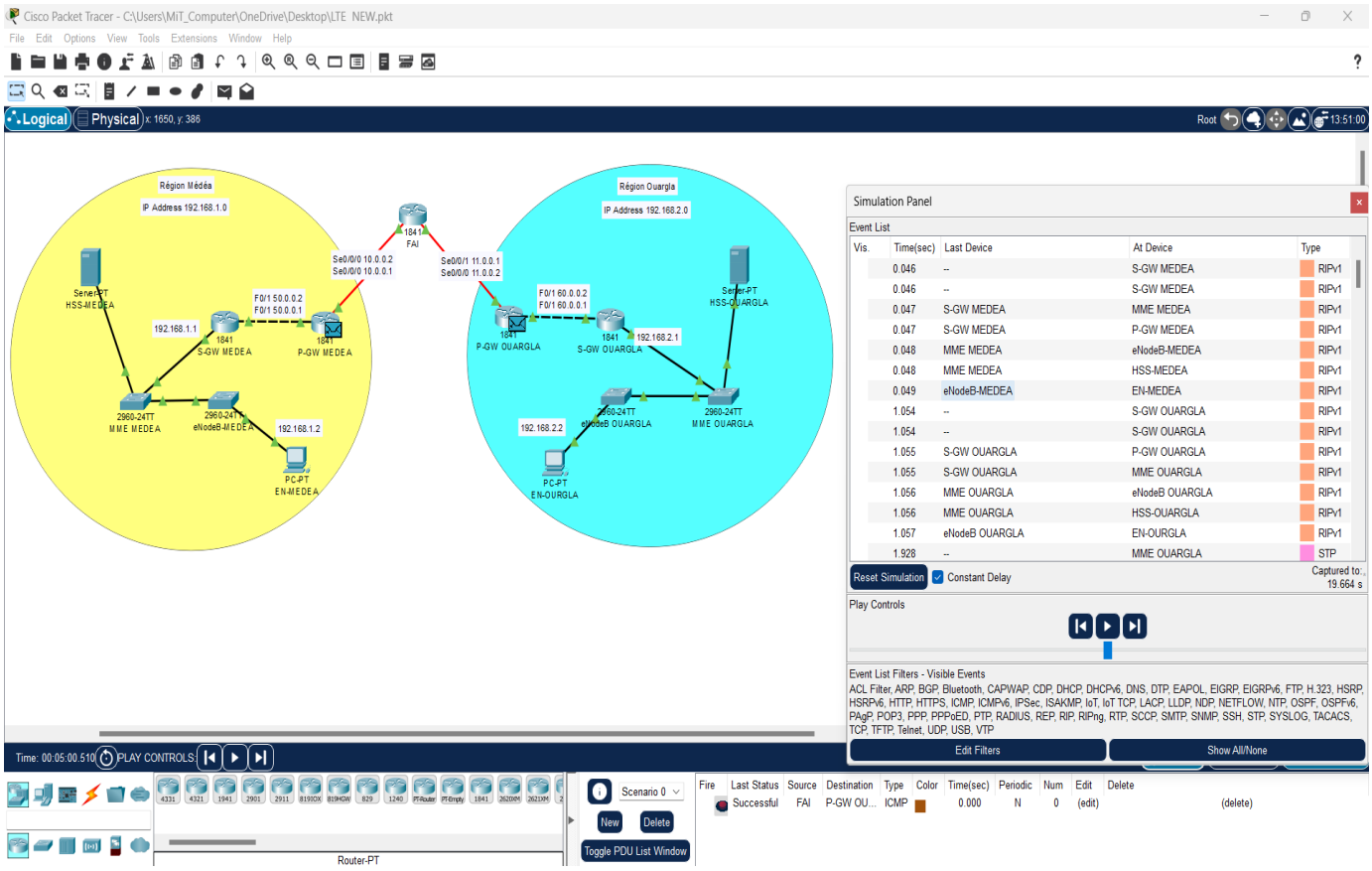


Figure 23 Le réseau 4G/LTE en mode simulation

IV.3.2 Vérification de la connectivité entre les 2 entreprises :

On constate que les deux entreprises communiquent entre elle, comme le montre La figure 24 montre que les deux entreprises communiquent entre elles, c'est-à-dire, lors de l'envoie des paquet d'une entreprise à une autre, le paquet arrive sans aucun problème, aucune perte d'information, et la durée du transfert ne dépasse pas la limite maximum qui est de 31ms.

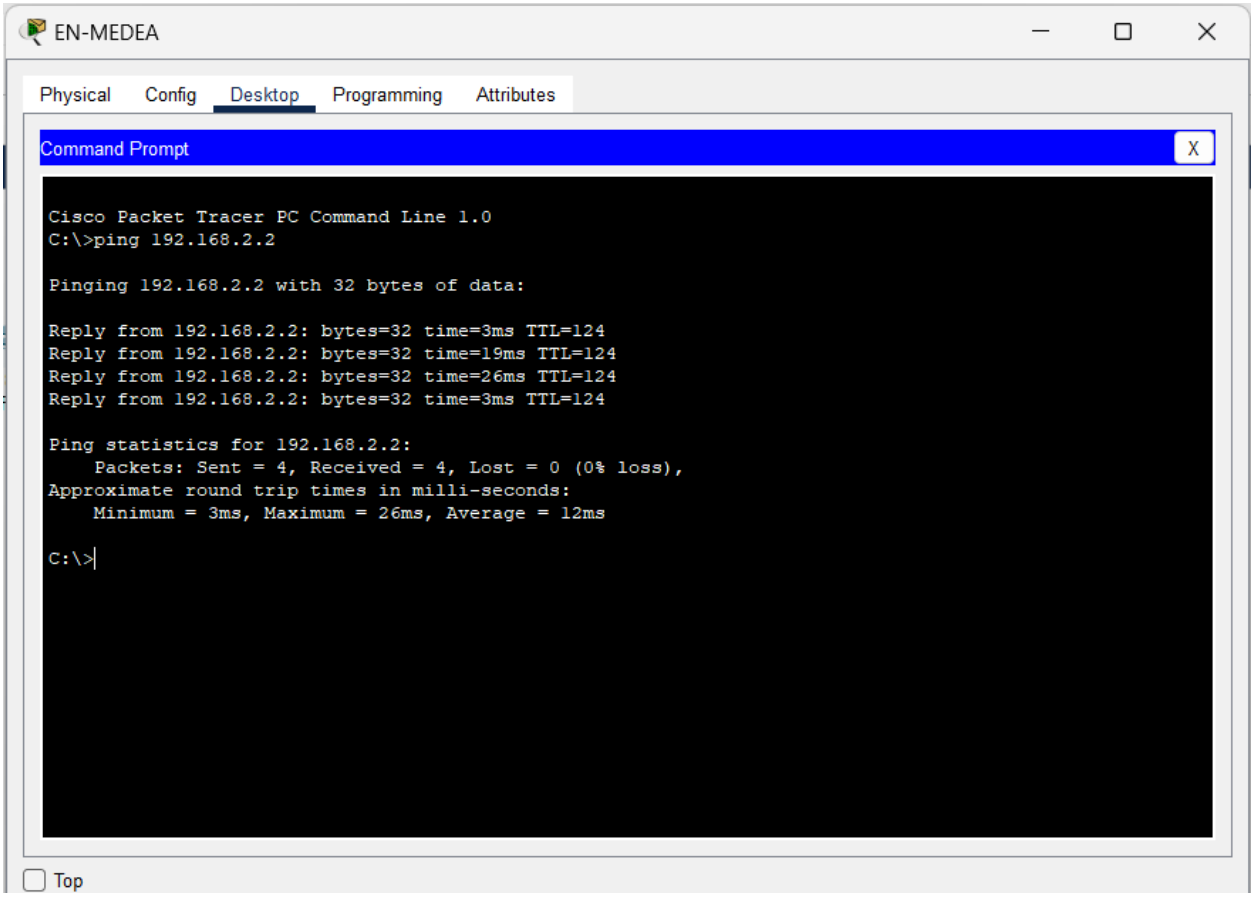


Figure 24 Connectivité réussie entre les entreprises

IV.4. La mise en œuvre de la solution de sécurité Configuration du VPN-IPSec :

Voici les différentes étapes afin de configurer la solution de sécurité basé sur la création d'un VPN sous le protocole IP Security sur les routeurs PGW-MEDEA et PGW-OUARGLA :

- ✓ Définir les règles de sécurité ISAKMP.
- ✓ Configurer les « transform set ».
- ✓ Configurer une ACL qui spécifiera quel trafic peut/doit emprunter le VPN.
- ✓ Configurer une « crypto-map ».
- ✓ Appliquer la « crypto-map » sur l'interface.
- ✓ Configurer une ACL sur l'interface « outside ».

1) Configuration des routeurs :

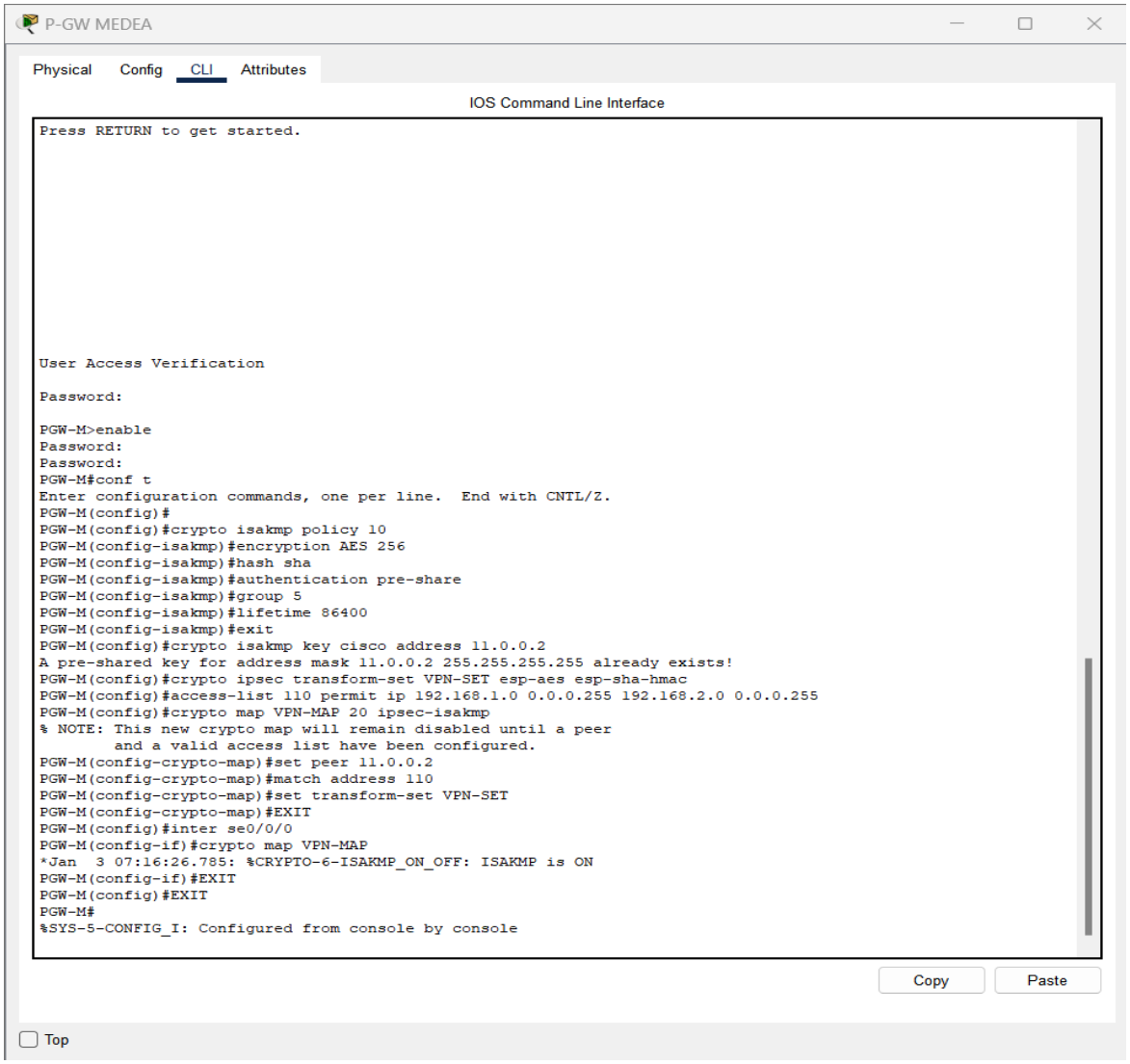


Figure 25 Configuration des routes sur PGW-MEDEA

Explication les étapes :

- **Etape 01 :** Nous devons d'abord activer le moteur isakmp.
- **Etape 02 :** Cette étape consiste à configurer les règles IKE sur les deux routeurs. Les règles IKE précisent le type d'encryptions et de découpage à utilisé ainsi le type d'authentification.
  - ❖ encryption AES 256: type d'endcryptage sur 256 bit.
  - ❖ authentication pre-share : Précise qu'aucun certificat d'autorité ne sera utilisé.
  - ❖ group 5 : Spécifie l'identifiant Di-e-Hallman.
  - ❖ Hash Md5 : Précise le type de découpage.

- ❖ lifetime 86400: c'est la durée de vie de l'échange de clé. Nous utiliserons 86400 secondes , une journée.

- **Etape 03 :** Configuration de la clé de partage : Sur un routeur, on configure la clé qui correspond au partenaire IPsec.
- **Etape 04 :** Une « transform-set » est une combinaison d'algorithmes et protocoles de sécurité « compatibles », Les routeurs essaieront de trouver la meilleure combinaison possible selon les configurations et capacités de chaque point de chute du VPN en se basant sur les « transform-set » disponibles.
- **Etape 05 :** Configuration des ACL : Elles permettent d'autoriser le trafic entre les sites distants.
- **Etape 06 :** Configuration du « crypto-map » : Le « crypto-map » permet d'associé l'access-list, le trafic et la destination.
- **Etape 07 :** que les fonctions précédentes puissent fonctionner. Il faut assigner la carte de cryptage sur l'interface WAN du routeur.
-

Remarque : Toutes ces configurations doivent être configurées sur l'autre routeur PGW-OUARGLA , mais avec une légère différence au niveau de l'adressages qui vont être comme suit :

- ✓ Crypto isakmp key cisco address 10.0.0.1.
- ✓ La configuration des ACL pour l'autorisation du trafic qui : de 192.168.2.0 0.0.0.255 vers 192.168.1.0 0.0.0.255.
- ✓ Set peer 10.0.0.1.

IV.5. Simulation et Résultats des configurations :

IV.5.1 En mode simulation :

On observe qu'à l'initialisation de la simulation (cf. Figure 26), le moteur ISKAMP s'active en premier, suivi par le protocole IPSec et l'application de ce protocole sur l'interface des deux routeurs. Cela indique qu'une négociation des fonctions de sécurité configurées a lieu.

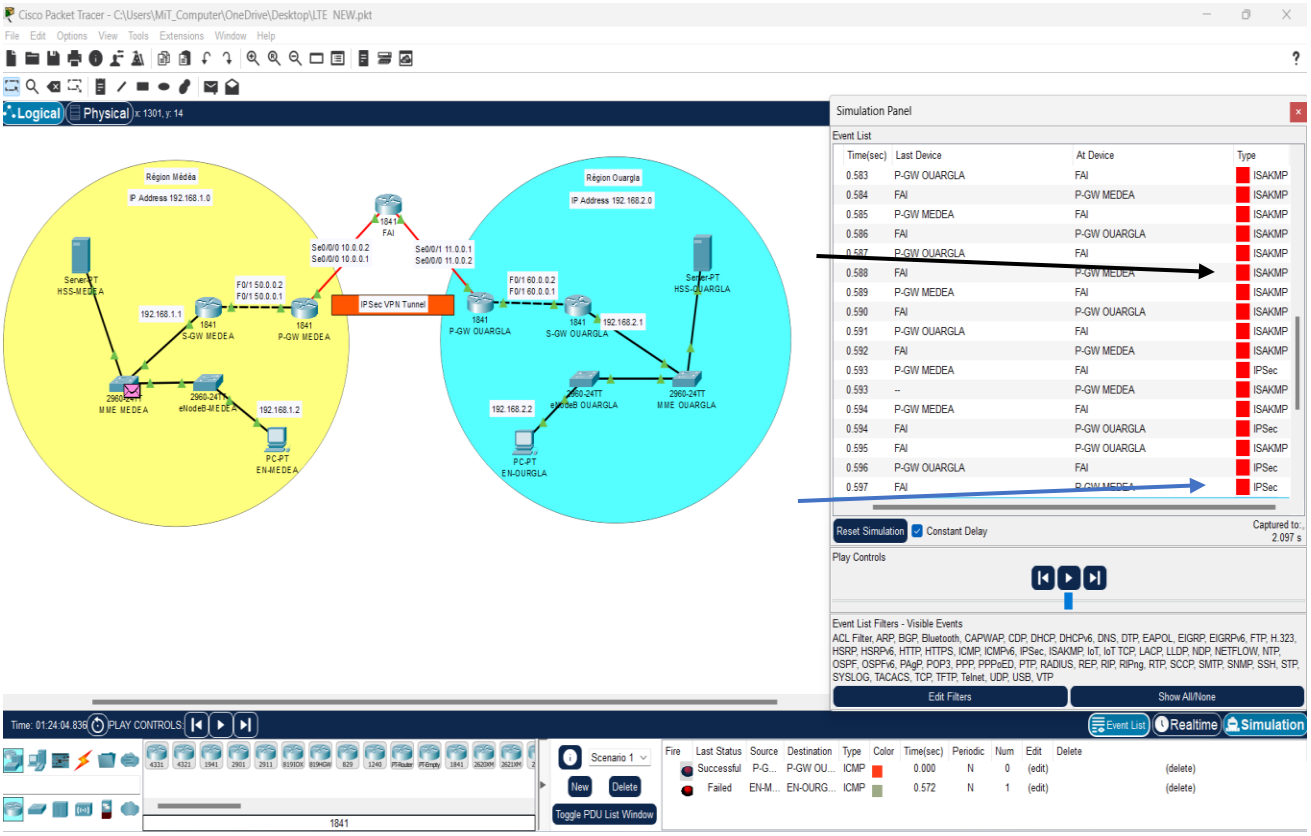


Figure 26 L'activation de ISKAMP et protocole IPSec

IV.5.2 Vérification du MAP du VPN :

On constate que les interfaces ont été bien configurées, ainsi les Access-List, La figure 4.17 montre que l'accès est permit pour le transfert des paquets de ce réseau (Médéa) vers l'autre réseau distant (Ouargla) , et vice vers. en spécifiant l'interface de réception (11.0.0.2 / 10.0.0.1). A ce ci s'ajout , qu'elle nous montre que l'ensemble de paires est activé, l'accès des listes est valide, le transfert entre les sites est permis en spécifiant l'interface d'échange.

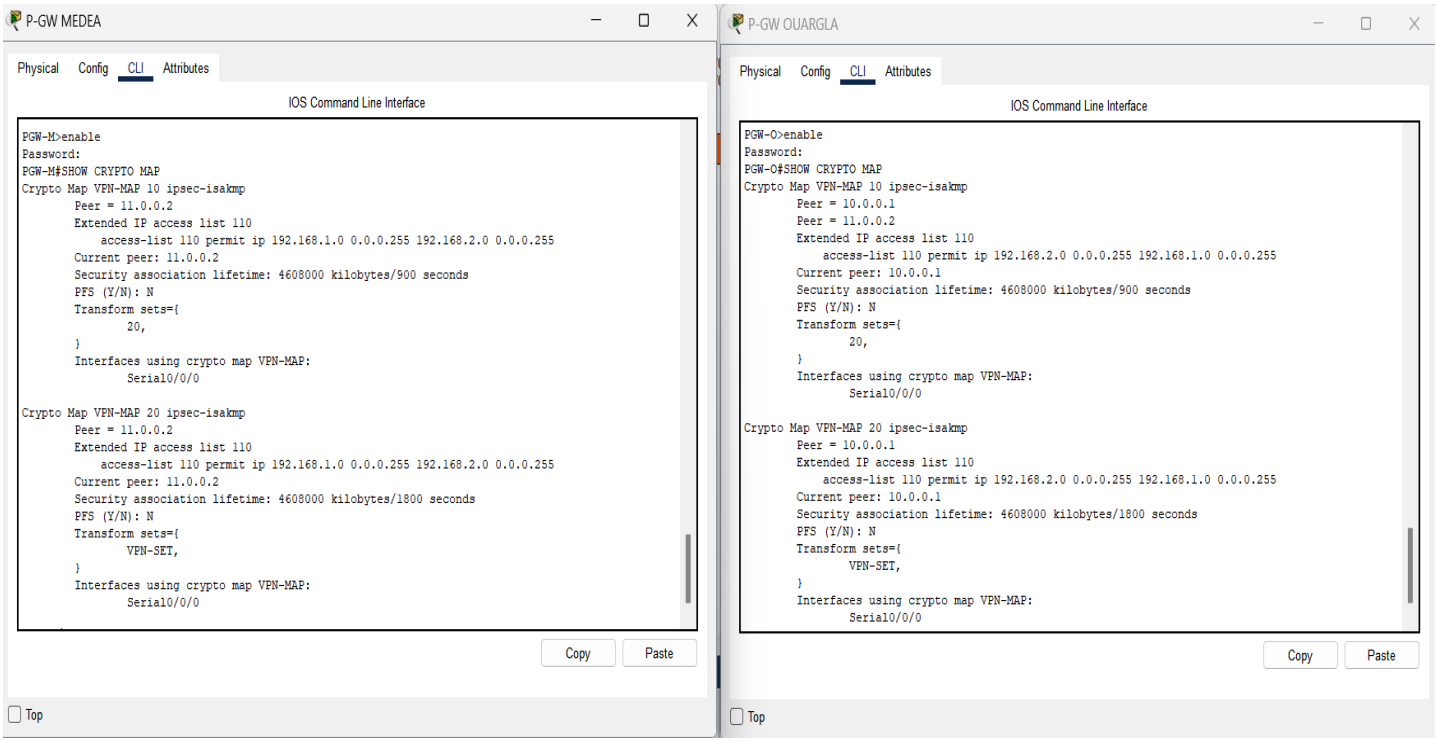


Figure 27 Le CRYPTO MAP sur le routeur PGW-MEDEA ET PGW-OUARGLA

IV.5.3 Réalisation d'un ping :

D'après ces résultats (cf. Figure 4.16), la communication reste intacte. Le paquet atteint l'entreprise distante avec un délai légèrement inférieur de 2 ms par rapport à une configuration sans VPN, sans aucune perte d'information.

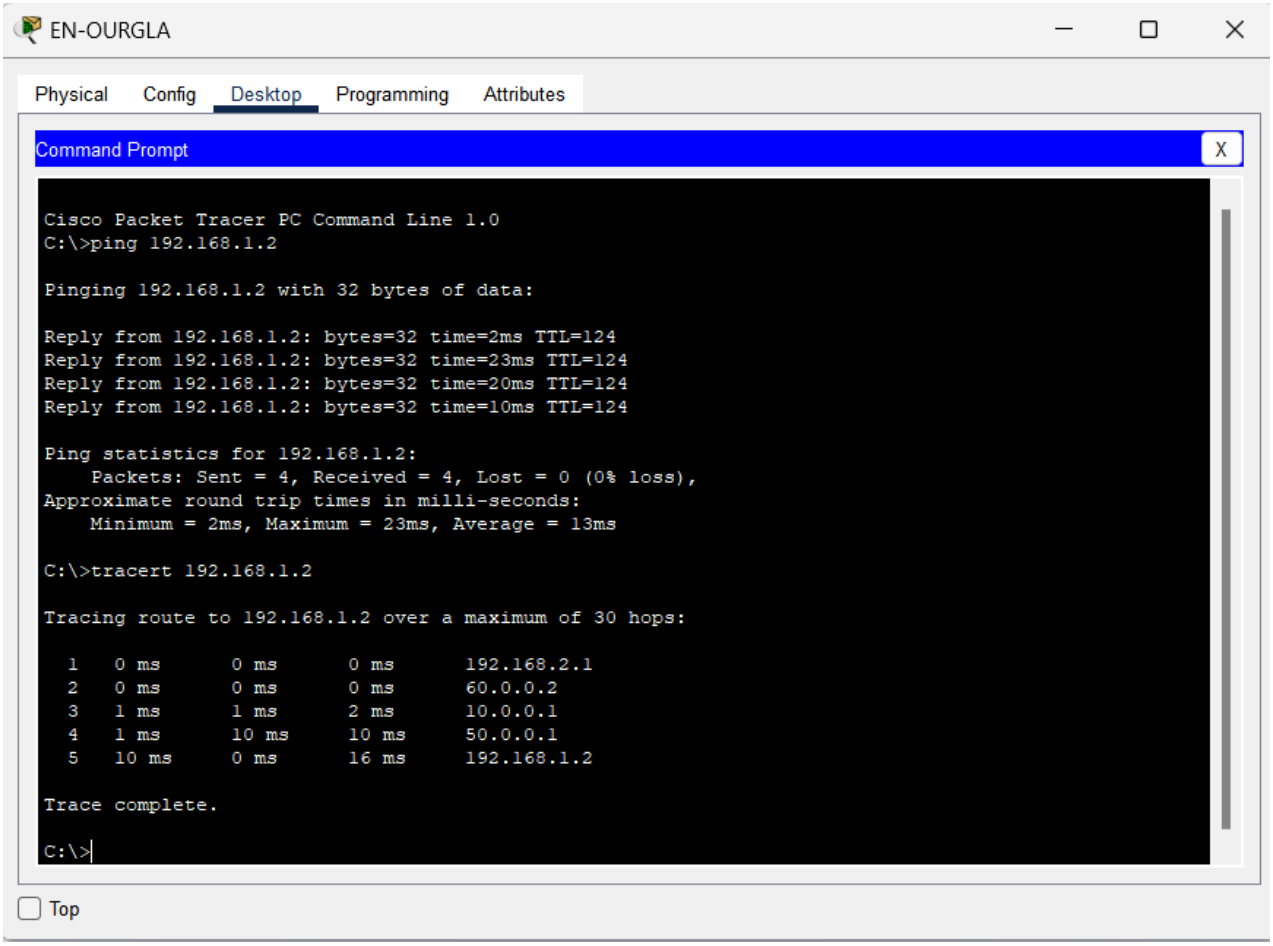


Figure 28 Réalisation du ping

IV.6. Conclusion :

Dans ce chapitre, nous avons présenté notre thématique et proposé une solution en définissant les exigences de sécurité à prendre en compte ainsi que les différents protocoles de sécurité à appliquer pour créer un réseau sécurisé.

L'IOS dans le simulateur a offert diverses commandes répondant à ces besoins, notamment les ACL (Access Control Lists) qui nous ont permis de filtrer des paquets selon des critères définis, ainsi que différentes commandes pour implémenter notre stratégie de sécurité basée sur la création d'un réseau privé virtuel utilisant le protocole IPSecurity.

Conclusion Générale

Dans ce projet de fin d'études, nous avons été motivées par l'opportunité d'étudier la sécurité des réseaux mobiles. Nous nous sommes concentrées sur l'objectif de créer un réseau VPN utilisant le protocole IPSec pour protéger contre les menaces présentes dans les réseaux TCP/IP, Notre motivation centrale est la sécurité des données dans le réseau 4G/LTE.

Pour développer notre idée, nous avons examiné la sécurité des réseaux informatiques et les risques auxquels notre réseau cellulaire est exposé lorsqu'il est connecté au réseau public IP. La méthodologie adoptée dans ce travail montre la migration progressive des protocoles de sécurité du la quatrième génération.

L'authentification mutuelle entre un terminal et le réseau opérateur, basée sur l'utilisation d'algorithmes de chiffrement, d'authentification et de génération de clés de sécurité robustes, représente une amélioration significative. Cependant, la couverture des protocoles de cette génération reste inférieure lorsqu'il s'agit d'une connexion au réseau Internet.

L'inconvénient souligné dans ce mémoire est que les données transmises dans le réseau 4G/LTE suivent une architecture bien définie en passant par le réseau public IP, ce qui les expose à des risques d'attaques et d'intrusions. Pour remédier à ces intrusions, nous avons proposé et implémenté une solution de sécurité après avoir analysé toute l'architecture du réseau 4G/LTE. Cette solution consiste à créer un tunnel VPN utilisant le protocole IPSecurity, garantissant une communication sécurisée entre les sites distants via le réseau IP.

Grâce aux outils de conception et de mesure de PACKET TRACER, nous avons pu développer et valider notre solution par une simulation. Cette simulation a démontré que notre réseau est sécurisé grâce à l'application du protocole IPSec intégré dans le VPN. Elle a prouvé que ce système est très complet, répondant à de nombreux besoins en matière de sécurité et capable de s'adapter à diverses situations.

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.

Références

1. *PUJOLLE Guy , Les Réseaux , Eyrolles, 2014.*

2. https://commumobile.wordpress.com/2015/06/06/les-reseaux-mobiles/

3. *https://bastienbonnard.com/1444-2 .*

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. *JOACHIN Tisal, Le Réseau GSM, DUNOD, 2003.*

6. *LESCUYER Pierre, Réseaux 3G : principe, architecture et services de l'UMTS, DUNOD, 2006.*

7. *PEREZ Andre , Architecture des réseaux de télécommunication, Lavoisier, 2002.*

8. *LAGRANGE Xavier, TABBANE Sami et JOLIVET Paul, Principe et évolutions de l'UMTS, Chapitre 2, Lavoisier, Edition 2005.*

9. *ABDOUL.R et MAHAMA.S, Optimisation des réseaux GSM pour la migration vers l'UMTS, Mémoire d'ingéniorat, ITO d'Oran, juin 2005.*

10. *JAVIER Sanchez et MAMADOU Thioune, UMTS, Lavoisier, Edition 2004.*

11. *https://www-igm.univ-mlv.fr/~dr/XPOSE2006/eric_meurisse/umts.php.*

12. *https://fr.slideshare.net/iamabdo1/long-term-evolution-lte-4g.*

13. *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.*

14. https://blog.j2sw.com/gear/wireless-2/lte-components/.

15. https://www.researchgate.net/figure/E-UTRAN-architecture-The-LTE-network-architecture-consists-of-evolved-NodeBs-eNBs_fig3_277687818.

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

17. Bechini.T , « Gestion de la Mobilité, de la Qualité de Service et Interconnexion de Réseaux Mobiles de Nouvelle Génération », Thèse de doctorat, Université e Toulouse,10/06/2010.

18. Couzinet.H, Nanfack.J et Njoudji.R, « Analyse et suivi de la QoS dans le système LTE », Rapport de Stage, Université Telecom Bretagne, 2009.

19. http://4glte.over-blog.com/page/2 / Date de consultation janvier 2017.

20. https://www.oreilly.com/library/view/lte-lte-advanced-and/9781119970453/ch14-sec002.html.

21. https://pacem.global/imsi-catcher-fonctionnement-et-realite-decryptage/.

22. ERICSON WCDMA System Overview,LZU1085418, Ericsson AB 2014.

23. (Jin Cao, Maode Ma, Senior Member, IEEE Hui Li, Member, IEEE, Yueyu Zhang, and ZhenxingLuo, A Survey on Security Aspects for LTE and LTE-A Networks,IEEE Com- munications Surveys Tutorials, Vol. 16, No. 1, First Quarter 2014.

24. Kasmi.C et Benjamin.M, État des lieux de la sécurité des communications cellulaires,ANSSI 51 bd.de la Tour Maubourg 75700 Paris Cedex 07 France.

25. https://web.maths.unsw.edu.au/~lafaye/CCM/crypto/crypto.htm.

26. https://www.cisco.com/c/fr_ca/products/security/firewalls/what-is-a-firewall.html.

27. https://web.maths.unsw.edu.au/~lafaye/CCM/protect/firewall.htm.

28. https://ccnareponses.com/notions-de-base-sur-la-commutation-le-routage-et-sans-fil-modules-14-concepts-du-routage/