REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté de Technologie

Département Ingénierie des Systèmes Electriques

Mémoire de Master

Présenté par :

LAIMECHE Dounia
ARKOUB Lyna Chaima
FAISI Camelia

Filière : Télécommunications
Spécialité : Réseaux et Télécommunications

POC LTE BACKHAULING OVER FTTH

Soutenu le 25 /06 /2024 devant le jury composé de :

HAMADOUCHE M'Hamed	Professeur	Université de Boumerdès	Président
MESSAOUDI Noureddine	Professeur	Université de Boumerdès	Examinateur
MERAIHI Yassine	Professeur	Université de Boumerdès	Encadreur
SAIDI Sofiane	Ingénieur	Optimum Télécom Algérie S.P.A	Co-Encadreur

Année Universitaire : 2023/2024

Remerciements

Nous tenons tout d'abord à adresser nos plus vifs remerciements à notre promoteur MERAIHI Yassine pour l'aide qu'il nous a apportée, ses précieux conseils, ses qualités humaines et scientifiques et son soutien constant tout au long de ce mémoire. Nous tenons à remercier également Monsieur SAIDI Sofiane Ingénieur à Optimum Télécom Algérie S.P.A pour avoir codirigé ce travail, pour son aide, ces critiques, ces précieux conseils et sa disponibilité imminente malgré ses différents engagements. Nous voudrons également remercier sincèrement les membres du jury. D'abord, le professeur HAMADOUCHE M'Hamed qui nous a honoré en acceptant d'être le président de jury formé pour la soutenance de notre mémoire. Ensuite, le professeur MESSAOUDI Noureddine pour avoir évalué notre thèse et apporté des commentaires judicieux.

Nous remercions bien évidement nos parents, à qui nous dédions ce travail. Ils nous ont non seulement encouragé et supporté tout au long de nos études mais dans toutes les sphères de notre vie.

Nous remercions également nos amis qui nous permettent de garder un équilibre de vie en alliant études, travail et loisir pour leur soutien durant la période de rédaction de ce mémoire.

Nous remercions tous nos enseignants et tous ceux qui ont contribué de prés ou de loin à l'aboutissement de notre travail.

A tous ceux que nous aimons, et à tous ceux qui nous aiment. . .

Pour tout, merci infiniment.

Dédicaces

Le voyage n’a pas été court et il n’aurait pas dû l’être. Le rêve n’était pas proche et le chemin n’était pas parsemé de facilités, mais je l’ai fait et je l’ai atteint. Celui qui dit "je suis prêt pour cela" l’accomplit, et je l’ai fait, même si cela ne voulait pas, je l’ai accompli de force.

Et dans le moment le plus fier, je dédie ce travail à celle qui a fait de moi ce que je suis aujourd’hui. Mon ange pur et ma force après Dieu. À celle qui m’a soutenue sans limites et m’a donnée sans contrepartie, à la main invisible qui a enlevé les épines de mon chemin, qui a supporté chaque moment de douleur que j’ai traversé, qui m’a soutenue et veillé de longues nuits pour mon confort, et qui se levait à l’aube pour prier pour moi. À ma précieuse et bien-aimée mère " Bounoughaz Houria", je te dédie cet accomplissement qui n’aurait pas été possible sans tes sacrifices, sans ta lumière dans mes yeux et ta foi en moi.

À moi-même, grande et forte, qui ai supporté tous les échecs et continué malgré les difficultés.

À ma famille et à chaque personne qui m’a soutenue tout au long de ma vie.

À mes amis de toujours, à ceux du lycée et université plus particulièrement à lyna chaimaa et camelia et aux inspirateurs de ma réussite, à tous ceux qui ont contribué à mes sourires.

Enfin, je me tiens devant vous aujourd’hui, le cœur rempli d’un mélange d’émotions contradictoires : la joie de l’accomplissement et la tristesse de la séparation, des sentiments mêlés aux souvenirs d’un long parcours éducatif, plein de défis et de réussites.

Dounia

Dédicaces

Je dédie ce modeste et humble travail à mes chers parents pour leur soutient, présence et patience. Spécialement ma chère mère, dont le soutien indéfectible et l'amour inconditionnel ont été les fondations sur lesquelles j'ai construit ce mémoire. Chers parents, votre encouragement constant et vos sacrifices ont été la source de ma motivation et de ma détermination à réussir.

A mes grandes mères, mon frère Abdelmalek et toute ma famille. À mes amis, qui ont partagé cette aventure avec moi, nous avons ri, pleuré et grandi ensemble. Votre soutien, vos encouragements et les échanges intellectuels ont été d'une valeur inestimable. Merci d'avoir été là à chaque étape du chemin. Plus particulièrement à Faisi Camelia et Laimeche Dounia.

Lyna

Dédicaces

Je dédie ce modeste travail à mes chers parents qui ont été toujours à mes côtés et m'ont toujours soutenu tout au long de ces grandes annés d'études.
À mes chers soeurs et leurs enfants.
À mon unique frére.
À ma famille FAISI et ZERROUKI.
Et à tous mes amies, tout particullièrement ARKOUB LYNA CHAIMA et LAIMECHE DOUNIA.
À tous ceux qui me sont chers, aux personnes qui m'ont aidé et encouragé de prés ou de loin,qui étaient toujours à mes côtés et qui m'ont accompagné durant mon chemin d'études.

Camelia

Résumé

De la première à la quatrième génération, les progrès technologiques des réseaux mobiles ont eu un effet considérable sur notre quotidien. Avec l'arrivée de la quatrième générateon (4G) , la transmission de données a connu une augmentation significative. Cette nouvelle génération a pour objectif d'améliorer l'efficacité spectrale, de gérer les appareils mobiles dans la même cellule et de garantir des débits élevés dans les situations mobiles.

Le défi majeur pour ces réseaux consiste à renforcer la sécurité du réseau tout en faisant des économies et en répondant aux exigences croissantes en matière de qualité de service et d'optimisation des ressources internes.

Le tunnel IPsec constitue une solution appropriée, qui repose sur des tunnels privés sécurisés pour la transmission des informations. Toutefois, la configuration et la gestion peuvent être difficiles, ainsi que l'introduction d'un traitement supplémentaire et la nécessité d'équipements supplémentaires.

Le but principal de cette étude consiste à présenter un réseau sécurisé afin de résoudre le problème de déploiement tout en réduisant au minimum les dépenses liées à l'équipement.

Il y a quatre chapitres dans l'étude : une étude préliminaire du réseau DJEZZY, une analyse de l'évolution des réseaux mobiles, des objectifs de la 4G, et une approche basée sur le réseau IPsec , MPLS et VRF, avec des protocoles de routage internes et externes.

Mots-clés : Tunnel IPsec , 4G, Réseaux Mobiles , protocoles de routage, Tunnel privés , VRF , MPLS.

Abstract

From the first to the fourth generation, technological advances in mobile networks had a considerable effect on our daily lives. With the arrival of the fourth generation (4G), data transmission has seen a significant increase. This new generation aims to improve spectral efficiency, manage mobile devices in the same cell and guarantee high speeds in mobile situations.

The major challenge for these networks is to strengthen network security while saving money and meeting increasing demands for quality of service and optimization of internal resources. The IPsec tunnel is a suitable solution, which relies on secure private tunnels for the transmission of information.

However, setup and management can be difficult, as well as the introduction of additional processing and the need for additional equipment. The main goal of this study is to present a secure network to solve the deployment problem while minimizing equipment expenses.

There are four chapters in the study : a preliminary study of the DJEZZY network, an analysis of the evolution of mobile networks, the objectives of 4G, and an approach based on the IPSEC, MPLS and VRF network, with internal and external routing protocols.

Keywords : IPsec Tunnel, 4G, Mobile Networks, Routing Protocols, Private Tunnel, VRF, MPLS

ملخص

من الجيل الأول إلى الجيل الرابع، كان للتقدم التكنولوجي في شبكات الهواتف المحمولة تأثير كبير على حياتنا اليومية. مع وصول الجيل الرابع، شهدت نقل شهدت نقل البيانات زيادة كبيرة. تهدف هذه الجيل الجديد إلى تحسين الكفاءة الطيفية، إدارة الأجهزة المحمولة في نفس الخلية وضمان سرعات عالية في الحالات المتنقلة.

التحدي الرئيسي لهذه الشبكات يكمن في تعزيز أمان الشبكة مع تحقيق وفورات مالية وتلبية المتطلبات المتزايدة فيما يتعلق بجودة الخدمة وتحسين الموارد الداخلية.

يشكل نفق IPsec حلاً مناسباً، حيث يعتمد على أنفاق خاصة مؤمنة لنقل المعلومات. ومع ذلك، قد تكون إعدادات وإدارة هذه الأنفاق صعبة، بالإضافة إلى تقديم معالجة إضافية والحاجة إلى معدات إضافية.

الهدف الرئيسي من هذه الدراسة هو تقديم شبكة آمنة لحل مشكلة النشر مع تقليل النفقات المتعلقة بالمعدات إلى الحد الأدنى.

تتكون الدراسة من أربعة فصول :دراسة أولية لشبكة ديجيزي، تحليل تطور شبكات الهواتف المحمولة، أهداف الجيل الرابع، ونهج يعتمد على شبكة IPsec و MPLS وVRF، مع بروتوكولات التوجيه الداخلية والخارجية.

الكلمات الرئيسية IPSec :، 4G، نفقIPSEC ، شبكات الهاتف المحمول، بروتوكولات التوجيه الداخلية والخارجية، نفق خاص، VRF، MPLS.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

A

ADSL : Asymmetric Digital Subscriber Line
AS : Autonomous System
ASG : Analytic Services Gateway
ASBR : Autonomous System Boundary Router

B

BGP : Border Gateway Protocol

C

CAN : Campus Area Network

E

E-UTRAN : Evolved Universal Terrestrial Radio Access Network
eNodeB : Evolved Node B
EPC : Evolved Packet Core
ePDG : evolved Packet Data Gateway
EGP :Exterior Gateway Protocol
E-BGP : External Border Gateway Protocol
ENSP : Enterprise Networking Solutions Provider

F

FDMA : Frequency Division Multiple Access
FDD : Frequency Division Duplexing

G

GSM : Global System for Mobile Communications

H

HSPA : High Speed Packet Access
HSS : Home Subscriber Server
HLR : Home Location Register

I

IoT : Internet of Things.
IP : Internet Protocol
IMS : IP Multimedia Subsystem
IGP : nterior Gateway Protocol
IS-IS : Intermediate System to Intermediate System
I-BGP : Internal Border Gateway Protocol

IP/MPLS : Internet Protocol/Multiprotocol Label Switching
IPv4 : Internet Protocol version 4
IPv6 : Internet Protocol version 6
IPsec : Internet Protocol Security
IETF : Internet Engineering Task Force

L

LTE : Long-Term Evolution
LAN : Local Area Network
LSA : Link State Advertisement
LDP : Label Distribution Protocol
LSP : Label-Switched Path

M

MMS : MultiMedia Messaging Service
MIMO : Multiple-Input Multiple-Output
MME : Mobility Management Entity
MAN : Metropolitan Area Network
MPLS : Multiprotocol Label Switching

O

OFDMA : Orthogonal Frequency Division Access.
OSI : Open Systems Interconnection
OSPF : Open Shortest Path First

P

PDN-GW : Packet Data Network Gateway
PCRF : Policy and Charging Rules Function

Q

QoS : Quality of Service

R

RNC : Radio Network Controller
RF : Radio Frequency
RIP : Routing Information Protocol
RD : Route Distinguisher
RSVP : Resource Reservation Protocol

S

SMS : Short Message Service
SC-FDMA : Single Carrier Frequency Division Multiple Access
SGW : Serving Gateway

SIP : Session Initiation Protocol
SAE : (System Architecture Evolution)

T

TDMA : Time Division Multiple Access
TDD : Time Division Duplexing
TAN : Tiny Area Network
TCP/IP :Transmission Control Protocol/Internet Protoco
TE : Traffic Engineering

U

UMTS : Universal Mobile Telecommunications System
UIT : Union internationale des télécommunications
UE : User Equipment

V

VoIP : Voice over Internet Protocol
VPN : Virtual Private Network
VRF : Virtual Routing and Forwarding
VPNv4 : Virtual Private Network Version 4

W

W-CDMA : Wideband Code Division Multiple Access
WIFI : Wireless Fidelity
WLAN : Wireless Local Area Network
WAN : Wireless Area Network

Introduction Générale

Les évolutions technologiques des réseaux mobiles ont connu un essor important de manière exponentielle ces dernières années allant de la première génération à la quatrième génération. Ces réseaux s'imposent d'une façon indéniable dans notre vie quotidienne permettant un accès permanant à des objets connectés.

En 2010, l'introduction de la Quatrième Génération (4G) a considérablement accéléré la transmission des données. Cette génération de technologie mobile vise à améliorer l'efficacité spectrale et à augmenter la capacité de gestion des appareils mobiles dans une même cellule. Elle cherche également à offrir des débits élevés en situation de mobilité et à garantir une mobilité totale à l'utilisateur en assurant l'interopérabilité entre diverses technologies existantes.

Pour une meilleure protection du réseau et des économies, les ingénieurs de l'entreprise ont proposé trois opérations. Pour répondre aux demandes croissantes de qualité de service et d'optimisation des Ressources, en prenant en compte les facteurs de performance, de cout et disponibilite des resources, afin d'optimiser l'efficacité du déploiement et de la qualite de service pour les utilisateurs et a couse d'économisassions de cout de la partie accès dJEZZY a propose tois scenario pour deployer un site 4G ce qui sera expliqué par la suite.

Le problème majeur des réseaux mobiles de la 4G est la sécurité et la protection du réseau en tenant compte des facteurs de performance, du coût et de disponibilité des ressources, afin d'optimiser l'efficacité du déploiement et la qualité de service pour les utilisateurs. Le réseau tunnel IPsec s'avère la solution la plus appropriée pour le résoudre.

L'objectif principal de notre travail est de proposer un tunnel sécurisé basé sur le protocole IPsec pour résoudre le problème de déploiement du réseau tout en respectant la contrainte du coût des équipements. Le tunnel IPsec est une technologie basée sur l'utilisation des tunnel privés sécurisés pour la transmission des données. Il est caractérisé par sa confidentialité, l'intégrité et l'authentification des données, ainsi que la protection contre les attaques par relecture, immunité aux interférences et faible coût ce qui le rend une alternative révolutionnaire à la transmission des données. Le tunnel IPsec est utilisé dans des communications des réseaux extérieures comme un réseau d'entreprise et un réseau Internet. Cependant, IPsec peut être complexe à configurer et gérer, introduire une surcharge de traitement, et nécessite des mises à jour ou des équipements supplémentaires pour une prise en charge complète.

Notre mémoire est divisé en quatre chapitres représentés comme suit :

Dans **le premier chapitre**, nous présentons une étude préalable du réseau de DJEZZY dans lequel nous introduisons l'organisme d'accueil , Par la suite, nous expliquons le réseau existant selon les trois niveaux du réseau CORE.

Dans **le deuxième chapitre**, nous traitons l'évolution des réseaux mobiles de la première génération à la quatrième génération, nous abordons aussi les avantages et limites de la 4G, son architecture ainsi que ces performances et caractéristiques.

Dans **le troisième chapitre**, nous nous intéressons aux différents types de routages et les protocoles à utiliser. Nous décrivons également les principes de fonctionnement des technologie MPLS, IPsec et VRFs.

Le quatrième chapitre, est consacré à la présentation de notre approche basée sur le réseau Tunnel IPSEC avec les protocoles de routages internes et externes avec Algérie Télécom pour la résolution des problèmes de sécurité tout on optimisant la capacité et la rentabilité du réseau.

Ce mémoire ce termine par une conclusion générale et des perspectives que nous avons tracé pour d'éventuelles améliorations et une poursuite de ce travail.

Chapitre 1

Étude préalable

1.1 Introduction

Afin de débuter notre étude et de mettre en contexte notre recherche, nous introduisons d'abord DJEZZY, l'un des principaux opérateurs de réseaux mobiles en algérie. Par la suite, nous examinons le niveau actuel du réseau et repérons les difficultés qui en résultent. D'après notre étude, nous suggérons des solutions qui permettront de résoudre ces problèmes de manière efficace.

1.2 Présentation de l'organisme d'accueil

L'opérateur de télécommunications Algérien Djezzy, fondé en juillet 2001, est leader dans le secteur de la téléphonie mobile en Algérie. Avec une base de plus de 15 millions d'abonnés en septembre 2023, Djezzy offre une gamme complète de services, allant du prépayé au post-payé, en passant par la Data, les services à valeur ajoutée et le SUT. Djezzy s'est toujours distinguée par son engagement envers l'innovation et la qualité de service, visant aujourd'hui à se positionner comme un acteur technologique de premier plan dans le pays.

Depuis juillet 2022, un tournant majeur s'est opéré avec le transfert de la quasi-totalité des actions de VEON au profit du FNI-Fonds National d'Investissement. En devenant une Entreprise Publique Economique, Djezzy est désormais détenue à hauteur de 96,57 par le FNI qui joue un rôle significatif dans le développement socio-économique du pays. L'entreprise s'est fixée pour objectif d'étendre son réseau commercial sur l'ensemble du territoire national, notamment dans le Grand Sud, en ouvrant des boutiques dans dix nouvelles wilayas.

Djezzy a déjà accompli des réalisations significatives en matière de connectivité, couvrant 95 de la population à travers l'Algérie et déployant avec succès des services 3G et 4G dans les 58 wilayas. Ces jalons clés dans son histoire, tels que l'octroi des licences 2G, 3G et 4G, illustrent son engagement constant envers l'expansion de la technologie.

L'ambition de Djezzy ne s'arrête pas là. En tant qu'entreprise publique économique, elle vise à devenir un acteur technologique majeur en Algérie. Son objectif est de favoriser le développement de la connectivité et de contribuer activement à la digitalisation du pays. Forte de son expérience et de son leadership, Djezzy s'efforce de façonner l'avenir technologique de l'Algérie en proposant des solutions innovantes et en garantissant un accès de qualité à la communication et à la connectivité à travers tout le pays [3].

1.3 Organigramme de djezzy

Structure de Djezzy : l'organisation d'optimum télécom Algérie S.P.A qui a une partie de manageant qui décompose en six parties et chaque partie et a ait décomposé.
Le département de manageant est constitué de plusieurs services comme le montre Structure, il est charge : (MEGRI, 2015)
. Du contrôle des transactions.
. De la surveillance des incidents.
. De la charge d'un réseau local ou interconnecté.
. L'administration du réseau.
. La mise en oeuvre des nouveaux services.
. l'administration des accès et de la bande passante. [4]

1.4 Zoom sur le service réseau dans lequel nous trouvons

Nous avons réalisé ce stage au service du Core Network qui se compose en cinq parties qui sont :
. Core planning , integration CS, PS.
. Core Data Network.
. Core Environnement , Power.
. Budget, Core Project.
. Core Infrastructure , Virtualisation. [4]

1.5 Étude de l'existant

Notre stage de fin d'étude s'est déroulé au sein de l'entreprise Djezzy Dar El Beida, plus précisement dans le service réseau LTE. Ce service est chargé de la gestion, du maintien et de l'amélioration de ce réseau, ainsi que de la définition de sa stratégie d'évolution. Nous avons pour mission principale d'analyser et d'étudier en profondeur le LTE actuel de Djezzy. La figure 1.1 illustre l'architecture de ce réseau et nous sert de référence. Nous visons à repérer les difficultés et les manques actuels du réseau afin de suggérer des solutions appropriées et efficaces pour les résoudre.

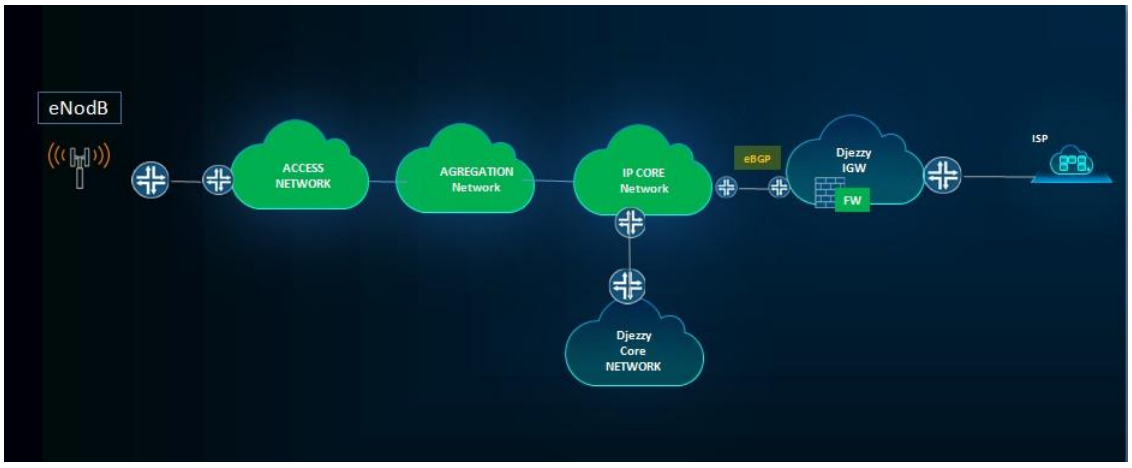

Figure 1.1 – Architecture du réseau de Djezzy .

La structure du réseau de djezzy est composée de trois niveaux, chacun jouant un rôle particulier dans le fonctionnement global du réseau. Le réseau d'accès, le réseau d'agrégation et le réseau coeur sont les niveaux suivants.

- **Le réseau d'accès**, qui est le premier niveau, joue un rôle essentiel dans la connexion entre djezzy et ses abonnés. C'est la section du réseau qui permet aux abonnés de se connecter directement aux services de l'opérateur. Le réseau d'accès collecte les données des utilisateurs connectés à travers divers réseaux, tels que la 1G, la 2G, la 3G ou la G4. Ces informations sont transférées vers le niveau suivant, le réseau d'agrégation.
- **Le réseau d'agrégation**, est le deuxième niveau chargé de recueillir et de regrouper le trafic provenant des différentes régions (wilayas) des services de djezzy. C'est un réseau intermédiaire qui regroupe le trafic des réseaux d'accès et le déplace vers le niveau supérieur, le réseau le plus important. L'agrégation est constituée de 48 réseaux.
- **le réseau coeur**, est le niveau central et principal du réseau de Djezzy.

1.6 Conclusion

Au début de ce chapitre, nous introduisons le contexte de notre étude et établissons les objectifs de recherche que nous visons à atteindre. Ce chapitre nous permet de passer à la prochaine étape de notre recherche, à savoir l'état actuel des connaissances. En saisissant le contexte et en exposant la problématique de manière claire, nous sommes prêts à examiner en détail les travaux récents et les progrès dans notre domaine d'étude.

Chapitre 2

Généralités sur le réseau Évolution à Long Terme (Long Term Evolution (LTE))

2.1 Introduction

Au cours des dernières décennies, les réseaux mobiles ont connu une évolution rapide, passant des réseaux mobiles de première génération (1G) qui ne permettaient que la communication vocale à des réseaux mobiles de cinquième génération (5G) qui proposent des vitesses de téléchargement Ultra-rapides et une latence réduite. La motivation de cette évolution réside dans la demande. croissante des utilisateurs pour des services de communication mobiles plus rapides et plus avancés, Comme :Internet des objets (IoT) et la télémédecine, ainsi que dans les progrès technologiques dans les domaines de la transmission de données, de la connectivité sans fil et de la Miniaturisation des composants électroniques. Ce chapitre commence par un bref aperçu sur l'évolution des réseaux mobiles. Ensuite, nous allons aborder la technologie quatrième génération (4G), ses différents aspects tels que les technologies et les exigences. Par ailleurs, nous soulignerons l'utilisation de l'optique sans fil et filaire dans la 4G.

2.2 Généralités sur les réseaux mobiles

Un réseau mobile est un système de télécommunications qui permet la communication sans fil entre des appareils mobiles tels que les téléphones portables, les tablettes et les ordinateurs portables. Ces réseaux sont conçus pour offrir une connectivité sans fil à grande échelle, permettant aux utilisateurs de communiquer, d'accéder à Internet, d'échanger des données et d'utiliser divers services en déplacement. Ils reposent généralement sur une architecture en cellules, où chaque zone géographique est divisée en cellules desservies par des stations de base, assurant une couverture continue et une gestion efficace des ressources radio. Chaque cellule est contrôlée par une station de base, qui établit la liaison radio avec les terminaux mobiles dans sa zone de couverture. La portée d'une station de base est déterminée par plusieurs facteurs, tels que la puissance d'émission des terminaux et des stations de base, la fréquence utilisée, le type d'antennes, l'environnement de la propagation et la technologie radio employée. Les réseaux mobiles varient en termes de qualité de service, ce qui a conduit à leur évolution de la 1G jusqu'à la 5G. [5]

2.3 L'evolution des différentes générations de téléphonie mobile

2.3.1 Réseaux de première génération (1G)

Le réseau mobile de la 1G est mis en service au milieu des années 70 et s'est lancé au début des années 80. Basée sur une technologie analogique, cette première génération permettait uniquement de passer et de recevoir des appels vocaux. Son émergence a marqué le début de la commercialisation des premiers appareils mobiles et a marqué la transition de la téléphonie analogique vers la téléphonie numérique, ouvrant ainsi la voie. [5]

2.3.2 Réseaux de deuxième génération (2G)

Au milieu des années 1990, le réseau GSM a fait son apparition. Il s'agit d'une norme de téléphonie mobile de deuxième génération largement utilisée à l'échelle mondiale. Le Système Global pour les Communications Mobiles (GSM) utilise une architecture en cellules et la technologie TDMA pour permettre la communication sans fil entre les appareils mobiles et les stations de base. En plus des services vocaux, le GSM offre des services de données à faible débit, tels que les SMS et les MMS. Cette technologie a été déployée à grande échelle dans les années 1990 et continue de jouer un rôle crucial dans les régions où les infrastructures de réseau plus avancées ne sont pas encore disponibles. [5]

2.3.3 Réseaux de troisième génération (3G)

Par la suite, au début des années 2000, est apparue la 3G (connue sous le nom de Système Universel de Télécommunications Mobiles UMTS), la troisième génération de réseau mobile, qui est sans doute la plus populaire et la plus connue du grand public, car elle a été à l'origine de l'émergence et de l'essor des smartphones à la fin des années 2000. Les utilisateurs peuvent ainsi naviguer sur internet, consulter leur courrier électronique, envoyer des photos et des vidéos avec un débit adéquat de 1,9 Mb/s, soit une vitesse 5 à 10 fois supérieure à celle des générations précédentes. [5]

2.3.4 Reseaux de quatrième génération (4G)

En 2010, l'introduction de la 4G entraîne une augmentation significative de la vitesse de transmission des données. Cette génération de réseau vise à améliorer l'utilisation du spectre et à gérer plus efficacement le nombre croissant d'appareils mobiles dans une même zone. Elle aspire également à fournir des débits élevés même en mobilité, tout en permettant une transition fluide entre différentes technologies existantes. Les principaux objectifs de la 4G comprennent la garantie de la continuité des sessions en cours, réduction des délais et du trafic de signalisation, amélioration de la qualité de service, l'optimisation des ressources, la réduction de la latence et des pertes depaquets, ainsi que la minimisation des coûts de signalisation. [5]

2.3.5 Réseaux de cinquième génération (5G)

La 5G est la dernière génération de réseau mobile qui a été mise en place progressivement depuis 2020. Elle permet une transmission de données en temps réel extrêmement rapide (par exemple, Elle permet théoriquement de télécharger un film en quelques secondes. Les réseaux 5G pourront envoyer les données à une vitesse jusqu'à 20 fois supérieure à celle des réseaux LTE permettront de connecter environ 1 million d'appareils par km2. En conséquence, cette technologie offre de nombreuses opportunités, telles que les voitures automatiques, la télémédecine, l'utilisation de la réalité augmentée dans

le domaine de l'éducation et les villes intelligentes. Bien que le déploiement officiel de la 5G ne soit pas encore en cours en Algérie, des études sont actuellement menée en vue de son adoption. [5]

2.4 L'objectif de la 4G

La 4G des réseaux mobiles a pour objectif d'optimiser l'efficacité spectrale et d'accroître la capacité de gestion du nombre de mobiles dans une seule cellule. Son objectif est également de garantir des débits élevés en situation de mobilité et d'assurer une transition fluide entre différentes technologies existantes. Elle vise principalement à rendre le passage entre les réseaux transparents pour les utilisateurs, à prévenir les interruptions de service lors des transferts entre les cellules et à migrer vers une infrastructure entièrement basée sur protocole Internet IP.
Les principaux objectifs des réseaux de 4éme génération comprennent :
• Maintenir la continuité des sessions en cours.
• Réduire les délais et le trafic de signalisation.
• Améliorer la qualité de service.
• Optimiser l'utilisation des ressources.
• Diminuer les délais de relève, les délais de bout en bout, la gigue et la perte de paquets.
• Réduire les coûts de signalisation. [6]

2.5 Les Avantages de la 4G

La 4G des réseaux cellulaires est de plus en plus employée afin de satisfaire lesbesoins d'une connectivité flexible et continue, ainsi que pour offrir une solution de secours pour assurer la continuité des activités dans le contexte des réseaux câblés classiques. Avec la 4G, la transmission de toutes les informations vocales et données se fait par IP, similaire à celui utilisé surInternet.
Cette transition rend la gestion plus simple et moins coûteuse pour les fournisseurs, tout en facilitant le développement d'applications multimédias.
Cette génération permet des vitesses de téléchargement plus rapide et des temps de latence plus courts. Selon les normes établies par L'UIT pour les réseaux cellulaires, la 4G devrait fournir des vitesses de téléchargement pouvant atteindre 100 Mbits/s pour les utilisateurs en mouvement et 1 Gbit/s en mode stationnaire. [7]

2.6 Les limites de la 4G

Un des principaux inconvénients de la 4G réside dans son coût potentiellement supérieur à celui de la 3G. En effet, elle requiert une technologie et une infrastructure plus avancées pour offrir les taux.de transfert de données à grande vitesse qu'elle propose. De plus, la 4G peut consommer plus d'énergie que la 3G, ce qui entraîne une décharge plus rapide de la batterie des smartphones lors de son utilisation. [7]

2.7 La fréquence utilisé par l'Évolution à Long Terme LTE

• **Fréquences inférieures (sub-1 GHz) :** Ces fréquences ont la particularité de mieux pénétrer à travers les bâtiments et de couvrir une plus grande distance. Elles sont fréquemment utilisées dans

les zones rurales ou suburbaines. En général, les bandes de fréquences inférieures sont situées autour de 700 MHz, 800 MHz et 900 MHz.

• **Fréquences moyennes (1-6 GHz) :** Ces fréquences offrent un bon équilibre entre la portée et la capacité. Elles sont couramment utilisées dans les zones urbaines et densément peuplées. Les bandes de fréquences moyennes incluent généralement des fréquences autour de 1,8 GHz et 2,6 GHz.

• **Fréquences supérieures (au-dessus de 6 GHz) :** Ces fréquences offrent une capacité. Élevées, mais ont une portée limitée et peuvent être plus sensibles aux obstacles. Elle a Utilisées pour augmenter la capacité dans les zones à forte densité de trafic. Les bandes des fréquences supérieures, généralement situées autour de 3,5 GHz et 5 GHz, font partie de ce Qu'on appelle "la gamme de fréquences millimétriques" (mmWave). [8]

2.8 Le canal utilisé par la 4G

L'Évolution à Long Terme (LTE) emploie une méthode connue sous le nom d'Accès Multiple par Répartition Orthogonale de Fréquence OFDMA pour séparer la bande de fréquences en sous-porteuses (ou canaux) afin de faciliter la transmission simultanée de plusieurs circulations de données. Les canaux dans la 4G LTE peuvent ajuster leur largeur en fonction des besoins de capacité et de performance du réseau, mais ils ont généralement une largeur de plusieurs mégahertz (MHz). Ces canaux LTE sont attribués de manière dynamique selon les exigences du réseau et les conditions de trafic. [9]

2.9 Performance et caractéristique des réseaux 4G

LTE vise principalement à améliorer le support des services de données en augmentant la capacité, en améliorant les débits et en réduisant la latence.

2.9.1 La capacité en nombre d'utilisateurs simultanés

En raison de l'augmentation des services qui requièrent une connexion continue, la limitation de la capacité d'utilisation simultanée devient croissante. Le système doit être capable de gérer.En même temps, un grand nombre d'utilisateurs par cellule. Il est prévu qu'il y ait au moins 25 utilisateurs simultanés par cellule à l'état actif pour une largeur de bande de 5 MHz, et auMoins de 100 utilisateurs pour des largeurs de bande supérieures. Il sera nécessaire de pouvoir.accueillir un nombre beaucoup plus élevé d'utilisateurs à l'état de veille .

2.9.2 Les débits

Des améliorations de débit ont également été demandées pour la technologie LTE par rapport au HSPA (Accès Haut Débit par Paquets). Les limites de débits maximales fixées pour le LTE sont les suivantes :

• Le débit descendant est de 100 Mbit/s pour une largeur de bande de 20 MHz, ce qui entraîne une efficacité spectrale crête de 5 bit/s/Hz.

• 50 Mbit/s en phase ascendante pour une largeur de bande de 20 MHz, ce qui entraîne une efficacité spectrale crête de 2,5 bit/s/Hz .

2.9.3 La latence

La latence du système se réfère à sa capacité à réagir rapidement aux demandes des utilisateurs ou des services, couvrant à la fois le plan de contrôle et le plan utilisateur.

• **Latence du plan de contrôle :** Pour le LTE, l'objectif est d'améliorer la latence du plan de contrôle par rapport à l'UMTS, en garantissant une transition en moins de 100 ms entre l'état de veille de l'équipement utilisateur et un état actif permettant l'établissement du plan. Utilisateur.

• **Latence du plan utilisateur** il s'agit du temps de transmission d'un paquet entre la couche.IP de l'UE et la couche IP d'un nœud du réseau d'accès, ou vice versa. En d'autres termes, c'est le délai de transmission d'un paquet IP dans le réseau d'accès. Le LTE vise à réduire cette latence à moins de 5 ms dans des conditions de faible charge du réseau, particulièrement pour des paquets IP de petite taille.

2.9.4 L'agilité en fréquence

Le LTE doit être capable de fonctionner sur des porteuses de diverses largeurs pour s'adapter à des allocations spectrales divergentes. Les bandes initialement nécessaires ont ensuite été ajustées pour être : 1,4 MHz, 3 MHz, 5 MHz, 10 MHz, 15. MHz et 20 MHz.

2.9.5 La mobilité

La mobilité joue un rôle essentiel dans un réseau mobile. Le LTE a pour objectif de Maintenir son fonctionnement pour des UE qui se déplacent à des vitesses élevées. (jusqu'à 350 km/h, et même 500 km/h en fonction de la bande de fréquences), tout en étant optimisé pour des vitesses de l'UE faibles (entre 0 et 15 km/h).

2.9.6 Codage et sécurité

Le codage Accès multiple par répartition orthogonale de la fréquence (OFDMA), est utilisé pour la liaison descendante, tandis que l'accès Multiple par Répartition en Fréquence à Porteuse Unique SC-FDMA, qui est une technologie de codage radio de type « accès multiple »par répartition en fréquence pour la liaison montante, est utilisé au lieu du accès Multiple par Répartition de Code à Large Bande W-CDMA.En Système Universel de Télécommunications Mobiles UMTS. L'OFDMA et sa variante SC-FDMA proviennent du codage OFDM (par exemple sur les liens ADSL (et dans les réseaux Wi-Fi), mais à la différence de l'OFDM, l'OFDMAEst conçu pour l'accès multiple, c'est-à-dire le partage simultané de la ressource.spectrale (bande de fréquence) entre plusieurs utilisateurs distants, les uns des autres. L'OFDMA est en adéquation avec la méthode.

2.9.7 Duplexage

Le fonctionnement de LTE est prévu en mode dual : duplexage de fréquences (FDD).Et duplexage temporel (TDD) conformément aux spécifications. L'émission et laRéception sont effectuées à des fréquences différentes en mode FDD (Frequency). Division duplexing. En mode TDD, la transmission et la réception se déroulent à la même fréquence, mais à des moments différents. Il s'agit du mode initial (FDD) qui est fréquemment utilisé dans les équipements. Télécoms et utilisé dans la plupart des premiers réseaux 4G LTE. Le second mode(TDD) opère sur des bandes de fréquences différentes qui seront attribuées plus tard. [10]

2.9.8 Les types de transmission utilisée dans la 4G

La technologie LTE offre un accès multiple distinct de celui de WCDMA, car en lien. Des cendant, elle repose sur l'OFDMA et en lien montant, elle repose sur le SC-FDMA. L'OFDMA garantit une protection efficace contre les conditions radio qui changent rapidement, telles que l'évanouissement rapide et les composants radio qui propagent à plusieurs trajets. Néanmoins, cette solution n'est pas particulièrement Performante, car le comportement du rapport de puissance du pic-à-moyenne par pose des problèmes lors de la conception des biens. C'est pourquoi le SC FDMA a été sélectionné dans la direction montante (UL) afin que l'UE puisse faire Face à cette contrainte. [10]

2.10 L'architecture de la 4G/LTE

Tout comme les générations précédentes, la technologie LTE a apporté des améliorations significatives en termes d'efficacité spectrale, de débit, de couverture et de capacité de traitement des appels par cellule. De même que ses prédécesseurs, elle est caractérisée par une architecture qui comporte.

- Un réseau d'accès : L'E-UTRAN.
- Un réseau Cœur : Réseau tout-IP. [7]

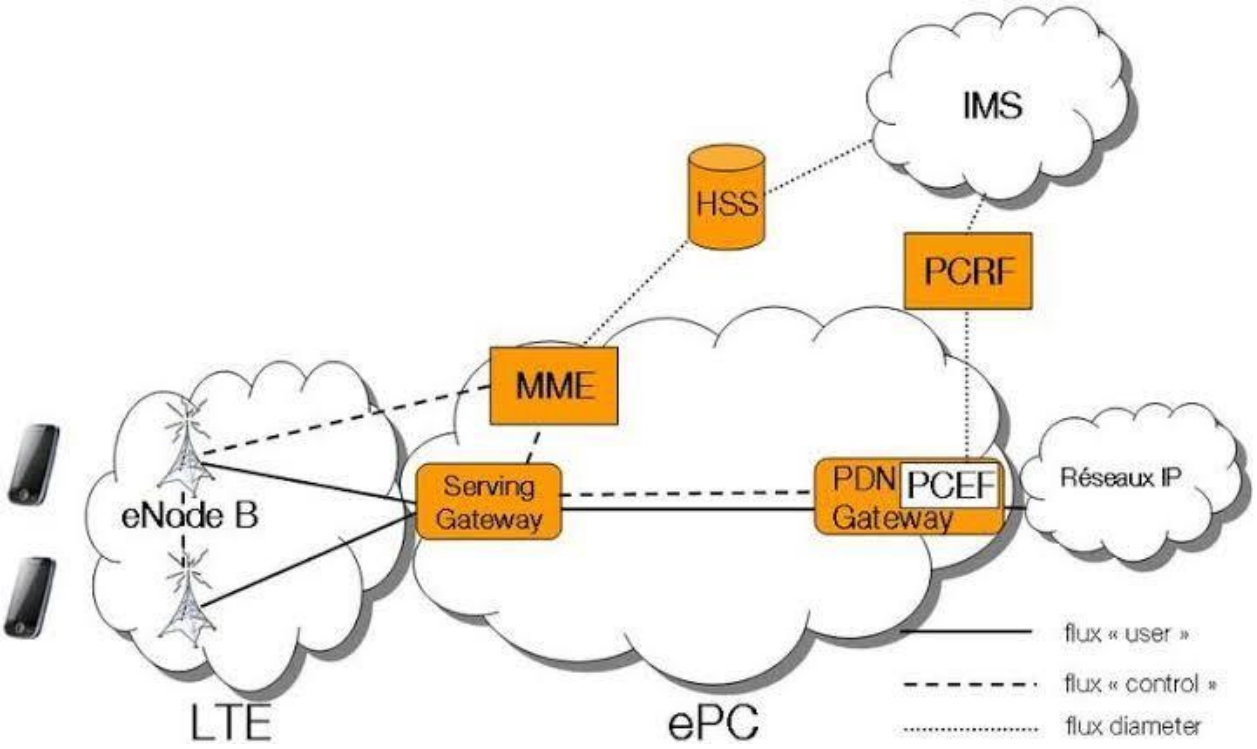

Figure 2.1 – Architecture de l'E-UTRAN. [1]

En fait, ce réseau est connu sous le nom d'EPS et il est constitué de deux parties distinctes : le réseau d'accès radio LTE évolué et le réseau coeur évolué appelé SAE.

2.10.1 Réseau d'accès (Evolved Universal Terrestrial Radio Access Network (E-UTRAN))

Seuls les bornes évoluée (eNodeB)composent ce système, assurant ainsi l'échange radio avec l'E-UTRAN. Contrairement à la 3G, les rôles du contrôleur de réseau radio (RNC)ont été répartis entre l'eNodeB et les entités du réseau central SGW. La responsabilité de cette section concerne la gestion des ressources radio, la gestion de la porteuse, la compression, la sécurité et la connectivité vers le réseau central évolué.

- **Nœud B Evolué (Evolved Node B (L'eNodeB))** L'eNodeB, équivalent de la NodeB dans le Système Universel de Télécommunications Mobiles (l'UMTS), a pour rôle principal de diriger les flux de données des équipements utilisateur (UE) vers le réseau cœur EPC. Il s'agit d'antennes qui connectent les UE avec le réseau central du LTE grâce aux interfaces radio RF. Les eNodeBs fournissent la fonctionnalité du contrôleur radio, ce qui permet d'obtenir des résultats plus efficaces et de réduire les latences du réseau.
- **L'interface X2 :**L'interface X2 est une interface logique conçue pour faciliter l'échange d'informations de signalisation entre les eNodeBs lors du handover ou de la signalisation, sans nécessiter l'intervention du réseau cœur. L'eNodeB est connecté au cœur du réseau via l'interface S1.
- **L'interface S1 :**Il s'agit de l'interface entre le réseau d'accès et le réseau cœur, et elle peut être subdivisée en deux interfaces distinctes :

. S1-U (S1-Usager) entre l'eNodeB et la passerelle de service (SGW).

. S1-C (S1-Contrôle) entre l'eNodeB et l'entité de gestion de la mobilité (MME).

Les eNodeB apportent deux avantages au réseau :

.Une amélioration de la sécurité en cas de défaillance d'un relais.

.Une optimisation du partage des ressources en cas de saturation du lien principal. [7]

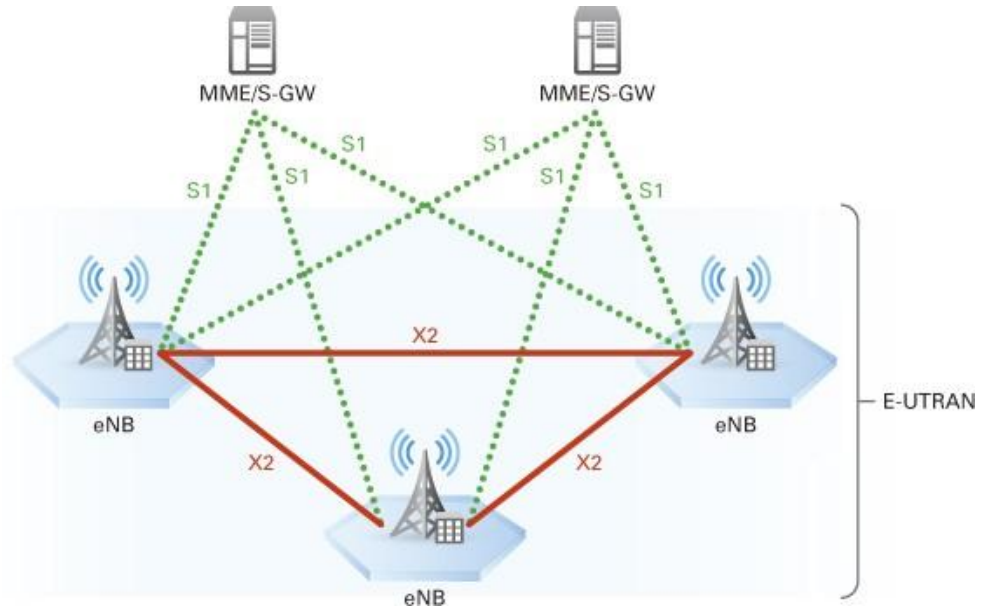

Figure 2.2 – Architecture E-UTRAN. [1]

2.10.2 Réseau Coeur (Evolved Packet Core (EPC))

Cœur de paquet évolué (EPC), est le nom du réseau cœur évolué, fonctionnant sur un système de paquets tout IP. Il est également capable de communiquer avec les réseaux 2G/3G. Ce réseau cœur assure diverses fonctions telles que la gestion des utilisateurs, la gestion de la mobilité, la gestion de la qualité de service et la gestion de la sécurité. Ces fonctions sont assurées par des équipements tels que le MME, le SGW, le PDN-GW et le PCRF.

- **MME :** La responsabilité de cette section est de connaître l'emplacement de l'utilisateur, de connaître son état et de gérer les procédures d'authentification et de mobilité des utilisateurs. Étant donné qu'elle effectue la dernière étape de la protection par codage, c'est donc le point qui confirme l'interception de signalisation. De cette manière, elle assure la gestion du signal entre l'UE (Utilisateur Equipment) et le réseau central. Les messages de paging sont diffusés par le MME lorsque l'UE ne peut pas recevoir les paquets qui lui sont destinés.
- **HSS :** Le serveur de l'abonné domicile (HSS) est une version améliorée du registre des emplacements domiciliaires (HLR). Il offre la possibilité de conserver des données d'abonnement qui peuvent être utilisées pour contrôler les appels et gérer les session des utilisateurs réalisés par le MME. Il stocke la numérotation et le profil des services auxquels les utilisateurs sont abonnés afin de les identifier. En outre, il renferme les données de connexion pour les autres réseaux, tels que le GSM, UMTS et LTE.
- **SGW :** La passerelle de service (SGW) est spécifiquement conçu pour la gestion des "données utilisateur" et est responsable de la routage et de la transmission des paquets de données entre les eUTRAN et le réseau coeur. Il joue le rôle d'une base de données locale qui facilite la mobilité entre les eNode B et permet de faire la transition entre les systèmes mobiles de différentes générations, tels que LTE et le système universel de télécommunications mobiles (UMTS). Il gère également le contexte du terminal mobile (UE), tels que les paramètres de la porteuse de service et le routage des informations.
- **PCRF :**La fonction de règles de politique et de tarification (PCRF) est un organisme chargé de garantir la qualité de service nécessaire au réseau, il est responsable de la prise de décision principale en matière de contrôle. Effectivement, il assure la gestion des politiques de facturation qui doivent être prises en considération par la passerelle de réseau de données par paquets (PDN-GW) et qui doivent être appliquées en fonction des actions de l'utilisateur.
- **PDN-GW :** La passerelle de réseau de données par paquets (PDN-GW)constitue le point de connexion entre l'utilisateur mobile et les autres réseaux PDN. Il joue le rôle d'un routeur par défaut par lequel les requêtes de l'utilisateur sont transmises. Le PDN Gateway assigne les adresses IP à chaque Terminal Mobile, filtre les paquets et enregistre les octets échangés.
- **ePDG :** Un composant réseau qui assure une interopérabilité avec le réseau WLAN en offrant des fonctionnalités de routage des paquets, de tunneling, d'authentification, d'autorisation et d'encapsulation / décapsulation des paquets.
- **La partie IMS :** Le système multimédia sur IP (IMS) est une nouvelle architecture utilisée dans les réseaux mobiles qui combine la technologie VoIP avec une mise en œuvre standardisée de la 3GPP, offrant ainsi aux opérateurs de télécommunications la possibilité de proposer des services sur IP à haute valeur ajoutée. Grâce à cette nouvelle structure, il est possible de créer des sessions multimédias peu importe le type d'accès à Internet utilisé. Dans une même session, cette architecture est également en mesure de supporter des applications en temps réel comme la voix et la vidéo, ainsi que des applications non temps réel comme le Push to Talk et la messagerie instantanée. L'IMS offre une interface en mode circuit aux réseaux et propose une interface standardisée basée sur le protocole SIP (Standards IP) pour accéder aux services. [7]

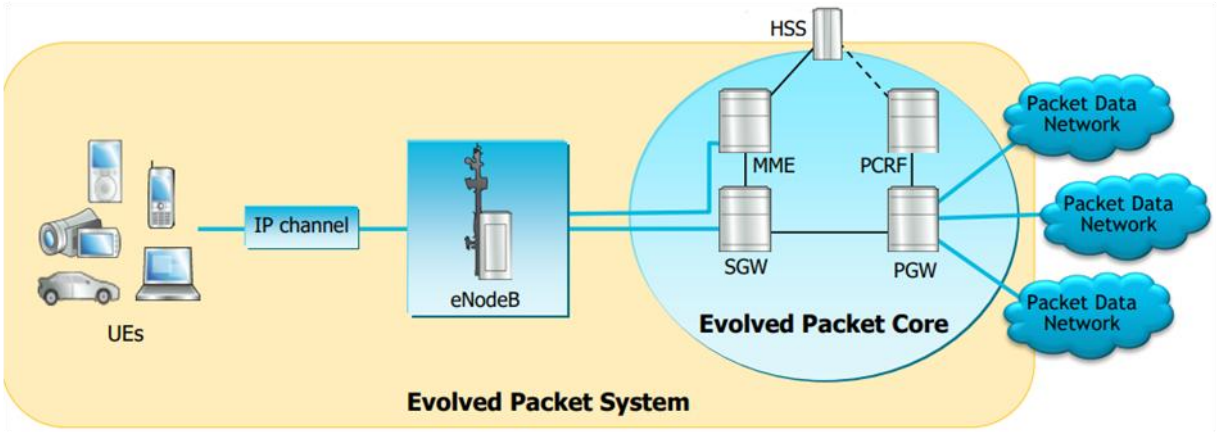

Figure 2.3 – Architecture de l'EPC. [1]

2.11 Conclusion

Dans ce chapitre, nous avons abordé de manière générale les différentes générations de téléphonie mobile, en commençant par la 1G jusqu'à la 5G. Nous avons également fourni un aperçu sur des composants et des caractéristiques essentielles des systèmes 4G/LTE. De plus, nous avons décrit les types de transmission et la structure des ressources de transmission utilisées dans cette technologie.

Chapitre 3

Généralités sur les protocoles de routage

3.1 Introduction

Dans ce chapitre, nous allons donner des généralités sur le réseau internet, et d'étudier les réseaux LAN et WAN. Ensuite, nous explorerons le modèle OSI en détaillant ses sept couches, le fonctionnement des réseaux IP, les principes d'adressage dans les réseaux IP, et enfin, nous examinerons les protocoles de routage IP.

3.2 Réseau Internet

Internet est le réseau le plus vaste au monde. Des millions d'utilisateurs sont connectés à travers le monde. Plusieurs sous-réseaux sont connectés sur un support physique de différentes capacités pour transporter les paquets de la source à la destination. Un réseau informatique est constitué d'un ensemble de moyens matériels et logiciels reliés les uns aux autres dans le but de transmettre des informations. Il est possible d'éloigner ou de les rapprocher. En fonction de la distance entre ces équipements, on peut identifier les réseaux suivants :

Le réseau local (LAN) à l'intérieur d'un bâtiment ou d'une superficie inférieure à 10 kilomètres carrés.

Le réseau métropolitain (MAN) est un réseau de transport urbain qui entoure une ville, comme par exemple le métro.

le réseau étendu (WAN) est un réseau qui a au moins la taille d'un pays et qui englobe souvent toute la planète. [4]

3.2.1 Le modèle Interconnexion de Systèmes Ouverts (Open System Interconnexion (OSI))

Le cadre conceptuel du modèle d'interconnexion de systèmes ouverts (OSI) établit la manière dont les systèmes réseau communiquent et envoient des données d'un émetteur à un destinataire. Le modèle est employé afin de définir chaque élément de la transmission de données afin de définir des règles et des normes pour les applications et l'infrastructure du réseau. Le modèle OSI comprend sept couches qui s'empilent de bas en haut de manière conceptuelle. Les figures 3.1 et 3.2 illustrent ces couches. [2]

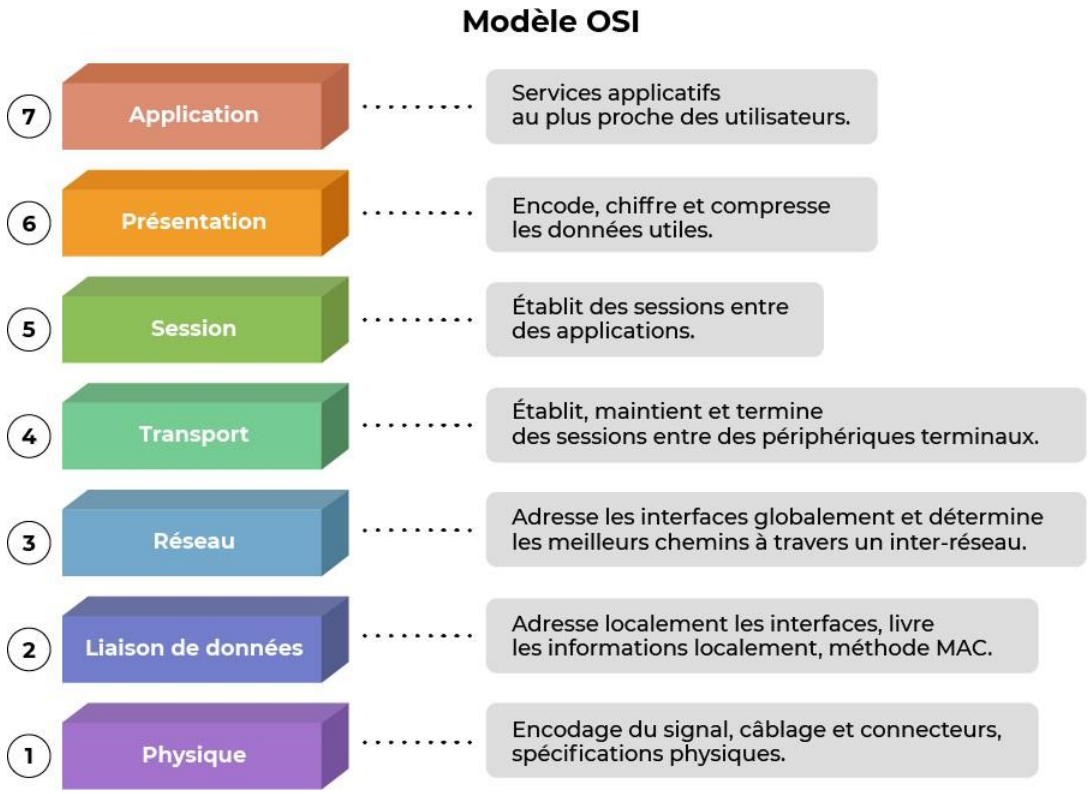

Figure 3.1 – Modèle OSI. [2]

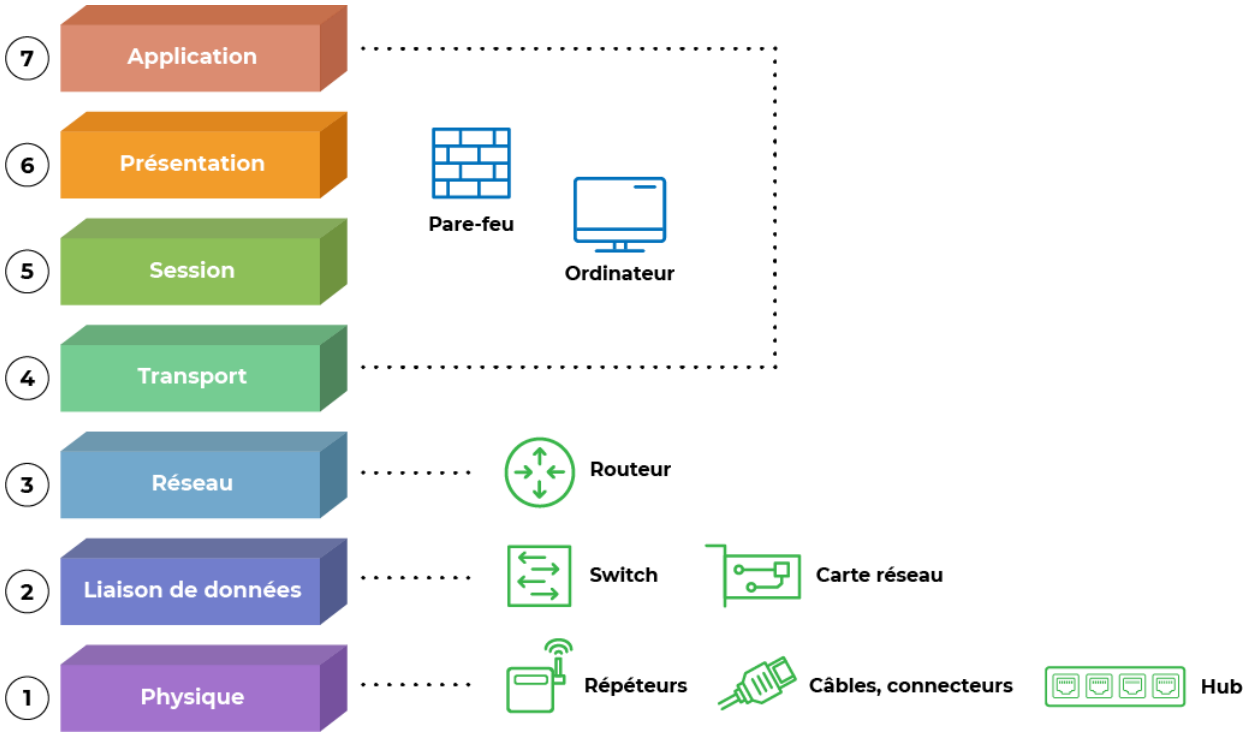

Figure 3.2 – Modèle OSI et les éléments du réseau associés. [2]

3.3 Le modèle Protocole de contrôle de transmission / Protocole Internet (TCP/IP)

Le modèle de transmission control protocol/Internet Protocol (TCP/IP), il s'agit d'un protocole ouvert qui ne dépend pas du support physique du réseau. TCP/IP peut être transmis par des supports et des technologies aussi variés qu'une ligne s'écrire, un câble coaxial Ethernet, une liaison louée, un réseau token-ring, une liaison radio (satellites, "Wireless" 802.11a/b/g), une liaison d'interface de données distribuée à fibres optiques (FDDI) 600Mbits, une liaison par rayon laser, infrarouge, xDSL, ATM, fibre optique, la liste des supports et des technologies n'est pas complète... [2]

3.4 Les couches du modèle TCP/IP

- La couche d'accès réseau ou couche de liaison est similaire aux couches de liaison.
- L'équivalent de la couche internet est la couche réseau du modèle OSI.
- La couche de transport correspond à la couche de transport du modèle OSI.
- La couche application regroupe les différentes couches du modèle OSI : session, présentation et application. [2]

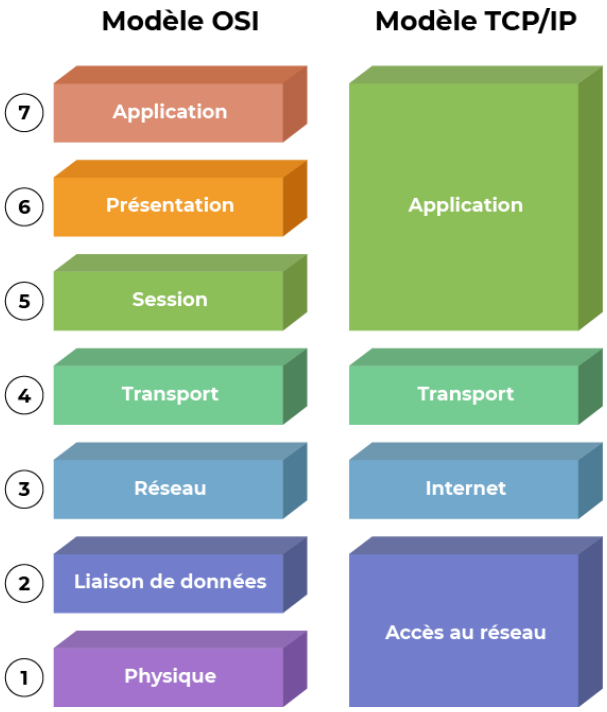

Figure 3.3 – Modèles OSI et TCP/IP. [2]

3.5 Le routage Internet Protocole (IP)

Le routage consiste à choisir des voies dans un réseau afin de transmettre des données (paquets) d'un routeur (réseau) à un autre en utilisant des adresses IP, depuis un expéditeur jusqu'à un ou plusieurs destinataires. Au début des réseaux, les tables de routage étaient fixes et donc mises à

jour manuellement. En raison de l'évolution et de l'expansion des réseaux, des protocoles de routage dynamiques échangent les informations de routage provenant d'autres systèmes du réseau pour mettre à jour les tables de routage. [2]

3.6 Les types de routage

La mise en place d'un protocole de routage peut être abordée à travers deux modes de routage distincts : le routage statique et le routage dynamique. [11]

3.6.1 Le routage statique

Le routage statique implique que l'administrateur réseau remplit manuellement les tables. On l'emploie sur de petits réseaux ou sur des réseaux d'extrémités. Les routes de chaque unité de routage du réseau doivent être gérées par l'administrateur, y compris les chemins statiques. Ils ne sont pas adaptés aux changements des environnements réseaux, les informations sont manuellement mises à jour à chaque changement topologique de l'inter-réseau. [11]

3.6.1.1 Connexion Directe

Une connexion directe fait référence à une situation où deux dispositifs réseau (comme des routeurs, des commutateurs, ou des ordinateurs) sont connectés l'un à l'autre sans passer par un intermédiaire ou un autre dispositif réseau. Les interfaces réseau de ces dispositifs partagent le même sous-réseau IP, permettant ainsi une communication directe. [11]

3.6.1.2 Route statique

Une route statique est une entrée dans une table de routage qui spécifie un chemin fixe et préconfiguré pour envoyer des paquets de données d'un réseau à un autre. Contrairement aux routes dynamiques, qui sont automatiquement apprises et ajustées par des protocoles de routage tels que OSPF ou BGP, les routes statiques doivent être manuellement configurées par un administrateur réseau. [11]

3.6.1.3 Route par Défaut

Une route par défaut est une configuration spéciale dans une table de routage utilisée pour diriger les paquets de données vers une passerelle (gateway) de dernier recours lorsqu'aucune autre route spécifique pour la destination du paquet n'existe dans la table. Elle est essentielle pour assurer que les paquets atteignent leur destination même si le chemin exact n'est pas connu à l'avance. [11]

3.6.2 Le routage dynamique

En utilisant cette méthode de routage, les tables sont complétées automatiquement. Un protocole est mis en place pour établir la topologie et compléter les tables de routage. Le routage dynamique offre aussi la possibilité de modifier automatiquement les tables de routage lorsque le lien sur un routeur est interrompu. Il offre aussi la possibilité de sélectionner la meilleure voie disponible pour passer d'un réseau à un autre. [11]

3.7 Les protocoles de routage

Il existe deux familles principales de protocoles de routage dans les réseaux IP : les protocoles de routage internes (IGP - Interior Gateway Protocol) et les protocoles de routage externes (EGP - Exterior Gateway Protocol). Le réseau Internet est divisé en systèmes autonomes, appelés AS (Autonomous System), ou en zones de responsabilité, qui sont un ensemble de routeurs et de réseaux reliés les uns aux autres, et qu'une même organisation gère. Dans un système autonome, on utilise un protocole de routage de type IGP. Pour les échanges de routage entre différents systèmes autonomes, un protocole de routage de type EGP est employé. Il peut arriver qu'un protocole de routage découvre plusieurs chemins menant à la même destination. Afin de choisir le meilleur chemin, il utilise une métrique qui évalue et différencie les chemins disponibles. Une métrique est un indicateur employé par les protocoles de routage afin d'influencer les frais d'accès aux réseaux distants. La métrique permet d'identifier le meilleur chemin en présence de plusieurs chemins vers le même réseau à distance. En fonction du protocole de routage employé, diverses mesures peuvent être prises lors d'une décision de routage, telles que le nombre de sauts, la bande passante, le délai, la fiabilité...etc [4]

3.7.1 Protocoles de routage internes (IGP)

Il existe plusieurs protocoles de routage internes spécifiques aux systèmes autonomes (AS) qui facilitent la communication entre les routeurs. Parmi ces protocoles, on peut distinguer : [2]

3.7.1.1 Protocole d'Information de Routage (RIP)

Le protocole d'information de routage (RIP) est un protocole de routage utilisé dans les réseaux informatiques. Il repose sur l'algorithme de routage décentralisé Bellman-Ford et utilise le nombre de sauts (hops) pour évaluer la distance entre les routeurs. Chaque routeur communique sa table de routage à ses voisins toute les 30 secondes. [2]

3.7.1.2 Protocole Système Intermédiaire à Système Intermédiaire (IS-IS)

Le protocole système intermédiaire à système intermédiaire (IS-IS), également connu sous le nom de protocole de routage à état de lien, est couramment employé dans les réseaux IP. Initialement conçu pour les réseaux à commutation de circuit, il a été modifié pour les réseaux à commutation de circuit. Les réseaux à transmission de paquets, en particulier les réseaux IP. Une des principales caractéristiques de l'IS-IS réside dans sa capacité à offrir une hiérarchie de routage efficace, en structurant les réseaux en niveaux et en domaines. Cela facilite la gestion optimale des réseaux de grande envergure en répartissant les données.

3.7.1.3 protocole Premier Chemin le Plus Court ouvert (OSPF)

Le protocole OSPF (Open Shortest Path First) a été utilisé afin de dépasser les contraintes du protocole RIP. Il offre plusieurs améliorations significatives, telles que la gestion de domaines de diamètre supérieur à 16, améliore le temps de convergence, utilise une métrique plus avancée qui prend en compte les débits, facilite l'agrégation des routes et permet de diviser le domaine en aires. Toutefois, OSPF présente également une complexité accrue, demandant des routeurs plus performants et une configuration moins simple que RIP. Dans OSPF, chaque routeur peut identifier ou identifier ses voisins en fonction de sa configuration. Dans le cas où un réseau comporte plusieurs routeurs, un routeur

principal et un routeur principal de secours sont choisis parmi eux. La base de données du routeur principal est obtenue par chaque routeur, qui renferme les données sur l'ensemble du réseau. Ensuite, chaque routeur diffuse des messages de type LSA (Link State Advertisement) à ses voisins, incluant la liste de ses voisins immédiats ainsi que le coût ou la métrique de la liaison vers chacun d'entre eux. Chaque routeur, en recevant ces messages, met à jour sa propre base de données, ce qui lui donne une vue d'ensemble du réseau. Ces données permettent à chaque routeur de déterminer les meilleures routes en se basant sur une métrique de coût minimum et en déduisant sa table de routage. Il est donc possible pour chaque routeur de sélectionner les routes les plus performantes pour le routage des paquets dans le réseau OSPF. [2]

3.7.1.4 le protocole de routage externe (EGP)

Le protocole de routage externe (EGP) était utilisé aux débuts d'Internet pour permettre aux routeurs de différents réseaux de partager des informations de routage, mais il a été largement remplacé par le Border Gateway Protocol (BGP) plus avancé et largement utilisé. Le BGP (Border Gateway Protocol) est le protocole standard employé sur Internet afin de faciliter les échanges entre les opérateurs. À la différence des protocoles de routage employés à l'intérieur des systèmes autonomes (IGP), comme OSPF, le BGP est spécifiquement conçu pour les interactions entre entités différentes et ne repose pas sur une prise de décision centralisée. Le BGP est employé par les opérateurs afin de partager des données de routage avec leurs collègues, fournisseurs ou clients. L'AS (Système Autonome) est l'unité de routage pour le BGP et représente une entité administrative indépendante avec ses propres politiques de routage. Les opérateurs peuvent établir des accords de transit ou de peering pour échanger du trafic, avec les fournisseurs de transit classés en fonction de leur envergure et de leur indépendance. Le BGP offre une flexibilité et une granularité plus importantes dans la gestion des politiques de routage par rapport aux protocoles IGP utilisés à l'intérieur des AS. [2]

3.7.1.5 Protocole de passerelle de frontière externe(EBGP)

L'abréviation eBGP désigne le protocole BGP externe, ce qui implique qu'il est employé pour créer des sessions BGP entre des routeurs appartenant à des AS différents. Les routeurs peuvent échanger des informations de routage entre leur propre AS et d'autres AS qu'ils ont acquises lors d'autres sessions EBGP grâce à EBGP. La mise en place de stratégies et de préférences de routage entre différents AS est également possible grâce à EBGP, comme la sélection du meilleur chemin, le filtrage des itinéraires ou l'utilisation de l'ingénierie du trafic. [4]

3.7.1.6 Protocole de passerelle de frontière interne(IBGP)

IBGP est la désignation abrégée de BGP interne, ce qui implique qu'il est employé pour créer des sessions BGP entre des routeurs du même système autonome(COMME). Un AS désigne un ensemble de réseaux qui ont la même politique de routage et la même conduite. IBGP permet aux routeurs d'un système d'exploitation d'échanger des données de routage avec des réseaux externes, comme Internet ou d'autres systèmes d'exploitation. IBGP offre également la possibilité de préserver la cohérence et d'éviter les boucles de routage à l'intérieur d'un AS. [4]

3.8 Protocole Internet / Commutation multiprotocole par étiquettes(IP/MPLS)

Les réseaux de télécommunications IP/MPLS utilisent le protocole IP pour le routage et MPLS (Multiprotocol Label Switching) pour la commutation de paquets. Grâce à cette technologie, il est possible de proposer des services de connexion complets, offrant une qualité de service (QoS) fiable, une sécurité améliorée et une évolutivité élevée.

3.8.1 Objectifs de MPLS

Transporter rapidement et efficacement les paquets de données à travers le réseau. Il est possible de gérer de grandes quantités de trafic et de proposer des solutions plus souples pour les réseaux de grande taille.
Proposer des options de sécurité comme la virtualisation des réseaux, la segmentation et la protection des données. [4]

3.8.2 Principe de fonctionnement de MPLS

Le Multiprotocol Label Switching (MPLS) est une méthode de transfert de données pour les réseaux télécoms à haute performance. En utilisant des étiquettes de chemin courtes plutôt que des adresses réseau longues, elle permet de rediriger les données d'un nœud de réseau à un autre, ce qui évite des recherches complexes dans une table de routage.
Le MPLS opère de manière très semblable aux méthodes de routage IP. En recevant un paquet de données entrant, un routeur classique ne fournit que l'adresse IP de destination, sans plus de détails sur les itinéraires ou la manière dont le réseau doit le transporter. Le MPLS utilise le protocole Internet de couche 3, c'est-à-dire le routeur, comme moyen de transfert. Le premier routeur, également appelé routeur Ingress, est utilisé pour débuter le processus de routage MPLS. Il insère une ou plusieurs étiquettes juste avant l'adresse IP du paquet de données, puis procède à son acheminement initial. Au lieu de se concentrer sur les données IP, les commutateurs de routage suivants se focalisent sur les informations contenues dans les étiquettes afin de transmettre le paquet vers sa destination. Finalement, le routeur Egress, qui est le dernier, enlève l'étiquette et envoie le paquet IP restant vers sa destination finale. Le MPLS présente également plusieurs bénéfices tels qu'une performance améliorée.

Le réseau offre une sécurité améliorée, une plus grande évolutivité et une meilleure qualité de service (QoS). Il joue également un rôle dans la réduction du coût des opérations et de la maintenance du réseau. [4]

3.8.3 Commutation multiprotocole par étiquettes/Protocole de distribution d'étiquettes (MPLS LDP)

LDP est un protocole utilisé dans les réseaux MPLS pour distribuer les labels. Il permet aux routeurs de communiquer entre eux et d'échanger les informations nécessaires pour associer les labels aux routes spécifiques. LDP facilite la configuration et la gestion des chemins de données dans un réseau MPLS. LDP fonctionne sur le modèle des protocoles de routage IP. Il utilise la table de routage générée par ces derniers pour construire les tables de commutation MPLS. Il offre différents modes de distribution et de conservation des labels, ce qui lui permet de s'adapter à différentes utilisations. Il gère en outre les traitements nécessaires à la compatibilité avec les commutateurs ATM (Asynchronous Transfert Mode). [2]

3.8.4 Réseau Privé Virtuel/Commutation multiprotocole par étiquettes (VPN MPLS)

La technologie MPLS (Multiprotocol Label Switching) est utilisée pour créer un réseau privé virtuel (VPN) appelé vpn mpls. Grâce à cette technologie, il est possible de créer des tunnels privés à travers un réseau public, ce qui offre aux entreprises une connexion privée et sûre. La création des VPN MPLS repose sur l'utilisation d'étiquettes pour repérer les chemins de routage préétablis dans le réseau. Les paquets de données sont enfermés dans ces tunnels et transportés à travers ces voies d'échange, assurant ainsi une sécurité accrue pour les informations sensibles. Ils offrent une grande souplesse, car ils peuvent être ajustés pour répondre aux besoins spécifiques de chaque société. Les entreprises font usage des VPN MPLS afin de relier des sites distants, des succursales ou des partenaires commerciaux. Ils peuvent aussi servir à offrir une connexion sécurisée aux travailleurs à distance ou aux utilisateurs mobiles. [2]

3.9 Le protocole Routage et Transfert Virtuels (VRF)

La technologie du VRF est employée dans les réseaux informatiques afin de générer des instances virtuelles de routage au sein d'un même routeur ou commutateur. Il a pour but de diviser et de séparer le trafic de divers clients ou applications au sein d'un réseau physique partagé. Lorsqu'un routeur ou un commutateur est configuré avec des VRF, il établit des tables de routage séparées pour chaque configuration. Chaque VRF dispose donc de sa propre table de routage distincte, comprenant ses propres entrées de routage et règles de transfert. Par conséquent, les VRF offrent la possibilité de concevoir des environnements de routage virtuels où différentes instances de routage coexistent et fonctionnent de manière autonome. Dans les réseaux d'entreprises ou de prestataires de services, les VRF sont fréquemment employés. [12]

3.9.1 Routage et Transfert Virtuelspour les adresse Réseau Privé Virtuel version 4 (VRF-adresse VPNv4)

Les adresses VPNv4 sont employées dans le domaine des VPN MPLS, en particulier pour les instances VRF. Les adresses VPNv4 servent à préciser les itinéraires clients dans un réseau MPLS de manière individuelle. Une adresse VPNv4 est un prolongement de l'adresse IPv4 classique. Il est composé d'un RD de 8 octets et d'une adresse IPv4 de 4 octets).
Le RD est employé afin de différencier les routes appartenant à différents clients qui pourraient autrement présenter des espaces d'adresses IP chevauchant. Le RD est ajouté à une adresse IPv4 déjà existante, ce qui crée une adresse VPNv4 distincte. Cela donne la possibilité au réseau MPLS de distinguer les adresses IP identiques de clients différents.
Quand une route est importée dans un VRF, son adresse IPv4 est transformée en adresse VPNv4 en la préfixant du RD attribué à ce protocole. La conversion permet au réseau MPLS de transmettre les itinéraires des clients à travers le réseau fédérateur du fournisseur de services tout en préservant la distinction entre le trafic des différents clients.
Conjointement avec le RD, le Route Target (RT) est un autre élément de communauté étendu employé dans les VPN. [13]

3.10 Sécurité du Protocole Internet (IPsec)

3.10.1 Définition IPsec

IPsec (Sécurité du Protocole Internet) est une série de règles ou de protocoles de communication qui permettent de créer des connexions sécurisées sur un réseau. La norme générale qui définit la manière dont les données circulent sur Internet est le protocole Internet (IP). IPsec intègre le chiffrement et l'authentification afin d'améliorer la sécurité du protocole. Par exemple, il enregistre les informations à leur origine et les décrypte à leur destination. Il confirme également la provenance des informations. [14]

3.10.2 L'importance de l'IPsec

IPsec a été créé dans les années 1990 par l'Internet Engineering Task Force afin d'assurer la confidentialité, l'intégrité et l'authenticité des données lors de l'utilisation des réseaux publics. Par exemple, les utilisateurs utilisent un VPN IPsec pour se connecter à Internet afin d'accéder à distance aux fichiers de l'entreprise. Le protocole IPsec enregistre les données confidentielles afin d'éviter les contrôles indésirables. Le serveur a aussi la possibilité de vérifier l'autorisation des paquets de données reçus. [15]

3.10.3 Les utilisations de l'IPsec

IPsec peut être employé pour les tâches ci-dessous : - Garantir la protection du routeur lors de l'envoi de données sur le réseau public d'Internet.
-Analyser les informations des applications.
-Si les données proviennent d'un expéditeur connu, il est important de les authentifier rapidement.
-Mettre en œuvre des circuits chiffrés, connus sous le nom de tunnels IPsec, afin de protéger les données du réseau, il est possible de chiffrer toutes les données envoyées entre deux points de terminaison.
Les entreprises font appel à IPSec afin de se prémunir contre les attaques de relecture. Une attaque de type man-in-the-middle, également appelée attaque par relecture, vise à intercepter et à modifier une transmission en cours en transférant les données vers un ordinateur intermédiaire. Le protocole IPSec donne à chaque paquet de données un numéro séquentiel et procède à des vérifications afin de repérer les signes de paquets en double.
[15]

3.10.4 Chiffrement IPsec

Le cryptage IPsec est un logiciel qui crypte les données pour préserver leur contenu vis-à-vis des personnes non autorisées. Une clé de chiffrement est utilisée pour protéger les données, tandis qu'une clé de déchiffrement est requise pour les déchiffrer. Différents types de chiffrement sont supportés par IPsec, tels que AES, Blowfish, Triple DES, ChaCha et DES-CBC.
IPsec met en place des méthodes de chiffrement asymétrique et symétrique afin de garantir la vitesse et la sécurité du transfert des données. La clé de chiffrement est publique dans le cadre du chiffrement asymétrique, tandis que la clé de déchiffrement reste privée. Le chiffrement symétrique fait appel à la même clé publique pour protéger et décrypter les données. IPsec met en place une connexion sécurisée en utilisant un chiffrement asymétrique, puis il passe au chiffrement symétrique afin de ralentir le

transfert des données.
[15]

3.10.5 Fonctionnement de l'IPsec

Les ordinateurs communiquent avec le protocole IPsec en respectant les étapes suivantes.
1- Selon la politique de sécurité de l'ordinateur expéditeur, il est nécessaire de vérifier si la transmission de données nécessite une protection IPsec. Lorsque cela se produit, l'ordinateur commence une transmission sécurisée IPSec avec l'ordinateur destinataire.
2-Les deux ordinateurs discutent des exigences nécessaires pour créer une connexion sécurisée. Cette approche implique un consensus mutuel concernant les paramètres de cryptage et d'authentification, ainsi que d'autres associations de sécurité (AS).
3-L'ordinateur transmet et reçoit les informations chiffrées, confirmant ainsi qu'elles sont issues de sources fiables. Son rôle est de vérifier le contenu sous-jacent afin de garantir sa fiabilité.
4-Une fois la transmission terminée ou la session expirée, l'ordinateur met un terme à la transmission.
[14]

3.10.6 Les protocoles de l'IPsec

Les protocoles IPsec assurent l'envoi sécurisé des paquets de données. Un paquet de données est une structure particulière qui organise et prépare les données afin de les transposer sur le réseau de communication. L'en-tête, la charge utile et la bande de fin constituent son composant.
-L'en-tête est une partie antérieure qui renferme des instructions pour orienter le paquet de données vers la destination appropriée.
-La charge utile désigne les informations authentiques présentes dans un ensemble de données.
-La bande de fin est une information additionnelle qui est ajoutée à la queue de la charge afin de marquer la fin du paquet de données.
Certains protocoles IPsec sont présentés ci-dessous.
En-tête d'authentification (AH) :
Le protocole d'en-tête d'authentification (AH) intègre un en-tête qui renferme les informations d'authentification de l'expéditeur et bloque toute modification du contenu du paquet par des personnes non autorisées. Il prévient le destinataire des manipulations éventuelles du paquet de données initial. Quand l'ordinateur reçoit le paquet de données, il compare le calcul du hachage cryptographique de la charge utile avec l'en-tête afin de vérifier que les deux valeurs sont identiques. Une fonction mathématique appelée hachage cryptographique permet de résumer les données en une seule valeur.
Encapsulation de la charge utile de sécurité (ESP) :
En fonction du mode IPsec choisi, le protocole ESP crypte l'ensemble du paquet IP ou seulement la charge utile. Lors du chiffrement, ESP intègre un en-tête et une bande de fin au paquet de données.
IKE(Internet Key Exchange) :
Le protocole de l'Internet Key Exchange (IKE) permet de créer une connexion sécurisée entre deux dispositifs en ligne. L'association de sécurité (SA) entre les deux appareils consiste à négocier des clés et des algorithmes de chiffrement afin de transmettre et recevoir les paquets de données suivants. [14] [15]

3.11 Conclusion

Dans ce chapitre, nous avons exploré les principes fondamentaux des réseaux informatiques, en examinant comment les protocoles de communication sont classés en fonction de leurs caractéristiques et de leur niveau d'opération. Pour cela, nous avons utilisé deux modèles représentatifs : les modèles OSI et TCP/IP. Ensuite, nous avons étudié en détail le fonctionnement du protocole IP et du processus de routage, en abordant notamment le routage interne et externe. De plus, nous avons analysé le fonctionnement des protocoles OSPF, VRF, MPLS, IGW, BGP(I-BGPIS, E-BGP) et IPsec.

Chapitre 4

Réalisation d'un réseau privé IPsec

4.1 Introduction

Dans ce chapitre, nous allons expliquer le but de cette étude, et de montrer les résultats de l'implémentation des protocoles MPLS et BGP dans le réseau IPSEC. Ce chapitre consiste à valider notre projet, en inférant les différentes configurations qu'il est important d'implémenter sur notre architecture, basée sur l'émulateur eNSP. Pour cela, nous présentons les configurations que nous avons réalisées, nous avons utilisé des captures d'écran montrant les étapes de configuration nécessaires et les tests que nous avons effectués.

4.2 Solution

Afin de satisfaire les exigences croissantes en matière de qualité de service et d'optimisation des ressources, Djezzy a décidé d'opter pour deux scénarios.Notre projet consiste a étudié les technologies du routage IP au sein du réseau DJEZZY d'une façon générale et d'une façon détaille le Protocol de routage OSPF, VRF, MPLS, IGW, BGP(I-BGPIS, E-BGP) et IPsec. Dans ce projet on a utilisé deux couches ; les deux couches sont : la couche liaison et la couche réseaux. La couche liaison de données : qui reçoit les données brutes de la couche physique, elle les organise en trames, et détecte les erreurs. La couche réseau (IP) : assure également un service de traduction des adresses logiques (adresse IP) en adresses physiques (adresse MAC). Dans cette couche on a étudié les adresse IP et le routage IP. Le but de notre projet est de sécuriser notre réseau .

4.2.1 Le premier scénario

Ce scénario est basé sur, la partie "access" du réseau, qui représente la connexion entre les utilisateurs finaux et le réseau principal, est concernée. Nous avons l'intention de remplacer l'infrastructure d'accès fournie par Djezzy par celle fournie par Algérie Télécom.

Pour ce faire, les EnodeB, qui sont des stations de base utilisées dans les réseaux de téléphonie mobile, établissent une connexion avec un ONT (Optical Network Terminal) via le réseau d'Algérie Télécom. Cette connexion se fait au niveau de la couche 2 du modèle OSI, ce qui signifie que les données sont échangées au niveau de liaison de données.

Une fois cette connexion établie, l'ONT est connecté à un OLT (Optical Line Terminal), qui est un équipement de réseau utilisé pour agréger les connexions des utilisateurs finaux. À partir de l'OLT, la connexion entre directement dans le réseau ASG (Agrégation Djezzy), qui est le réseau principal de

Djezzy.

En résumé, cette configuration permet d'utiliser l'infrastructure d'accès fournie par Algérie Télécom pour acheminer le trafic des utilisateurs finaux vers le réseau principal de Djezzy, en remplaçant la partie "access" précédemment fournie par Djezzy.

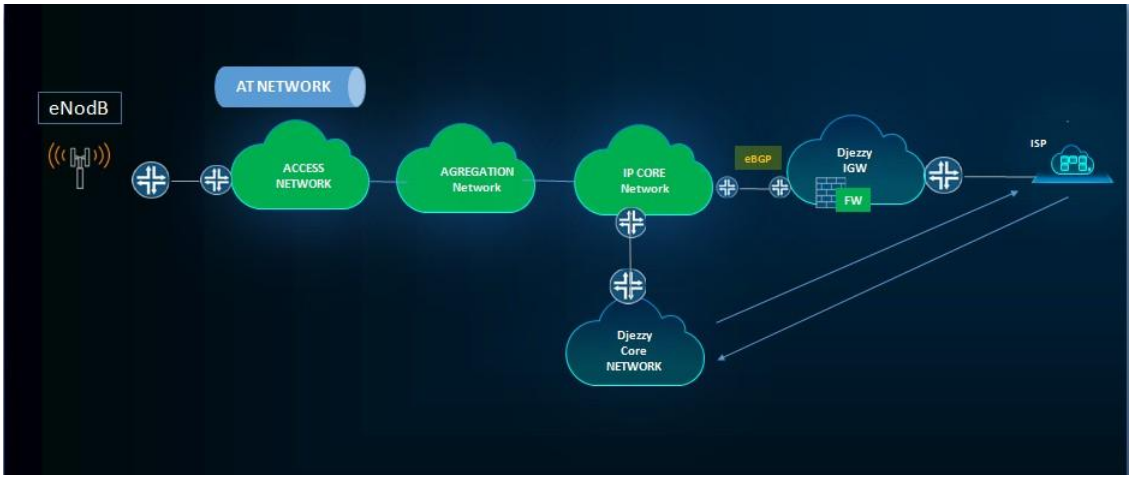

Figure 4.1 – le premier scénario.

4.2.2 Le deuxième scénario

Dans le cadre de l'intégration des réseaux de télécommunications d'Algérie Télécom et de Djezzy, plusieurs mesures sont mises en place pour assurer la sécurité et l'efficacité des transmissions de données. Une solution clé est l'implémentation du protocole IPsec (Internet Protocol Security) pour sécuriser les connexions entre les équipements des deux réseaux. Voici les détails spécifiques de l'ajout d'IPsec entre les routeurs, ainsi que le flux de données à travers les réseaux :

- **Ajout d'IPsec entre un routeur installé avec l'eNodeB de Djezzy et un routeur ou firewall dans la couche EGW de Djezzy**

IPsec est déployé entre un routeur connecté à l'eNodeB de Djezzy et un autre routeur ou firewall situé dans la couche EGW (Evolved Gateway) de DJEZZY. Cette mesure assure une connexion sécurisée en chiffrant les données échangées, garantissant ainsi la confidentialité et l'intégrité des informations transmises.

- **Flux de Données à travers les réseaux**

1.Couche d'accès : Les données entrent dans le réseau d'Algérie Telecom via la couche d'accès.

2.RMS et EGW d'Algérie Telecom : Les données passent ensuite par le RMS (Réseau de Multiplexage de Signaux) et l'EGW d'Algérie Telecom, où elles sont traitées et acheminées vers leur destination respective.

3.Internet : Les données sortent vers Internet, traversant les infrastructures d'Algérie Telecom de manière sécurisée grâce à IPsec.

4.DJEZZY : Les données entrent dans le réseau Djezzy via l'EGW, mais elles restent cryptées avec IPsec pour assurer la sécurité pendant le transit.

- **Avantages de l'utilisation d'IPsec**

1. Utilisation de l'Internet normal : Permet l'utilisation de l'Internet public, évitant ainsi des coûts supplémentaires et économisant de l'argent.

2.Sécurité renforcée : IPsec chiffre les données, assurant leur protection lorsqu'elles traversent des ré-

seaux externes non sécurisés.

- **Retour des données vers Algérie Telecom**

1. Connexion OLT : Les données de retour de Djezzy se connectent à l'OLT (Optical Line Terminal) d'Algérie Telecom.
2. Réseau d'agrégation : L'OLT intègre ensuite les données dans le réseau d'agrégation d'Algérie Telecom pour leur traitement ultérieur.

- **Équipements dans le réseau d'Algérie Telecom**

1. Modem : Utilisé pour l'accès initial au réseau, le modem fait partie des équipements d'accès d'Algérie Telecom.
2. OLT et Fibre Optique : L'OLT reçoit le signal fibre optique du modem et le transmet au réseau d'agrégation pour une connectivité plus large.

En résumé, ce processus garantit une transmission sécurisée des données grâce à IPsec tout en optimisant l'utilisation des infrastructures existantes d'Algérie Telecom et de DJEZZY. Cela permet une intégration économique et efficace des réseaux, assurant la sécurité et la fluidité des communications entre les deux opérateurs.

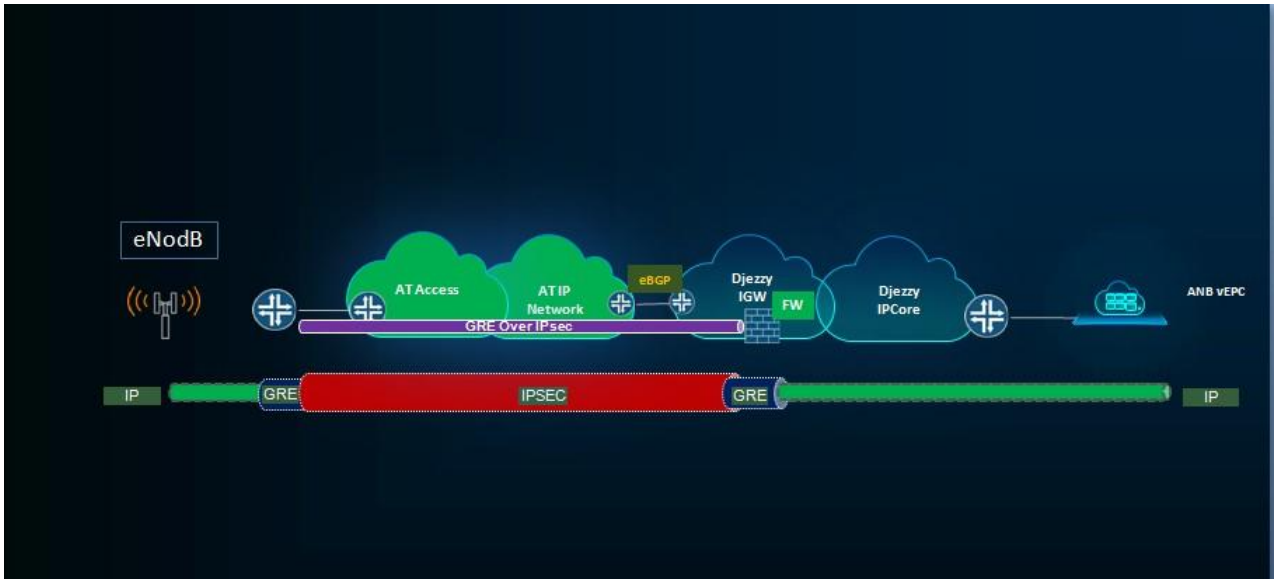

Figure 4.2 – Le deuxième scénario.

4.3 eNSP

La plate-forme de simulation de réseau d'entreprise de Huawei - ou eNSP est un outil graphique gratuit prenant en charge la simulation de réseau à grande échelle. Il simule avec précision le déploiement et les performances des pare-feu, des commutateurs réseau, des routeurs et des périphériques WLAN dans votre réseau tel que construit ou dans un réseau virtuel lorsque aucun périphérique est disponible. [16]

4.4 Réalisation du réseau

Dans cette partie, nous allons présenter le réseau utilisé et ses différentes configurations :

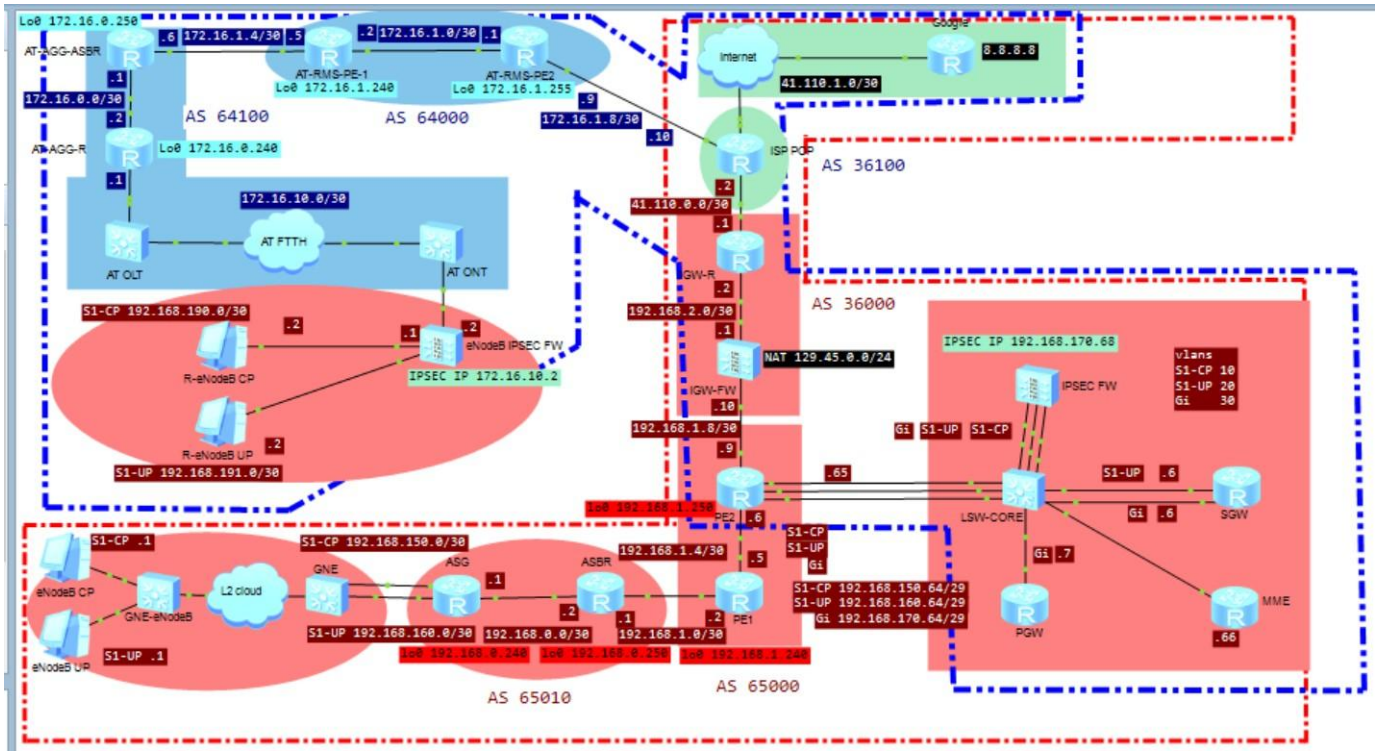

Figure 4.3 – Topologie du réseau simulé.

4.4.1 Présentation du réseau

Nous avons utilisé des routeurs, des switchs, des PCs et des firewalls dont :

PARTIE 1 (le premier scénario)

1. Le réseau d'accès de DJEEZY :

   Simulant 2 PCS pour une seu le eNodeB un pour le CP et l'autre pour UP 2 switchs représentant le GNE de l'eNodeB

2. Le réseau d'agrégation de DJEEZY :

   simulant les routeurs ASG et ASBR .

3. le réseau de l'IP CORE de DJEEZY :

   2 (routeurs PE : provided edge) : PE1 et PE2.

4. Le réseau CORE de DJEEZY :

   simulant les routeurs : SGW, PGW et MME.

   un switch : LSW-CORE.

   un firwall : IPSEC FW.

5. Le réseau de la getway Internet :

   Un firwall : IGW-FW

   Un routeur : IGW-R

6. Le réseau INTERNET :

   2 routeurs : ISP POP et GOOGLE

PARTIE 2 (Le deuxième scénario)

1. Le réseau d'accès de Djezzy :

   Simulant 2 PCS pour une seule eNodeB un pour le CP et l'autre pour UP

   Un firwall : IPsec eNodeB

   2 switchs : AT ONT et AT OLT.
2. Le réseau d'agrégation de Djezzy :

   simulant les routeurs AT-AGG-R et AT-AGG-ASBR .
3. le réseau de l'IP CORE de DJEEZY :

   2 (routeurs PE : provided edge) : AT-RMS-PE1 et AT-RMS-PE2
4. Le réseau CORE de DJEEZY :

   et simulant les routeurs : SGW, PGW et MME.

   un switch : LSW-CORE.

   un firwall : IPSEC FW.
5. Le réseau de la getway Internet :

   Un firwall : IGW-FW.

   Un routeur : IGW-R.
6. Le réseau INTERNET :

   2 routeurs : ISP POP et GOOGLE.

4.4.2 Configuration du réseau

Les différentes étapes de la configuration du réseau seront montrées dans cette section :

Table d'adressage La configuration des adresses IP attribuées aux interfaces de chaque routeur est illustrée dans le tableau suivant :

Equipemente	Interface	Adresse IP	Adresse Loopback0
ASG	G0/0/0 G0/0/1 G0/0/2	192.168.0.1/30 192.168.150.2/30 192.168.160.2/30	192.168.0.240/32
ASBR	G0/0/0 G0/0/3	192.168.0.2/30 192.168.1.1/30	192.168.0.250/32
PE1	G0/0/0 G0/0/3	192.168.1.5/30 192.168.1.2/30	192.168.1.240/32
PE2	Eth0/0/0 G0/0/0 G0/0/1 G0/0/2 G0/0/3	192.168.1.9/30 192.168.1.6/30 192.168.150.65/29 192.168.160.65/29 192.168.170.65/29	192.168.1.250/32
ASG	G0/0/0 G0/0/1 G0/0/2	192.168.0.1/30 192.168.150.2/30 192.168.160.2/30	192.168.0.240/32
SGW	G0/0/0 G0/0/1	192.168.160.66/29 192.168.170.66/29	/
PGW	G0/0/0	192.168.170.67/29	/
MME	G0/0/0	192.168.150.66/29	/
IGW-R	G0/0/0 G0/0/1	192.168.2.2/30 41.110.0.2/30	/
ISP POP	Eth0/0/0 G0/0/0 G0/0/1	41.110.1.2/30 172.16.1.10/30 41.110.0.1/30	/
AT-AGG-R	G0/0/0 G0/0/1	172.16.0.2/30 172.16.10.1/30	172.16.0.240/32
AT-AGG-ASBR	G0/0/0 G0/0/3	172.16.0.1/30 172.16.1.6/30	172.16.0.250/32

AT-RMS-PE1	G0/0/0 G0/0/3	172.16.1.2/30 172.16.1.5/30	172.16.1.240/32
AT-RMS-PE2	G0/0/0 G0/0/1	172.16.1.9/30 172.16.1.255/32	172.16.1.240/32
EnodeB IP-SEC FW	G0/0/0 G1/0/0 G1/0/1 G1/0/2	192.168.0.1/24 172.16.10.2/30 192.168.190.1/30 192.168.191.1/30	/
IPSEC IP FW	G0/0/0 G1/0/4 G1/0/5 G1/0/6	192.168.0.1/24 192.168.150.68/29 192.168.160.68/29 192.168.170.68/29	/
Google	Eth0/0/0	41.110.1.1/30	8.8.8.8/32
IGW-FW	G0/0/0 G1/0/0 G1/0/1	192.168.0.1/24 192.168.2.1/30 192.168.1.10/30	/

Table 4.1 – Table d'adressage des interfaces des routeurs du réseau.

4.4.2.1 Configuration des différents routeurs

Cette partie consiste à effectuer une configuration initiale sur les routeurs primaires (réseau) en suivant les étapes mentionnées ci-dessous :

. Configuration de l'adressage.
. Configuration des interfaces .
. Configuration de routage. IGP (le protocole OSPF) .
. Configuration du protocole MPLS .
. Configuration du BGP (IBGP /EBGP) .
. Les VRF et IPSEC.

4.4.2.2 Intégration des routeurs

Nous sélectionnons des routeurs pour les configurer et les intégrer dans la partie centrale de L'ENSP comme le montre la figure suivante :
pour les configurer et les intégrer dans la partie centrale de L'ENSP comme le montre la figure suivante :

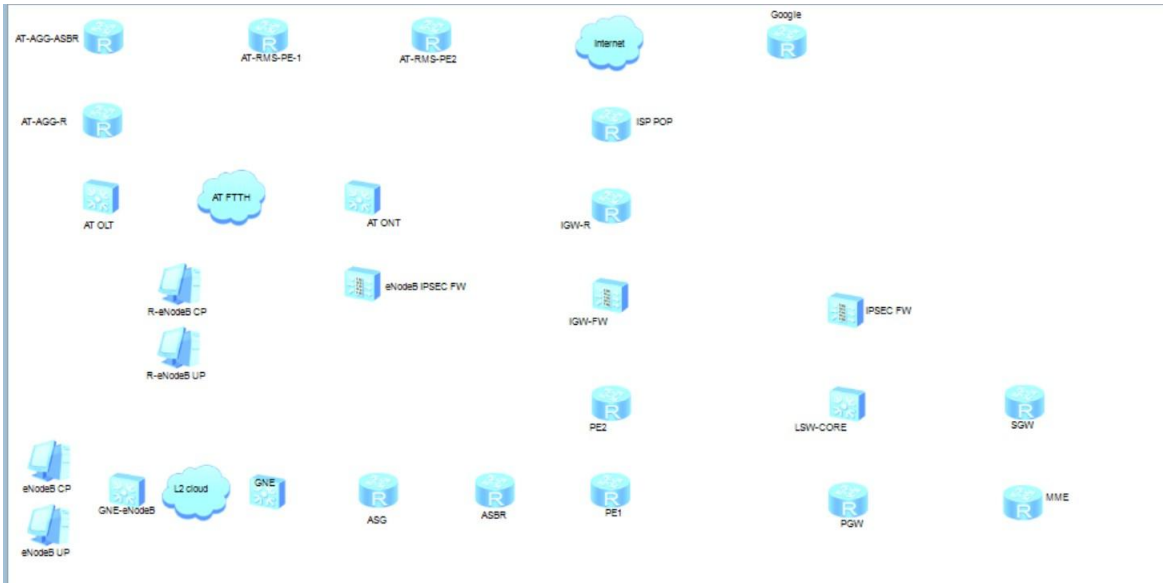

Figure 4.4 – Intégration des routeurs.

4.4.2.3 Interconnexion des routeurs

On connecte les routeurs aux câbles, et quand la plateforme est prête, on active la topologie avec l'icône sur la barre de menu en haut. Est montrée sur la figure ci-dessous :

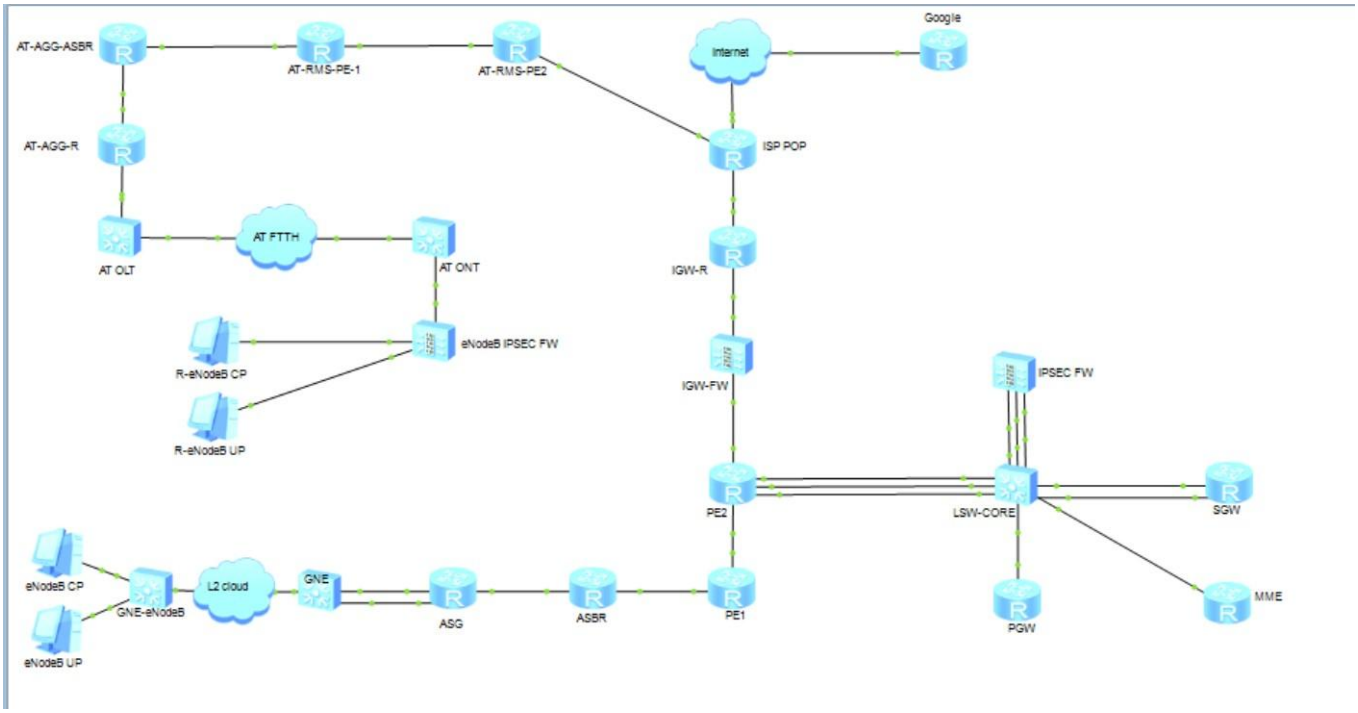

Figure 4.5 – Liaison des routeurs.

4.4.2.4 Configuration des interfaces loopbacks

Interface loopback : est une interface virtuelle, cette interface est perçue comme une interface physique, pour activée cette interface en utilisée cette commande **« interface loopback n° »**, en suit utilisant la commande **« Ip Address »**.
Comme le montre la figure ci-dessus et on configure les routeurs ASBR, PE1 ,PE2, AT AGG R, AT AGG ASBR, AT RMS PE1 et AT RMS PE2 de la même manière :

```
<ASG>
<ASG>sys
<ASG>system-view
Enter system view, return user view with Ctrl+Z.
[ASG]interface loopback 0
[ASG-LoopBack0]ip add
[ASG-LoopBack0]ip address  192.168.0.240 32
```

Figure 4.6 – Configuration loopbacks.

4.4.2.5 Configuration de l'adressage

pour les interfaces nous configurons chaque interface par la commande **« interface Ethernet X/Y/Z »** ou bien avec **« interface GigabitEthernet X/Y/Z »**. Nous attribuons une IP à chaque interface, en utilisant la commande **« ip address »**, ensuite on les active avec la commande **« UNDO shutdown »**.
Comme le montre la figure ci-dessous cette étape est primordiale pour tous les routeurs switches pcs et firewalls :

```
<ASG>
<ASG>SYS
Enter system view, return user view with Ctrl+Z.
[ASG]INT G0/0/0
[ASG-GigabitEthernet0/0/0]IP ADD 192.168.0.1 30
```

Figure 4.7 – Configuration des interfaces.

L'étape de la vérification des interfaces qu'on a activées avec la commande **« dis ip int brief »** dans le consol est montré sur la figure ci-dessous :

```
[ASG]
[ASG]display ip interface brief
*down: administratively down
!down: FIB overload down
^down: standby
(l): loopback
(s): spoofing
(d): Dampening Suppressed
The number of interface that is UP in Physical is 2
The number of interface that is DOWN in Physical is 10
The number of interface that is UP in Protocol is 2
The number of interface that is DOWN in Protocol is 10

Interface                         IP Address/Mask      Physical   Protocol
Ethernet0/0/0                     unassigned           down       down
Ethernet0/0/1                     unassigned           down       down
GigabitEthernet0/0/0              192.168.0.1/30       down       down
GigabitEthernet0/0/1              192.168.150.2/30     down       down
GigabitEthernet0/0/2              192.168.160.2/30     down       down
GigabitEthernet0/0/3              unassigned           down       down
LoopBack0                         192.168.0.240/32     up         up(s)
NULL0                             unassigned           up         up(s)
Serial0/0/0                       unassigned           down       down
Serial0/0/1                       unassigned           down       down
Serial0/0/2                       unassigned           down       down
Serial0/0/3                       unassigned           down       down
[ASG]
```

Figure 4.8 – Vérification des interfaces activées après configuration.

4.4.2.6 Configuration du protocole OSPF

Est un protocole servant à déterminer le meilleur chemin que peuvent emprunter des paquets pour transiter par une série de réseaux connectés, L'utilité d'OSPF pour établir session OSPF plus rapide de RIP et utilise les loopback pour un réseau plus stable en se trouver dans la table publique. Nous configurons OSPF sur les routeurs du réseau MPLS comme suit :

- **« OSPF X »** : pour déclencher le processus ospf, la lettre X représente l'identifiant du routeur.
- **« Area »** : pour spécifier la zone participante au processus ospf.
- **« Network »** : pour déclarer et spécifier le réseau participant au processus ospf.
- **« Quit »** : pour sortir du mode configuration.

Est montrée sur la figure ci-dessous :

```
[ASG]
[ASG]
[ASG]ospf 100
[ASG-ospf-100] area 0.0.0.0
[ASG-ospf-100-area-0.0.0.0]  network 192.168.0.0 0.0.0.3
[ASG-ospf-100-area-0.0.0.0]  network 192.168.0.240 0.0.0.0
[ASG-ospf-100-area-0.0.0.0]
May 29 2024 02:21:42-08:00 ASG DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 3, the c
hange loop count is 0, and the maximum number of records is 4095.
[ASG-ospf-100-area-0.0.0.0]
```

Figure 4.9 – Configuration OSPF.

On configure l'OSPF dans les networks chaque network possède un ospf unique : « ASG-ASBR » « PE1-PE2 » « IGW-FW-IGW-R » « AT AGG R -AT AGG ASBR » « AT RMS PE1 - AT RMS PE2». Après la configuration, en teste l'activation de protocole OSPF avec la commande **« display current-configuration OSPF »** qui nous montre la table de routage. Est montrée sur la figure ci-dessous :

```
<ASG>
<ASG>
<ASG>dis c c ospf
#
ospf 100
 area 0.0.0.0
  network 192.168.0.0 0.0.0.3
  network 192.168.0.240 0.0.0.0
#
return
```

Figure 4.10 – Vérification de l'activation OSPF.

4.4.2.7 Création OSPF pour une VRF

La configuration se fait dans le routeur PE2 pour le routeur IGW **« ospf 300 vpn Gi area 0.0.0.0 network 192.168.1.8 0.0.0.3 import direct »**

4.4.2.8 Configuration de MPLS

Est une technologie conçue pour améliore la vitesse et l'efficacité du transfert des données, on utilise le MPLS pour offre une meilleur rapidité de commutation des paquets, en effet la décision de routage se fait en analysant un label insérée par le protocole MPLS. Ainsi chaque routeur posséde une table associant un port / label d'entrée à un port / label de sortie.
La configuration de MPLS sur chaque routeur se fait en 3 étapes :

- en activant MPLS sur les Routeurs.
- en activant MPLS sur les interfaces qu'on veut participer au domaine MPLS.
- on active Le protocole LDP.

La configuration est la même pour les routeurs restants. Nous devrons donc faire les commandes suivantes sur chaque routeur.

- « interface » : pour l'activation d'MPLS sur l'interface .
- « mpls lsr-id X.X.X.X» : pour l'activation d'MPLS sur le routeur.
- « mpls » : pour l'activation d'MPLS .
- « mpls ldp » : pour l'activation d'MPLS ldp sur l'interface.

Sur la figure ci-dessous, nous montrons la configuration de MPLS :

```
<ASG>
<ASG>sys
<ASG>system-view
Enter system view, return user view with Ctrl+Z.
[ASG]interface LoopBack0
[ASG-LoopBack0]ip address 192.168.0.240 255.255.255.255
Error: The address already exists.
[ASG-LoopBack0]
[ASG-LoopBack0]
[ASG-LoopBack0]mpls lsr-id 192.168.0.240
Warning: Can't configure lsr-id when MPLS is enabled.
[ASG]mpls
[ASG-mpls]#
[ASG-mpls]mpls ldp
[ASG-mpls-ldp]#
[ASG-mpls-ldp]
```

Figure 4.11 – Configuration de MPLS.

On met la commande **« display mpls interfaces »** afin de voir les interfaces activées et la commande **« display mpls ldp »** afin de voir les informations sur le status, ID du routeur comme indiqué dans le document suivant :

```
<PE1>sys
Enter system view, return user view with Ctrl+Z.
[PE1]display mpls ldp

                         LDP Global Information
 ------------------------------------------------------------------------------
 Protocol Version        : V1            Neighbor Liveness     : 600 Sec
 Graceful Restart        : Off           FT Reconnect Timer    : 300 Sec
 MTU Signalling          : On            Recovery Timer        : 300 Sec
 Capability-Announcement : Off           Longest-match         : Off

                        LDP Instance Information
 ------------------------------------------------------------------------------
 Instance ID             : 0             VPN-Instance          :
 Instance Status         : Active        LSR ID                : 192.168.1.240
 Loop Detection          : Off           Path Vector Limit     : 32
 Label Distribution Mode : Ordered       Label Retention Mode  : Liberal
 Instance Deleting State : No            Instance Reseting State : No
 Graceful-Delete         : Off           Graceful-Delete Timer : 5 Sec
 ------------------------------------------------------------------------------

[PE1]dis mpls int
Interface             Status    TE Attr   LSP Count  CRLSP Count Effective MTU
GE0/0/0               Up        Dis       2          0           1500
GE0/0/3               Up        Dis       0          0           1500
[PE1]
```

Figure 4.12 – Vérification de l'activation MPLS..

Dans la figure, nous voyons l'activation des MPLS via l'interface G0/0/0 et l'interface GE0/0/3.
Les configurations sont fait sur les routeurs suivants : « ASG, ASBR, PE1, PE2, AT AGG R, AT AGG ASBR, AT RMS PE1 et AT RMS PE2 ».

4.4.2.9 Configuration des vrfs CP et UP

Dans le routeur PE2

- « ip vpn-instance CP » donne le nom a la vrf.

« ipv4-family » créé la vrf.
« route-distinguisher 192.168.1.250 :1 » préciser le routeur id de la vrf.
« apply-label per-instance » donne un label a la vrf.
« vpn-target 100 :100 export-extcommunity » cette commande exporte la vrf.
« vpn-target 100 :100 import-extcommunity » importe la vrf.

- « ip vpn-instance UP » donne le nom a la vrf.

« ipv4-family » crée la vrf.
« route-distinguisher 192.168.1.250 :2 » préciser le routeur id de la vrf.
« apply-label per-instance » applique un label pour qu'il puisse l'importer et l'exporter sur mpls.
« vpn-target 200 :200 export-extcommunity ».
« vpn-target 200 :200 import-extcommunity ».

- « ip vpn-instance Gi » donne le nom a la vrf.

« ipv4-family »crée la vrf.
« route-distinguisher 192.168.1.250 :3 » préciser le routeur id de la vrf.
« apply-label per-instance » applique un label pour qu'il puisse l'importer et l'exporter sur mpls.
« vpn-target 300 :300 export-extcommunity » exporte la vrf.

- « vpn-target 300 :300 import-extcommunity »importe la vrf.

```
[PE2]
[PE2]ip vpn-instance CP
[PE2-vpn-instance-CP]ipv4-family
[PE2-vpn-instance-CP-af-ipv4]route-distinguisher 192.168.1.250:1
[PE2-vpn-instance-CP-af-ipv4]apply-label per-instance
[PE2-vpn-instance-CP-af-ipv4]vpn-target 100:100 export-extcommunity
 EVT Assignment result:
Info: VPN-Target assignment is successful.
[PE2-vpn-instance-CP-af-ipv4]vpn-target 100:100 import-extcommunity
 IVT Assignment result:
Info: VPN-Target assignment is successful.
[PE2-vpn-instance-CP-af-ipv4]
[PE2-vpn-instance-CP-af-ipv4]ip vpn-instance UP
[PE2-vpn-instance-UP]ipv4-family
[PE2-vpn-instance-UP-af-ipv4]route-distinguisher 192.168.1.250:2
[PE2-vpn-instance-UP-af-ipv4]apply-label per-instance
[PE2-vpn-instance-UP-af-ipv4]vpn-target 200:200 export-extcommunity
 EVT Assignment result:
Info: VPN-Target assignment is successful.
[PE2-vpn-instance-UP-af-ipv4]vpn-target 200:200 import-extcommunity
 IVT Assignment result:
Info: VPN-Target assignment is successful.
[PE2-vpn-instance-UP-af-ipv4]
[PE2-vpn-instance-UP-af-ipv4]ip vpn-instance Gi
[PE2-vpn-instance-Gi]ipv4-family
[PE2-vpn-instance-Gi-af-ipv4]route-distinguisher 192.168.1.250:3
[PE2-vpn-instance-Gi-af-ipv4]apply-label per-instance
[PE2-vpn-instance-Gi-af-ipv4]vpn-target 300:300 export-extcommunity
 EVT Assignment result:
Info: VPN-Target assignment is successful.
[PE2-vpn-instance-Gi-af-ipv4]vpn-target 300:300 import-extcommunity
 IVT Assignment result:
Info: VPN-Target assignment is successful.
[PE2-vpn-instance-Gi-af-ipv4]
```

Figure 4.13 – Configuration VRF.

Pour configurer le réseau Internet gateway

• « interface ethernet0/0/0
ip binding vpn-instance Gi
ip address 192.168.1.9 255.255.255.252 » on crée une adresse ip a la vrf Gi via une interface physique eth0/0/0.

• « ospf 300 vpn Gi
area 0.0.0.0
network 192.168.1.8 0.0.0.3
import direct » on a créé un ospf pour la vrf Gi.

Pour configurer la réseau core de djezzy

• « interface GigabitEthernet0/0/1
ip binding vpn-instance CP
ip address 192.168.150.65 255.255.255.248 » on crée une adresse ip a la vrf CP via une interface physique

• « interface GigabitEthernet0/0/2
ip binding vpn-instance UP
ip address 192.168.160.65 255.255.255.248 » on crée une adresse ip a la vrf UP via une interface physique

• « interface GigabitEthernet0/0/3
ip binding vpn-instance Gi
ip address 192.168.170.65 255.255.255.248 » on crée une adresse a la vrf Gi via une interface physique.

4.4.2.10 configuration des routes statique

Dans le routeur PE2

« ip route-static vpn-instance UP 8.8.8.8 255.255.255.255 192.168.160.66 » on a crée une route static qui dit Que quand la vrf UP veut aller a Google 8 .8.8.8 le traffic passe a SGW 192.168.160.66.
« ip route-static vpn-instance Gi 192.168.160.1 255.255.255.255 192.168.170.67 » on dit au routeur PE2 Quand la vrf Gi veut aller au 192.168.160.1 ASG le traffic doit passer par PGW.

Dans le Firewall IGW

« ip route-static 129.45.0.0 255.255.255.0 NULL0 » créer un blackhaul pour le subnet 129.45.0.0.
« ip route-static 192.168.170.68 255.255.255.255 192.168.1.9 » on a crée une route static qui incite a passer le traffic du FW IPSEC a travers PE2 192.168.1.9.
« ip route-static 192.168.160.1 255.255.255.255 192.168.1.9 » on a créer une route static qui incite a passer le traffic de l'EnodeB UP a travers PE2 192.168.1.9.

```
[IGW-FW]
[IGW-FW]ip route-static 129.45.0.0 255.255.255.0 NULL0
Error: The route already exists.
[IGW-FW]ip route-static 192.168.170.68 255.255.255.255 192.168.1.9
Error: The route already exists.
[IGW-FW]ip route-static 192.168.160.1 255.255.255.255 192.168.1.9
Error: The route already exists.
[IGW-FW]dis ip rou
[IGW-FW]dis ip routing-table s
[IGW-FW]dis ip routing-table statistics
2024-06-06 21:34:12.220
Summary Prefixes : 11
Proto     total      active     added      deleted    freed
          routes     routes     routes     routes     routes
DIRECT    6          6          6          0          0
STATIC    4          4          4          0          0
RIP       0          0          0          0          0
OSPF      1          1          1          0          0
IS-IS     0          0          0          0          0
BGP       0          0          0          0          0
UNR       0          0          0          0          0
Total     11         11         11         0          0
[IGW-FW]
```

Figure 4.14 – configuration des routes statique.

4.4.2.11 Configuration du BGP

Nous commençons par attribuer le même numéro d'AS à chaque routeur appartenant à la même zone en utilisant la commande :

« bgp X » le x représente un nombre d'AS au choix.

Nous avons choisi des numéros d'AS public : 65000 65010 36000 36100 64100 64000. Ensuite, nous configurons le BGP interne (I-BGP) entre « ASG et ASBR » « PE1 et PE2 » « AT AGG R et AT AGG ASBR » « AT RMS PE1 et AT RMS PE2 » en utilisant les commandes :

Exemple on fait le peer entre le routeur ASG et ASBR :

« bgp 65010
peer 192.168.0.250 as-number 65010
peer 192.168.0.250 connect-interface LoopBack0 »

```
<ASG>
<ASG>sys
Enter system view, return user view with Ctrl+Z.
[ASG]bgp 65010
[ASG-bgp] peer 192.168.0.250 as-number 65010
Error: The peer already exists in AS 65010.
[ASG-bgp] peer 192.168.0.250 connect-interface LoopBack0
[ASG-bgp]
[ASG-bgp]
```

Figure 4.15 – Configuration BGP interne(I-BGP).

Ensuite, nous configurons le BGP externe (E-BGP) entre « PE1 et ASBR » « IGW R et ISP POP» « AT RMS PE1 et AT AGG ASBR » « ISP POP et AT RMS PE2 » en utilisant les commandes :

EXEMPLE on fait le peer entre le routeur PE1 et ASBR :
« bgp 65010
peer 192.168.1.2 as-number 65000 »

```
<ASBR>
<ASBR>sys
Enter system view, return user view with Ctrl+Z.
[ASBR]bgp 65010
[ASBR-bgp]peer 192.168.1.2 as-number 65000
Error: The peer already exists in AS 65000.
[ASBR-bgp]
[ASBR-bgp]
```

Figure 4.16 – Configuration BGP externe(E-BGP).

On continue les configurations de la table public du bgp et les vrf dans les routeurs « ASG » « ASBR » « PE1 » « PE2 » « AT AGG R » « AT AGG ASBR » « AT RMS PE1 » « AT RMS PE2 » « IGW-R » « ISP POP ».
« ipv4-family unicast » pour la configuration dans la table public.
« undo synchronization » cette commande a pour but de synchronizer la table.
« network 192.168.1.250 255.255.255.255 » de préciser notre address du réseau.
« peer 192.168.1.240 enable » pour activer le peer avec l'adresse 192.168.1.240.
« peer 192.168.1.240 label-route-capability » pour tracer la route.

Pour configurer la vrf dans les routeurs « ASG » « ASBR » « PE1 » « PE2 » :
« ipv4-family vpnv4
policy vpn-target
peer 192.168.1.240 enable » pour activer la vrf sur cette adresse ip.

« ipv4-family vpn-instance CP
import-route direct » indique s'il se trouve une vrf CP il l'import avec une route directe.

« ipv4-family vpn-instance UP
import-route direct
import-route static » » indique s'il se trouve une vrf CP il l'import avec une route static et direct.
voici une capture des configurations précédentes dans le routeur PE2 :

```
<PE2>sys
Enter system view, return user view with Ctrl+Z.
[PE2]bgp 65000
[PE2-bgp] peer 192.168.1.240 as-number 65000
Error: The peer already exists in AS 65000.
[PE2-bgp] peer 192.168.1.240 connect-interface LoopBack0
[PE2-bgp] #
[PE2-bgp] ipv4-family unicast
[PE2-bgp-af-ipv4]  undo synchronization
[PE2-bgp-af-ipv4]  network 192.168.1.250 255.255.255.255
[PE2-bgp-af-ipv4]  peer 192.168.1.240 enable
[PE2-bgp-af-ipv4]  peer 192.168.1.240 label-route-capability
[PE2-bgp-af-ipv4] #
[PE2-bgp-af-ipv4] ipv4-family vpnv4
[PE2-bgp-af-vpnv4]  policy vpn-target
[PE2-bgp-af-vpnv4]  peer 192.168.1.240 enable
[PE2-bgp-af-vpnv4] #
[PE2-bgp-af-vpnv4] ipv4-family vpn-instance CP
[PE2-bgp-CP]  import-route direct
Error: The policy already exists.
[PE2-bgp-CP] #
[PE2-bgp-CP] ipv4-family vpn-instance UP
[PE2-bgp-UP]  import-route direct
Error: The policy already exists.
[PE2-bgp-UP]  import-route static
Error: The policy already exists.
[PE2-bgp-UP]
```

Figure 4.17 – Configuration BGP-VRF.

4.4.2.12 IPsec configurations

Ses principales forces résident dans sa capacité à :

• Authentification : IPsec utilise des mécanismes d'authentification renforcés pour garantir que les données proviennent de sources fiables, empêchant ainsi les attaques par usurpation d'identité.

• Confidentialité : Grâce au chiffrement, IPsec assure que les données transmises restent confidentielles, empêchant ainsi les interceptions et les accès non autorisés.

• Intégrité des Données : IPsec protège l'intégrité des données en utilisant des mécanismes de contrôle qui détectent toute altération non autorisée des données en transit.

• Flexibilité : Compatible avec de nombreux protocoles, IPsec peut être déployé dans diverses configurations réseau, y compris les VPN, les communications entre routeurs et les communications hôte-à-hôte.

Cependant, IPsec présente quelques inconvénients. Sa configuration et sa gestion peuvent être complexes, surtout dans les environnements de grande envergure. De plus, le chiffrement et le déchiffrement des données peuvent introduire une latence et une surcharge de traitement.
Voici les configurations du Firewall IPec IP 192.168.170.68 ci-dessous :

« « acl number 3000 »
« rule 5 permit ip source 192.168.150.66 0 destination 192.168.190.2 0 »flux du CP
« rule 10 permit ip source 8.8.8.8 0 destination 192.168.191.2 0 » flux du UP » .

« ipsec proposal 1
esp authentication-algorithm sha1
esp encryption-algorithm 3des » la negociation des blocs de l'IPsec.

« ike proposal 1
encryption-algorithm 3des
dh group1
authentication-algorithm sha1
authentication-method pre-share
integrity-algorithm hmac-sha1-96
prf hmac-sha1 » les informations nécessaires qui sont partager en toute sécurité entre les deux firwall pour que le tunnel ipsec s'active , on va l'appeler une langue specifique entre les deux firewalls .

« ike peer 1 » les informations du peer entre les firewalls .
« pre-shared-key Pfe@2024 » la clé partager exemple Pfe@2024.
« ike-proposal 1 » la langue spécifique entre eux .
« remote-id 172.16.10.2 » le firewall destiné.
« local-id 192.168.170.68 »le firewall source .
« remote-address 172.16.10.2 » .

« ipsec policy IPsec 1 isakmp
security acl 3000
ike-peer 1
proposal 1 » on crée une policy d'IPsec avec les informations suivantes ACL ike-peer et ike proposal.

« interface GigabitEthernet1/0/6
ipsec policy IPsec » on configure l'installation de la policy de l'IPsec dans l'interface G1/0/6 et on applique les configurations précédentes dans le FW IPsec.

```
<IPSEC FW>sys
Enter system view, return user view with Ctrl+Z.
[IPSEC FW]acl number 3000
[IPSEC FW-acl-adv-3000]rule 5 permit ip source 192.168.150.66 0 destination 192.
168.190.2 0
  Warning: The rule already exists. Are you sure to update? [Y/N]:n
[IPSEC FW-acl-adv-3000]
[IPSEC FW-acl-adv-3000]ipsec proposal 1
[IPSEC FW-ipsec-proposal-1]esp authentication-algorithm sha1
Warning: The security level of md5/sha1 is low.
[IPSEC FW-ipsec-proposal-1]esp encryption-algorithm 3des
Warning: The security level of des/3des this algorithm is low.
[IPSEC FW-ipsec-proposal-1]
[IPSEC FW-ipsec-proposal-1]ike proposal 1
[IPSEC FW-ike-proposal-1]encryption-algorithm 3des
 Warning: The security level of des/3des is low.
[IPSEC FW-ike-proposal-1]dh group1
Warning: The security level of group1/group2/group5 is low.
[IPSEC FW-ike-proposal-1]authentication-algorithm sha1
Warning: The security level of md5/sha1 is low.
[IPSEC FW-ike-proposal-1]authentication-method pre-share
[IPSEC FW-ike-proposal-1]integrity-algorithm hmac-sha1-96
Warning: The security level of md5/sha1 is low.
[IPSEC FW-ike-proposal-1]prf hmac-sha1
Warning: The security level of md5/sha1 is low.
[IPSEC FW-ike-proposal-1]
[IPSEC FW-ike-proposal-1]ike peer 1
[IPSEC FW-ike-peer-1]pre-shared-key Pfe@2024
[IPSEC FW-ike-peer-1]ike-proposal 1
[IPSEC FW-ike-peer-1]remote-id 172.16.10.2
[IPSEC FW-ike-peer-1]local-id 192.168.170.68
[IPSEC FW-ike-peer-1]remote-address 172.16.10.2
[IPSEC FW-ike-peer-1]
[IPSEC FW-ike-peer-1]
[IPSEC FW-ike-peer-1]ipsec policy IPSEC 1 isakmp
Info: The ISAKMP policy sequence number should be smaller than the template poli
cy sequence number in the policy group. Otherwise, the ISAKMP policy does not ta
ke effect.
[IPSEC FW-ipsec-policy-isakmp-IPSEC-1]security acl 3000
[IPSEC FW-ipsec-policy-isakmp-IPSEC-1]ike-peer 1
[IPSEC FW-ipsec-policy-isakmp-IPSEC-1]proposal 1
```

Figure 4.18 – Configuration IPsec FW.

4.4.2.13 Configuration pour le FW IGW

« firewall zone trust
add interface GigabitEthernet1/0/1 » on determine l'interface ou le firewall laisse passer le traffic.

« firewall zone untrust
add interface GigabitEthernet1/0/0 » le firwall block tout le traffic qui passe de cette interface.

« nat address-group NAT 1
mode pat
section 1 129.45.0.1 129.45.0.254 » la configue du nat .

« nat-policy
rule name NAT
source-zone trust

destination-zone untrust
action source-nat address-group NAT
source-address 192.168.160.1 mask 255.255.255.255 » la policy du nat le traffic qui vient de l'EnodeB UP se Nat pour sortir a Internet .

```
[IGW-FW]
[IGW-FW]
[IGW-FW]firewall zone trust
[IGW-FW-zone-trust]add interface GigabitEthernet1/0/1
 Error: The interface has been added to trust security zone.
[IGW-FW-zone-trust]#
[IGW-FW-zone-trust]firewall zone untrust
[IGW-FW-zone-untrust]add interface GigabitEthernet1/0/0
 Error: The interface has been added to untrust security zone.
[IGW-FW-zone-untrust]
[IGW-FW-zone-untrust]
[IGW-FW-zone-untrust]
[IGW-FW-zone-untrust]
[IGW-FW-zone-untrust]
[IGW-FW-zone-untrust]
[IGW-FW-zone-untrust]
[IGW-FW-zone-untrust]nat address-group NAT 1
[IGW-FW-address-group-NAT]mode pat
[IGW-FW-address-group-NAT]section 1 129.45.0.1 129.45.0.254
Error: The section ID is existing.

[IGW-FW-address-group-NAT]
[IGW-FW-address-group-NAT]
[IGW-FW-address-group-NAT]nat-policy
[IGW-FW-policy-nat]rule name NAT
[IGW-FW-policy-nat-rule-NAT]source-zone trust
[IGW-FW-policy-nat-rule-NAT]destination-zone untrust
[IGW-FW-policy-nat-rule-NAT]action source-nat address-group NAT
[IGW-FW-policy-nat-rule-NAT]source-address 192.168.160.1 mask 255.255.255.255
[IGW-FW-policy-nat-rule-NAT]
[IGW-FW-policy-nat-rule-NAT]
```

Figure 4.19 – Configuration NAT IGW.

4.4.2.14 Tester le tunnel IPsec s'il est activé

Pour cela on utilise la commande ping pour voir si les packets passent et qu'il n'y a pas de perte.

```
PC>PING 8.8.8.8

Ping 8.8.8.8: 32 data bytes, Press Ctrl_C to break
From 8.8.8.8: bytes=32 seq=1 ttl=248 time=468 ms
From 8.8.8.8: bytes=32 seq=2 ttl=248 time=469 ms
From 8.8.8.8: bytes=32 seq=3 ttl=248 time=484 ms
From 8.8.8.8: bytes=32 seq=4 ttl=248 time=375 ms
From 8.8.8.8: bytes=32 seq=5 ttl=248 time=454 ms

--- 8.8.8.8 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 375/450/484 ms
```

Figure 4.20 – Ping UP.

Exemple : On applique cette commande au PC R-EnodeB UP et R-EnodeB CP :

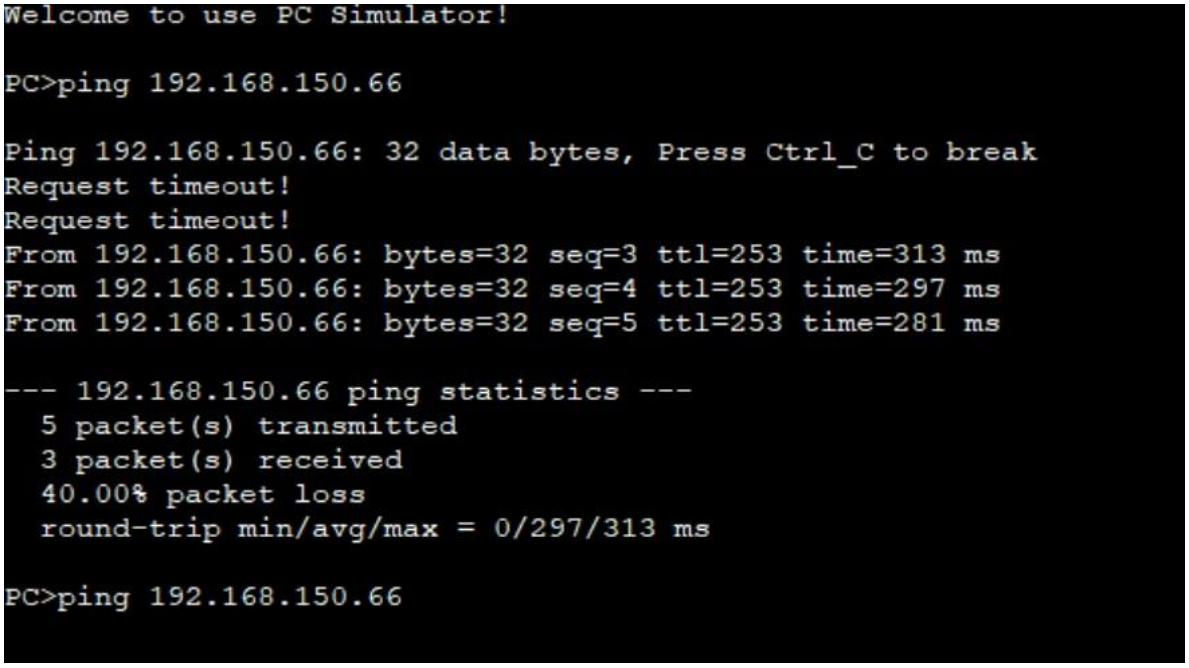

Figure 4.21 – Ping GCP.

4.5 Conclusion

En résumé, le troisième scénario de l'IPsec se révèle être une solution robuste et polyvalente pour sécuriser les communications réseau. Il contribue à améliorer le routage du trafic, à optimiser les capacités du réseau et ne nécessite pas de coûts supplémentaires en termes de matériel. Au contraire, cette solution a un impact financier positif sur Djezzy.
C'est un investissement judicieux pour réduire les dépenses inutiles.

Conclusion Générale

Le développement technologique a augmenté la capacité et la fonctionnalité des réseaux. IPSEC est devenu une solution phare qui facilite l'intégration des technologies existantes dans le réseau fédérateur, permettant à l'administrateur de gérer entièrement le réseau.

Une étude biographique des concepts de base est faite dans le premier et le deuxième chapitre, ce qui nous a permis de fournir une description des équipements de base du réseau mobile, des différents protocoles de routage, et des concepts de la technologie IP/MPLS, VRF et IPSEC, ce qui a aidé à comprendre et étudier le réseau privé IPSEC .

Le dernier chapitre a été consacré à la mise en œuvre de ce réseau en configurant et en activant les protocoles OSPF, IBGP, protocoles de routage internes et externes, sur les interfaces de routeur respectives, puis en passant à la configuration de VRF sur le routeur de périphérie.

A la fin de notre projet, pour assurer la connexion externe des routeurs, EBGP a été configuré sous l'autorité du protocole BGP. Ensuite, nous avons configuré notre tunnel IPSEC sur les deux firwalls au niveau de Djezzy et l'autre d'Algérie Télécom pour créer notre réseau privé. Nous avons testé le trafic entre les clients d'un site source ver un site distant. Nous avons conclu que le trafic est correctement propagé. Nous avons amélioré notre réseau privé IPSEC avec l'utilisation de nouvelles technologies du réseau, qui a permis également d'offrir des débits élevés en situation de mobilité et à garantir une mobilité totale à l'utilisateur en assurant l'interopérabilité entre diverses technologies existantes, ainsi qu'améliorer la protection du réseau tout en réalisant des économies, en proposant une opération répondant aux demandes croissantes de qualité de service.

Enfin, nous pouvons dire que la technologie IP SEC est parfaite pour le système du réeseau Djezzy, nous pouvons même passer prochainement à la cinquième génération avec un débit élevé offert par cette solution, mais ce n'est pas une solution idéale pour les autres services de Djezzy, nous pouvons ouvrir de nouvelles voies de recherche, soit de proposer un autre protocole pouvant le remplacer, ou bien de configurer IPSEC avec une autre application et améliorer la qualité de service (QoS).

Bibliographie

[1] SAIDI Sofiane . Organisme d'accueil DJEZZY, 2023/2024.

[2] Sami CHERFI et Mohamed Abderrahmane BOURENANE . Intégration et application de la technologie segment routing dans un réseau atm basé sur ip/mpls. *Université M'HAMED BOUGARA de BOUMERDES*, 2022/2023.

[3] https://www.djezzy.dz/djezzy/nous-connaitre/a-propos-de-djezzy.

[4] NASRI Rafika. Etude et intégration du protocole mpls dans le réseau core network au niveau de l'opérateur djezzy. *Université de boumerdes*, 2022/2023.

[5] https://forum.videotron.com/t5/blogue/de-la-1g-a-la-5g-la-petite-histoire-des-reseaux-mobil ba-p/43207.

[6] https://www.memoireonline.com/10/17/10061/m_Etudes-des-performances-des-reseaux-4G18.html.

[7] DJABOURABI Ines et MOKHTARI Asma. Mise en place d'un réseau 4g (lte) sécurisé. *Université Badji Mokhtar Annaba*, 2019/2020.

[8] https ://developer.orange.com/od-uploads/Generalites-et-architecture-de-la-4G.pdf.

[9] https://blogs.univ-poitiers.fr/f-launay/2012/04/24/pourquoi-la-4g-utilise-lofdma/#:~:text=La%20technique%20nomm%C3%A9e%20OFDMA%20est,partie%20de%20la%20famille%20OFDMA.,.

[10] Hocine Dounia et Missoum Abderzak . Analyse et optimisation du réseau d'accès radio 4g lte. *Université SAAD DAHLAB de BLIDA*, 2019/2020.

[11] https ://community.cisco.com/t5/networking-knowledge-base/dynamic-routing-protocols-ospf-eigrp-ripv2-is-is-bgp/ta-p/4511577.

[12] https ://www.cbtnuggets.com/blog/technology/networking/what-is-cisco-vrf-virtual-routing-forwarding.

[13] https ://support.huawei.com/enterprise/en/doc/EDOC1100171957.

[14] https ://networklessons.com/cisco/ccie-routing-switching/ipsec-internet-protocol-security.

[15] https ://aws.amazon.com/fr/what-is/ipsec/ : :text=IPSec

[16] https ://forum.huawei.com/enterprise/fr/forums/667480998545338368.

[17] https://blogs.univ-poitiers.fr/f-launay/2012/04/24/pourquoi-la-4g-utilise-lofdma/#:~:text=La%20technique%20nomm%C3%A9e%20OFDMA%20est,partie%20de%20la%20famille%20OFDMA.,.