République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mouloud-Mammeri
de Tizi Ouzou

FACULTE DU GENIE ELECTRIQUE ET D'INFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de Fin d'Etudes
De MASTER ACADEMIQUE

Domaine : Science et Technologies
Filière : Génie électrique
Spécialité : Télécommunication et Réseaux

Présenté par :
DERRIDJ Kaci Anis
GHERRAS Noureddine

Thème

Conception et développement d'un outil de Dimensionnement de réseau Packet Core Virtualisé dédié pour la 4G et 5G

	Président
M. AIT BACHIR,	*UMMTO Encadreur*
M. RIAHI Mustapha et M.CHERFI Saïd,	*Co-encadreur (ERICSSON)*
	Examinateur
	Examinateur
	Examinateur

Date de soutenance : /07/2016

Remerciements

On tient à exprimer nos sincères remerciements à tous ceux qui ont contribué de près ou de loin à la réalisation de ce mémoire et au bon déroulement de ce stage de fin d'études.

On remercie le bon **Dieu** de nous avoir guidés dans le droit chemin et de nous avoir donné le courage de mener à terme ce projet.

A Monsieur ***Cherfi Saïd***, pour nous avoir permis de réaliser ce stage au sein de l'entreprise ERICSSON Algérie. Lui qui nous a accueilli chaleureusement et accordé sa confiance lors de l'entretien, et nous avoir tout de suite mis à l'aise.

A Monsieur ***Riahi Mustapha,*** notre encadreur au sein d'ERICSSON, pour sa disponibilité et ses précieux conseils tout au long du stage, qui ont grandement contribué à la qualité du travail accomplie.

A Monsieur ***Aït Bachir Youcef*** notre promoteur-encadreur, pour ces conseils avisés, sa disponibilité tout au long de notre travail.

Et un grand merci à nos **PARENTS**, eux qui nous ont toujours soutenus et sont toujours présent, prêts à faire tout les sacrifices pour nous satisfaire. Ainsi qu'à toute la famille et nos amis.

Table des matières

Table des figures

Introduction générale :

Le monde des réseaux et des télécommunications mobiles connait une évolution très rapide. Cette évolution s'accompagne toujours par une nouvelle technologie et plus de complexité pour subvenir à une forte recrudescence des demandes de clients en termes de débit et de disponibilité des services proposés. Pour répondre à cette grande sollicitation des réseaux, les opérateurs télécom cherchent des solutions pour augmenter la capacité et la couverture tout en maintenant le KPI (Key Performance Indicator) souhaité.

Les opérateurs souhaitent déployer leurs réseaux et introduire de nouveaux et divers services plus rapidement et à moindre cout. Pour cela, ils doivent avoir des environnements de travail flexibles. C'est ici qu'intervient la virtualisation des fonctions réseaux (qu'on va étudier en détail par la suite) en permettant aux fournisseurs de services la possibilité d'évoluer plus rapidement et plus aisément au sein des nouvelles infrastructures telles que le LTE (Long Term Evolution). Elle permet aussi d'automatiser et de donner une certaine intelligence au réseau et d'utiliser plus efficacement les ressources pour accroitre ou diminuer les services. La virtualisation va apporter un plus en ce qui concerne la réduction des couts et les délais de commercialisation des services réseaux.

Les architectures des réseaux de télécommunications mobiles sont constituées de trois domaines essentiels, à savoir le domaine qui comprend les équipements propre à l'utilisateur, à savoir les terminaux, le domaine du réseau d'accès qui permet à l'abonné d'accéder aux ressources radio, et contribue à la gestion de sa mobilité, et enfin le domaine du réseau cœur qui regroupe l'ensemble des équipements assurant des fonctions telles que l'enregistrement de l'abonné au réseau et la mise à jour de sa localisation etc. Dans ce projet de fin d'études nous allons nous focaliser sur le domaine réseaux cœur, plus précisément le réseau cœur paquet EPC (Evolved Packet Core) de la quatrième génération de réseau mobile, et faire le lien entre la virtualisation et l'EPC pour la conception d'un vEPC (réseau cœur paquet virtualisé), considéré comme un bloc fonctionnel essentiel des réseaux de 5ème génération.

Ce projet se veut pertinent en ce qui concerne les nouvelles approches et technologies des réseaux de mobile, ceci détaillé en quatre chapitres qui forme ce rapport. Dans le premier chapitre, nous allons revoir brièvement les quatre générations de réseaux mobiles et mettre l'accent sur les évolutions opérées et puis présenter les perspectives pour la cinquième génération. Dans le second chapitre nous allons présenter l'IoT (Internet of Things) et la relation entre celle-ci et la téléphonie mobile. Puis on va étudier en détails le réseau cœur EPC du réseau mobile 4G et les différents composants. Lors du troisième chapitre nous allons introduire une nouvelle technique utilisée de plus en plus dans les réseaux, qui est la virtualisation. Le dernier chapitre (chapitre 4) est dédié à la présentation de notre application qui est un outil de dimensionnement d'un réseau cœur virtualisé vEPC.

1 L'évolution des réseaux de télécommunication mobiles

1.1 Introduction :

Au fil des années la téléphonie mobile a connu un réel essor. En effet la communication entre utilisateurs mobiles se développe et représente un marché immense en ce début du XXI^{e} siècle.

Quatre générations se sont succédées, se distinguant chacune d'entre elles par la nature de la communication transitant dans le réseau : avec tout d'abord une communication analogique, ensuite une communication numérique sous forme circuit, puis troisième avec, en plus de la voix numérique, des applications sous forme paquet, Enfin la quatrième que nous vivons actuellement et qui propose beaucoup plus de débits et d'applications que la précédente.

A ces quatre générations s'ajoute une cinquième en cours de recherches et de développements et prévu pour 2020 offrant encore plus de débits (de l'ordre de plusieurs Gbps par utilisateurs) et concrétisant la notion de société connectée.

Dans ce chapitre on va étudier brièvement et se familiariser avec ces différentes technologies en prenant comme exemple les systèmes et standards NMT, GSM, GPRS, UMTS, LTE et en fin la 5G.

1.2 Le NMT (Nordic Mobile Telephone):

C'est un système analogique de communications mobiles. Le système est développé en Suède, au Danemark, en Norvège et en Finlande. La première version, le NMT-450 était introduit en 1981, Le système a été utilisé par plusieurs pays, la plupart en Europe. Le NMT fonctionne à 450 MHZ sur la bande (450-470 MHZ). Ensuite la seconde version, NMT-900, a été introduite en 1986 Cette version fonctionne sur une fréquence de 900 MHZ, qui est utilisée en ce moment pour le GSM. [2]

Cette première génération ne propose aucun service autre que la voix, elle repose sur une communication analogique. Elle n'a pas connu de réel succès en raison des coûts des équipements, les terminaux eux étaient lourds car ils n'ont pas connu de miniaturisation. Toutefois la flexibilité et la portabilité que propose cette technologie la rendent rapidement populaire. En effet les réseaux cellulaires de première génération ont été les premiers à rendre possible l'utilisation du téléphone mobile de façon continue.

Les problèmes rencontrés dans cette première technologie, qui présente certains avantages comme la flexibilité et la portabilité, ont poussé les chercheurs à améliorer la qualité de service. La numérisation et la miniaturisation des équipements ont rendu la communication mobile accessible et beaucoup plus flexible, ce qui a permis l'introduction de la deuxième génération de téléphonie mobile, notamment le GSM.

1.3 Le GSM (Global System for Mobile communication) :

Le GSM est la première norme de téléphonie mobile numérique. Le GSM a connu un grand succès, grâce notamment à équipements terminaux plus petits, plus maniable et plus facile à transporter, avec plus d'autonomie et à un coût moindre.

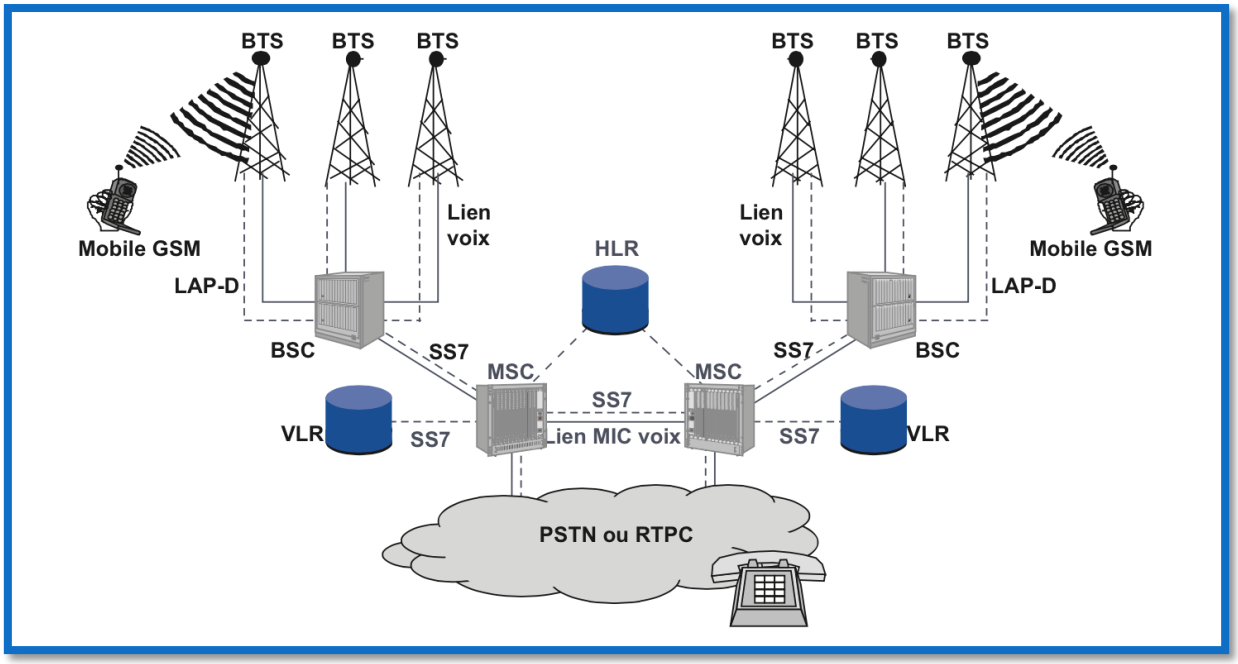

Figure 1.1 Architecture d'un réseau GSM [1]

L'architecture d'un système GSM se décompose en trois sous-systèmes [1] :

- Le sous-système radio (BSS, Base Station Subsystem) :
  Le BSS gère la partie radio des communications et est constitué de plusieurs BTS (Base Tranceiver Station), les BTS sont des émetteurs-récepteurs contrôlés par des BSC (Base Station Controller). Les BTS couvrent une zone géographique où éventuellement peut se trouver un utilisateur avec son terminal mobile MS (Mobile Station).

- Le sous-système réseaux (NSS, Network SubSystem) : comprenant les commutateurs de cœur de réseau MSC (Mobile services Switching Center) associés aux bases de données VLR (Visited Location Register) et HLR (Home Location Register).

- Le sous-système d'exploitation : appelé l'OMC ou le centre et l'exploitation de la maintenance qui regroupe trois activités principales qui sont la gestion administrative, commerciale et technique. Il permet de gérer les fautes, les alarmes et les performances des équipements, contrôle les droits d'accès des gestionnaires au réseau, et assure l'interface homme-machine d'exploitation.

1.4 Le GPRS (General Packet Radio Service) :

C'est un réseau mobile IP utilisant l'accès du GSM. Il est considéré comme la génération 2,5G ou la 2G+. C'est une mise à jour logicielle et matérielle des éléments de base du réseau GSM. Aussi on a introduit de nouveaux équipements permettant l'accès au réseau de données (ex. Internet). Ces équipements sont le PCU, GGSN, le SGSN.

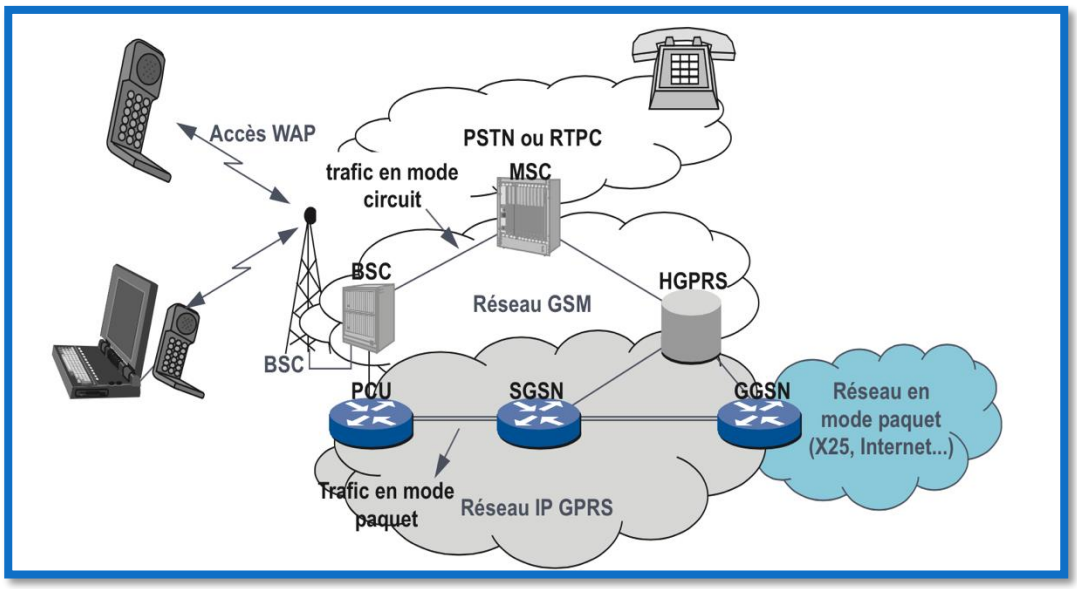

Figure 1.2 Structure d'un réseau GPRS [1]

PCU (Packet Controler Unit) : Le PCU assure l'adaptation des données issues du terminal mobile au format paquet et inversement.

SGSN (Serving GPRS Support Node) : c'est un nœud qui gère la signalisation dans le réseau cœur GPRS, afin de permettre la gestion de la gestion de la mobilité, l'attachement de l'abonné et l'établissement des sessions IP.

GGSN (Gateway GPRS Support Node) : c'est la passerelle dans le réseau cœur du GPRS qui permet aux utilisateurs d'accéder à Internet. On retrouve également ces deux nœuds (SGSN, GGSN) dans le réseau cœur de l'UMTS qu'on verra juste après. [1]

L'ensemble des équipements SGSN et GGSN forme ce que l'on appelle «le réseau fédérateur» ou *Backbone*.

1.5 L'UMTS (Universal Mobile Telecommunications System) :

L'arrivée de l'année 2000 a vu apparaitre une nouvelle génération de réseau mobile, la 3G. Cette troisième génération a connu un fort déploiement dès l'année 2005. La nouveauté par rapport à la deuxième génération concerne l'introduction du mode paquet à l'exception de la parole téléphonique, qui reste très semblable à celle du GSM. Toutes autres

informations, en dehors de la parole, sont mises dans des paquets et transportées dans un réseau à transfert de paquets.

On constate une nette amélioration des débits proposés par rapport au GSM, qui plafonne 9.6 Kbit/s, puisque le débit 3G atteint 384 kbit/s, lors de la première génération de l'UMTS. La 3G permet ainsi à l'utilisateur d'accéder aux premiers services multimédias.

Plusieurs types de schémas de modulations ont été étudiés pour l'émission numérique du signal. Il s'agit d'extensions des modulations classiques en fréquence, en amplitude et en phase. L'accès au canal radio utilise les techniques FDMA, TDMA et CDMA. Mais la méthode principale retenue pour la troisième génération est le CDMA. Les mobiles de la même cellule se partagent un canal radio par des techniques d'étalement de spectre, le système alloue un code unique à chaque client. [2]

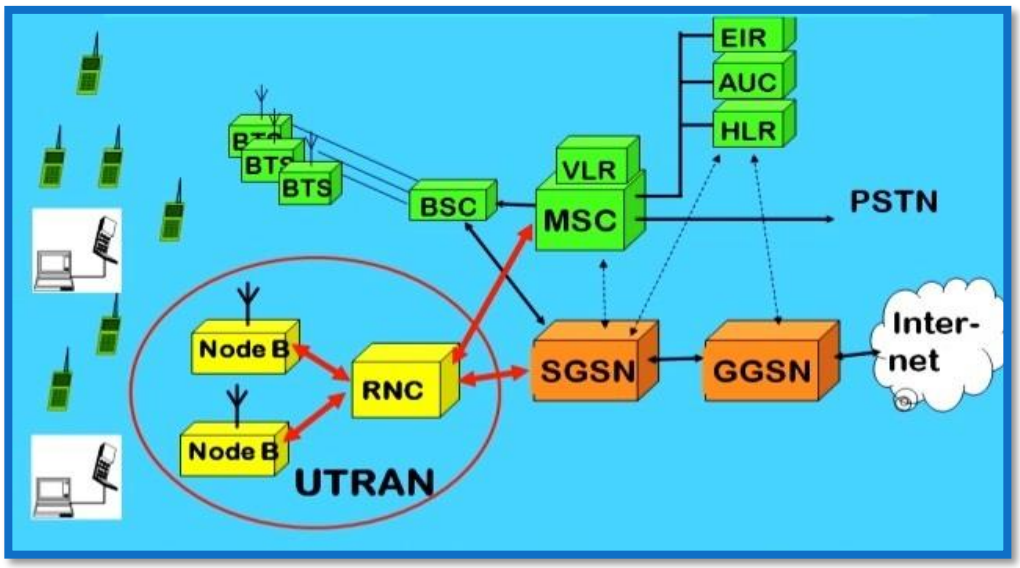

Figure 1.3 Architecture de l'UMTS [5]

L'architecture du réseau UMTS est modulaire. Ses éléments constituants sont indépendants, de façon à autoriser en théorie des mises à jour de telle ou telle partie du système sans avoir à en redéfinir la totalité. Toutefois les règles de compatibilité et d'interopérabilité sont à observer.

L'UMTS définit trois domaines qui sont les suivants:

- le domaine utilisateur ;
- le domaine d'accès radio, ou UTRAN (Universal Terrestrial Radio Access Network) ;
- le domaine du réseau cœur (Core Network).

L'interface Iu permet de connecter la Radio au cœur paquet (Iu entre RNC et SGSN et Iu-U entre RNC et SGSN en cas de 3GDT).

Le domaine utilisateur est similaire à celui du GSM. Il se compose d'un terminal capable de gérer l'interface radio et d'une carte à puce, qui contient les caractéristiques de l'utilisateur et de son abonnement. En revanche, l'accès radio de l'UMTS (UTRAN) est complètement différent. L'UTRAN regroupe les stations de base NodeB et les contrôleurs de station de base, ou RNC (Radio Network Controller).

Le réseau cœur est composés de deux parties, le réseau cœur de type circuit contenants les commutateurs circuits, les MSC (Mobile Service Switching Center) et le réseau cœur de type paquet composé de commutateurs paquet, les SGSN et GGSN (Serving and Gateway GPRS Support Node) qui relient le réseau de l'opérateur au monde extérieure.

Pour gérer les données relatives aux utilisateurs, telles que leur position dans le réseau, leur abonnement, etc., les bases de données introduites dans le GSM sont toujours présente dans l'UMTS. Il s'agit, entre autres, des HLR (Home Location Register), VLR (Visitor Location Register) et EIR (Equipement Identity Register). La figure 1.3 décrit l'architecture générale de l'UMTS.

1.6 La quatrième génération ou 4G :

C'est la génération de téléphonie mobile (et parfois fixe) succédant à la 2G et 3G. Elle permet le très haut débit mobile (débit théorique 150 Mbit/s, par cellule, voir plus) et permet également l'accès à plusieurs réseaux simultanément. L'une des caractéristiques de la 4G est d'avoir un réseau cœur basé que sur l'IP, c'est le *Evolved Packet Core*, en voulant simplifier l'architecture et de ne pas avoir, comme dans les générations précédentes, des réseaux cœur traitant les deux domaines circuit et paquet. La voix peut être transportée en VoIP (ou VoLTE, Voice over LTE). Il est possible aussi de permettre à l'utilisateur de passer des appels Circuit sur le réseau 2G/3G (CS Fallback).

Le contrôleur de station de base (RNC) a été supprimé pour permettre une architecture plus plate. L'architecture de la 4G sera étudiée en détail un peu plus dans ce chapitre.

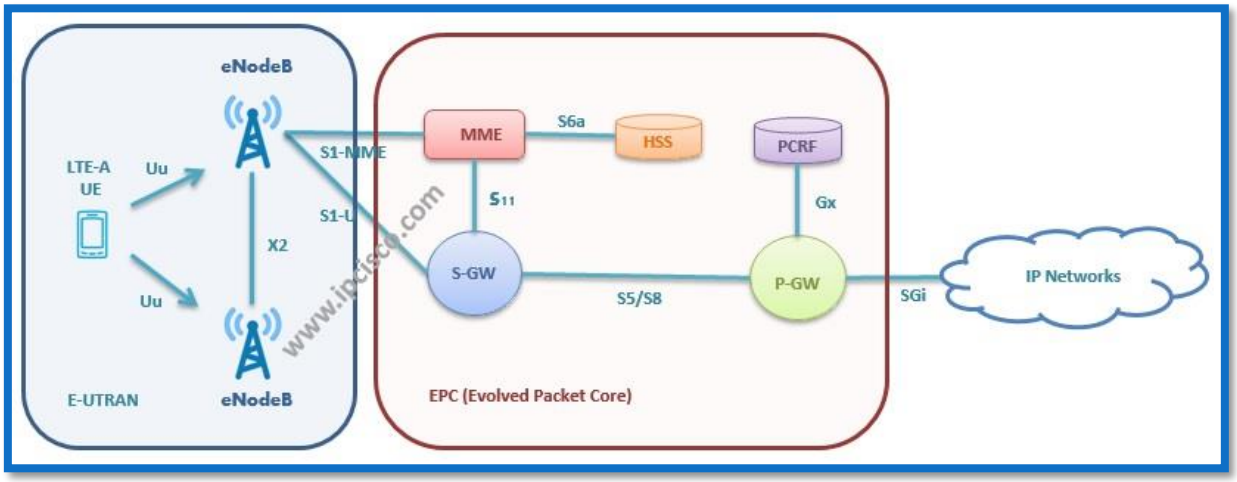

Figure 1.4 Architecture 4G [6]

Les différents nœuds (MME, S-GW, P-GW etc.) seront traités en détail. Les stations de bases peuvent être Co-localisés avec les stations de bases 2G/3G avec un rajout de module matériel et logiciel, grâce aux fonctionnalités Multistandards offerts par la plupart des équipementiers.

Le tableau ci-dessous résume les caractéristiques de ces quatre générations de la téléphonie mobiles. La cinquième génération (5G) n'est pas encore normalisée, elle le sera vers 2020. Mais on verra quand même dans les lignes suivantes quelques nouveautés apportées par cette dernière technologie.

Génération	*1G*	*2G*	*2.5G*	*3G*	*4G*
Standards	NMT, AMPS, TACS	GSM, IS95 A	GPRS, IS95 B	UMTS, CDMA2000	LTE
Techniques d'accès	FDMA	TDMA	FDMA/TDMA	CDMA	OFDMA
Fréquences	900 MHz	900 et 1800MHz	900 et 1800MHz	1900-2024MHz 2110-2200Mhz	800 MHz et 2600MHz
Débits réels	-	9.6 Kbps	48kbps	384kbps HSPA 14,4Mbps HSPA+ 42Mbps	150 Mbps

Figure 1.5 Tableau récapitulatif des quatre générations de réseaux mobiles

1.7 La cinquième génération ou 5G :

La cinquième génération de téléphonie mobile faisant suite à la 4G, permet des débits plus importants, le débit maximum devrait se situer entre 1 et 10 Gbit/s soit 100 à 1000 fois plus rapide que celui de la 4G. L'une des caractéristiques principales concerne l'internet des objets (IoT) qu'on va voir juste après, les applications IoT couvriront plus le domaine médical, le domicile (application domotique) et d'autres domaines.

Voici une la figure illustrant comment serait éventuellement l'architecture de la cinquième génération des réseaux mobiles.

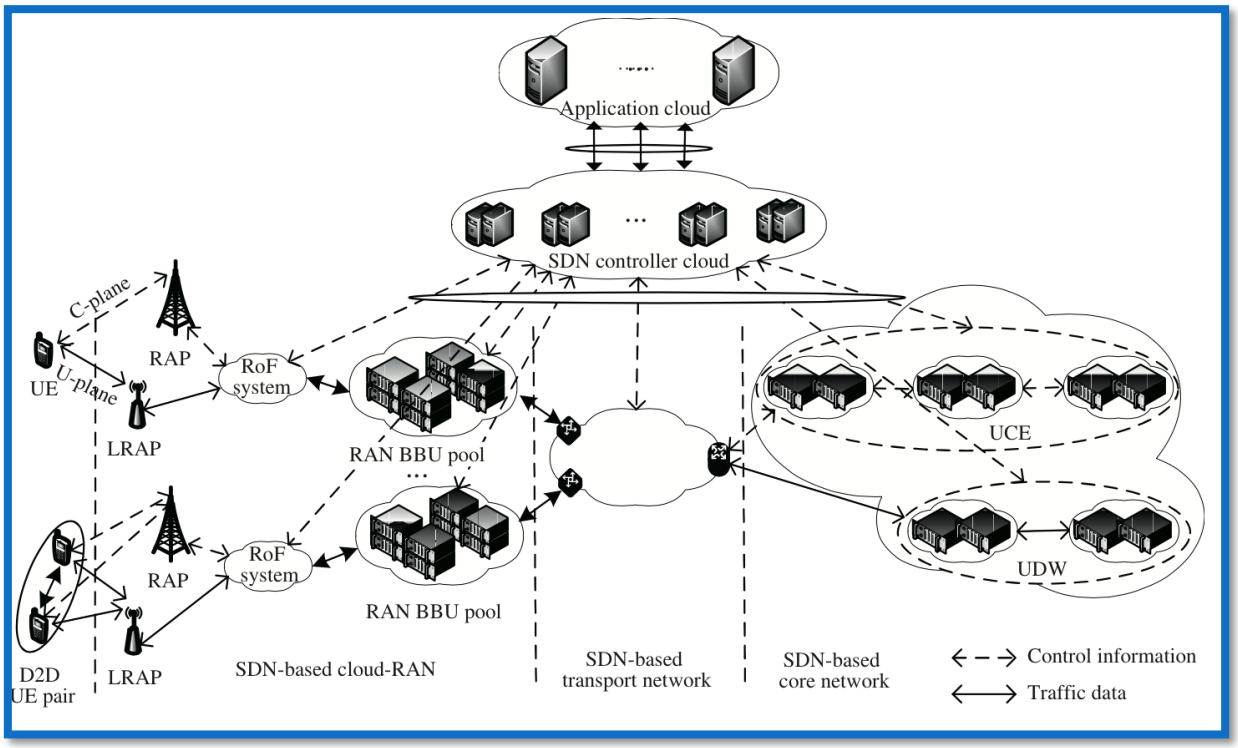

Figure 1.6 Architecture 5G [26]

Cette technologie n'est pas encore normalisée, il se pourrait qu'il y ait des modifications. Cependant on peut citer des éléments et technologies clés caractérisant cette cinquième génération, ces termes vont aider le lecteur à mieux s'informer sur cette dernière génération de réseaux cellulaires :

- UWB (Ultra Wide Band), une très large bande passante

- Smart Antenna, c'est des antennes intelligentes capables de récupérer n'importe quel type de signal de différentes technologies radio (Wi-Fi, 2G, 3G etc.), utilisant des différentes techniques de codage et de modulation. Elles peuvent travailler pratiquement sur une fréquence quelconque.

- La virtualisation, que l'on va étudier en détail au chapitre 2, est à la base de la révolution du monde des réseaux, il suffit d'écrire un code qui fait exactement ce que fait le matériel. Ainsi toutes les machines matérielles peuvent ce transformées en machines logicielles (virtuelles) à l'instar d'un certain nombre d'élément comme une antenne ou un capteur.

- Le C-RAN (Cloud- Radio Access Network)

- Le RAP (Radio Access Point) et le LRAP (Light Radio Access Point)

- Le SDN (Software-Defined Networking),qu'on va voir au chapitre 3
- Multi-homing, c'est le multi-accès
- Machine to Machine (M2M) ou bien Device to Device (D2D).

L'architecture réseau est basée sur le Cloud RAN (C-RAN) et le SDN (Softwar-Defined Networking) (voir chapitre 3). En plus du réseau de transport et du réseau cœur l'architecture 5G est constituée d'un Cloud d'application et un Cloud de contrôleur SDN. [26]

1.8 Conclusion :

A l'issu de ce chapitre on a pu voir les différentes étapes qu'a connu la téléphonie mobile qui est à ce jour en plein développement. On a suivi globalement l'évolution des réseaux mobiles en passants du mode analogique au mode circuit numérique, ensuite au mode paquet.

La monté du Cloud et du SDN ont permis de grandes révolutions dans le monde des réseaux cellulaires et dans le monde des réseaux tout court. EN effet ils ont contribué à l'intégration de l'internet des objets, et l'automatisation des réseaux.

2 Notions de l'IoT et le Mobile Broadband

2.1 Introduction :

L'Internet des objets (Internet of Things) est né avec l'idée de rattacher à Internet des capteurs que l'on peut trouver dans le monde physique notamment dans le domicile, lieu de travail, villes ou partout ailleurs.

Dans ce chapitre on va introduire la notion d'Internet of Things (IoT), nous allons voir les différents éléments et étapes nous permettant de bâtir un système IoT, la relation entre celle-ci et le mobile Broadband. Nous allons également étudier l'architecture d'un réseau cœur 4G, l'EPC (Evolved Packet Core).

2.2 IoT (Internet of Things) :

L'IoT est la communication des objets entre eux. Certains considèrent que c'est la troisième génération d'Internet connue sous le nom du web 3.0. IoT représente les échanges d'informations et de données provenant des dispositifs physiques vers le réseau Internet. L'IoT est un concept permettant aux objets physiques d'être identifiés, de communiquer entre eux, et de pouvoir mesurer et échanger des données entre le monde physique et virtuel (informatique).

Ces objets sont des dispositifs permettant de collecter, stocker, transmettre et traiter des données issues du monde physique. Ce sont des sources de données identifiés de façon unique et ayant un lien direct ou pas avec Internet.

Un objet peut être connecté à Internet ou bien à d'autres objets. Pour permettre ces objets de communiquer et échanger des informations, plusieurs étapes et outils sont nécessaires :

2.2.1 L'identification :

Il faut identifier chaque système ou objet connectable, en effet, un identifiant unique pour chaque objet permet de le reconnaître dans le réseau, c'est ce qu'on appelle le nommage. L'objet peut être identifié par une étiquette **RFID** (Radio Frequency Identification) composée d'une antenne est d'une puce électronique. Ce dispositif permet de recevoir et de répondre à des requêtes via une fréquence radio, l'objet devient unique et reconnaissable.

2.2.2 Capteur :

Les signaux analogiques (phénomènes physique) captés seront convertis en signaux numérique, on obtient alors des données.

2.2.3 Connexion :

Cette étapes nous permet de connecter les objets entre eux afin qu'ils puissent échanger leurs données ou leurs informations.

2.2.4 Intégration :

Chaque objet devrait avoir un moyen de communication qui le rattache au monde virtuel comme le Bluetooth, Wifi, une technologie cellulaire (GSM, GPRS, LTE…). Cette dernière nous intéresse particulièrement.

2.2.5 Le réseau :

Il faut relier le monde physique au monde informatique via Internet qui permet un pilotage et un contrôle à distance.

Nous avons désormais un système complet ou chaque objet peut interagir avec un autre ou bien avec l'extérieur via Internet (voir la figure ci-dessous) :

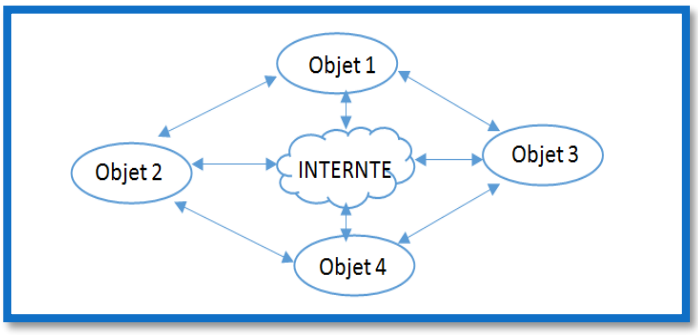

Figure 2.1 Système IoT

2.3 L'IoT et le Mobile Broadband :

Tout d'abord on définit les termes : **MTC, Cat 0, Cat 1, LTE-M, EC-GSM, NB-IoT** et **LPWA**.

Cat 0, Cat 1, sont des catégories. Les catégories définissent les performances générales de l'UE (User Equipment). Par exemple, le taux de transfert max sur la liaison montante et descendante supporté par les canaux de données. Ces catégories sont normalisées par la 3GPP (3rd Generation Partnership Project).

MTC, Machine Type communications c'est un terme utilisé par la 3GPP pour désigner les communications Machine To Machine (M2M). Le mobile Broadband est notamment un moyen de communication pour les machines entre eux.

LTE-M, ou LTE-MTC peut être utilisé pour faire référence à toute utilisation de la technologie LTE pour les communications M2M et IoT.

NB-IoT, signifie Narrow Band-IoT et c'est une nouvelle technologie radio à bande étroite en cours de normalisation par la 3GPP. Elle couvre tous les paramètres recherchés (faible consommation d'énergie, faible complexité, et longue portée)

EC-GSM-IoT, ou Extended Coverage GSM précédemment appelé EC-EGPRS, signifie la couverture étendue du GSM pour IOT. Il intègre les dernières améliorations apportées aux normes GSM et EGPRS pour soutenir une meilleure couverture et d'autres améliorations pour IoT**.**

LPWA(Low Power Wide Area),signifie faible puissance large zone, c'est les technologies radio offrants une faible consommation électrique et une large couverture.

La figure ci-dessous nous montre comment intégrer au mieux ces différentes technologies pour les divers cas d'applications IoT : chaque application IoT utilise une technologie d'accès qui lui est adéquate. Si par exemple une application a besoin de débits élevés (vidéo surveillances), pour quelle puisse fonctionner correctement elle utilise l'LTE-M. Si l'application n'a besoin que de quelques dizaines de kb/s pour quelle puisse remplir ces fonction (ex : smart metering) elle utilise dans ce cas le NB-IoT. Ça permet de gérer la bande passante.

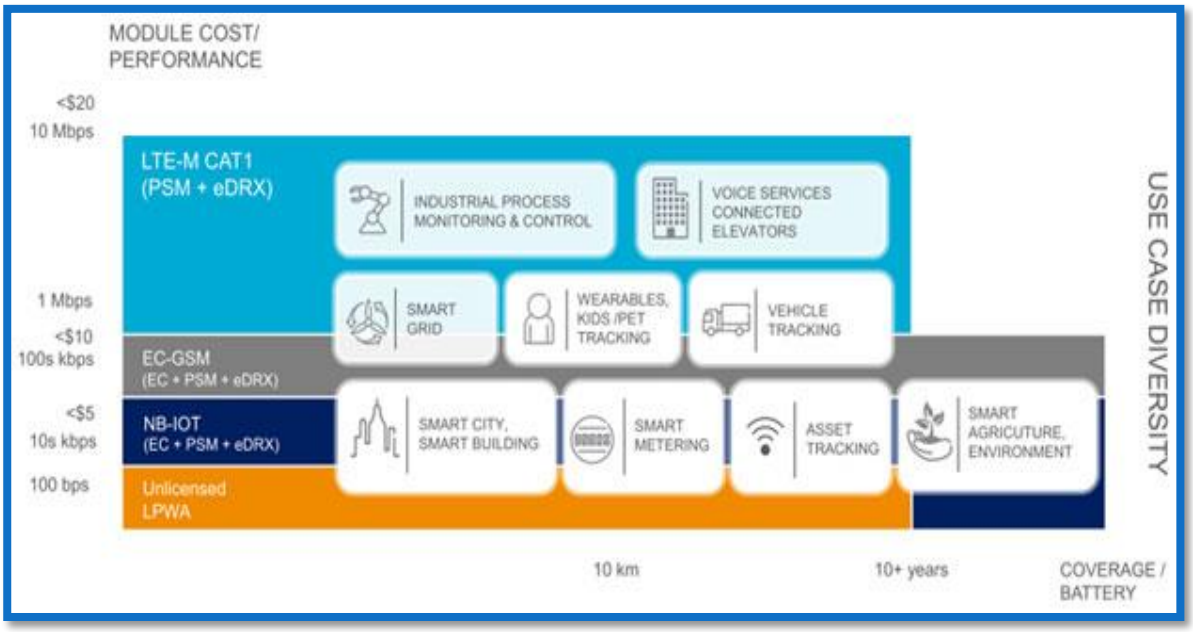

Figure 2.2 Techniques d'accès utilisées pour différente application IoT [8]

2.3.1 Quelques exigences M2M affectant le réseau PacketCore :

- Prévoir un grand nombre d'objets
- Configuration automatique des objets
- Fiabilité du système
- Supporter plusieurs technologies d'accès.
-

2.3.2 Quelques Solutions :

- Un support pour l'IPv6/IPv4
- Support de l'ADD (Automated Device Detection) et l'ADC (Automated Device Configuration)
- Haute performance de service
- Un support multi-accès.

2.3.3 Exemples d'applications :

Le smart metering (compteur intelligent) et la smart car(véhicule connecté) sont deux exemples d'applications ayant chacun différents paramètres et critères :

2.3.3.1 Le smart metering :

- Fiabilité
- Haute disponibilité du système
- Prévoir un grand nombre d'objets
- Faible coût du système.

2.3.3.2 La smart car :

- Mobilité
- Fiabilité et robustesse du système
- Itinérance
- Sécurité
- Localisation du véhicule en TR
- Faible Latence du système.

2.4 L'architecture EPC (Evolved PacketCore) :

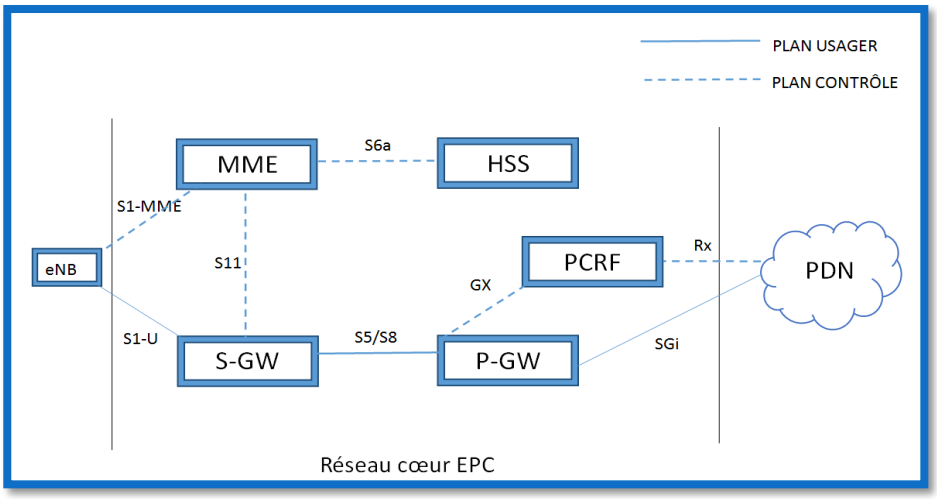

Figure 2.3 Architecture EPC

2.4.1 Notions de plan de contrôle et de plan usager :

Deux types de données transitent sur les interfaces de l'architecture EPC : les données de signalisation portées par le plan de contrôle (control plane), les données utilisateurs quant à elles sont portées par le plan usager (user plane).

Le plan de contrôle d'une interface permet de contrôler le plan usager en établissant, reconfigurant, ou relâchant une connexion, échange de messages associés à l'UE (Equipement Utilisateur ou *en anglais* User Equipment). Toutefois le plan de contrôle d'une interface ne porte pas forcement des messages à destination ou en provenance de l'UE.

Le plan usager d'une interface, inclus les fonctions et protocoles mise en place pour le traitement des données à destination ou en provenance de l'abonné (l'UE) circulant dans le réseau mobile. [4]

2.4.2 Les différents nœuds constituants l'EPC sont :

-MME (Mobility Management Entity) ;
-HSS (Home subscriber Server) ;
-P-GW (Packet Data Network Gateway) ;
-S-GW (Serving Gateway) ;
-PCRF (Policy Control and ChargingRulesFunction**).**

Définissons les fonctions de chacun des nœuds constituants l'EPC :

MME : c'est le nœud de contrôle qui gère la signalisation entre l'UE et le réseau cœur. Il est responsable de la gestion des bearers (session), notamment les phases d'établissement, de reconfiguration et de la relâche des bearers.

Le MME prend en charge la gestion de la connexion et de la sécurité, il est notamment le point de terminaison des protocoles NAS (Non Access Stratum) au sein de l'architecture EPC. Le MME permet de gérer la mobilité de l'utilisateur et initie les handover Inter système.

HHS : le HSS contient les informations de souscriptions des utilisateurs, telles que la qualité de service (QoS) appliquée pour l'abonné ou la restriction d'accès en cas de roaming .Il détient aussi les informations concernant le type de réseaux PDN auxquels l'abonné peut se connecter. Le HSS peut aussi indiquer l'identité du MME auquel l'utilisateur est attaché. Il peut également intégrer un centre d'authentification ou AuC (Authentification Center), qui permet d'authentifier des abonnés et fournir les clés de chiffrement nécessaires.

S-GW : la S-GW transfère tous les paquets IP à destination d'utilisateurs, elle est également le point d'ancrage pour les bearers de données lorsque l'UE est en mobilité entre eNBs.
La S-GW conserve aussi les contextes sur les bearers de l'UE lorsque celui-ci est en mode veille, elle gère aussi quelques fonctions supplémentaires au sein du réseau visité, en cas d'itinérance (roaming) elle envoie des informations au réseau visité pour effectuer la facturation. Enfin la S-GW sert également d'un point d'ancrage pour l'interfonctionnement avec d'autres technologies d'accès 3GPP comme l'UMTS.

P-GW : la P-GW a pour rôle principal d'allouer les adresses IP à l'UE. Elle supporte la fonction d'inspection approfondie des paquets, dite **DPI** (Deep Packet Inspection), qui analyse les paquets du plan usager, identifie la nature des flux, applique les règles prédéfinies pour les clients selon leur souscription. La P-GW alloue des paquets IP transférés au sein des bearers de QoS différentes, et joue ainsi un rôle principal pour gérer la QoS, également pour les bearers dédié (à débit garanti). Elle permet aussi de mettre en œuvre la facturation par flux de données en respectant les règles définies par le PCRF. Enfin elle sert de point d'ancrage pour l'interfonctionnement avec d'autres technologies d'accès non 3GPP tel que WiMax ou encore le CDMA 2000.

PCRF : le PCRF est un nœud optionnel au sein de l'architecture EPC. Il applique des règles de gestion évoluées sur le trafic et la facturation de l'abonné en fonction de l'offre souscrite. Pour appliquer ces règles, il communique avec le PCEF (Policy Control Enforcement Function), fonction intégrée à la P-GW. Si par exemple l'abonné atteint le seuil de volume de données inclus sa souscription, le PCRF donne l'ordre au PCEF afin que ce dernier limite le débit d'utilisation à travers l'interface Gx. Le PCRF est capable d'indiquer les caractéristiques de qualité de service **QCI** (QoS Class Identifier) et débits appliqués par le PCEF sur les flux de données, lors de l'établissement d'une session ou en cours de session. Le PCRF veille à ce que le traitement appliqué est en accord avec le profil de souscription de l'abonné.

2.4.3 Les interfaces standards de l'architecture EPC :

S1-MME : traite les flux du plan de contrôle entre le MME et l'eNB.

S11 : elle relie le MME à la S-GW.

Les interfaces S1-MME et S11 utilisent un protocole appelé GTP-C (GPRS Tunneling Protocol-Control plan), et sont notamment utilisées pour la signalisation.

S6a : elle relie le MME au HSS elle permet de transmettre les informations de l'abonnement et d'authentification pour authentifier et autoriser l'accès des utilisateurs.

Gx : elle relie le P-GW au PCRF. Elle transmet à la P-GW, plus exactement au PCEF, les décisions prises par le PCRF à propos de la QoS à appliquer aux abonnés. L'interface Gx permet aussi au PCEF de reporter au PCRF certaines informations sur la session de l'abonné telles que l'usage de données.

Les interfaces S6a et Gx sont basées sur le protocole Diameter.

Rx : elle relie le PCRF au PDN (Packet Data Network/ service network et plus spécifiquement à un serveur Application function).Dans le cas d'un appel VOLTE, Rx relie le PCRF au serveur IMS.

S3 : elle établit une connexion entre le MME et le SGSN, elle permet l'échange d'informations pour la mobilité entre les réseaux d'accès inter-3GPP.

S1-U : traite les flux du plan usager entre la S-GW et l'eNB.

S5/S8 : elle relie la S-GW à la P-GW, elle transmet les paquets de données. En cas d'itinérance et que la P-GW se trouve dans le réseau visité (VPLMN ou Visited PLMN ou bien *local breakout*), S5 sera utilisée, dans le cas contraire où la P-GW se trouve dans le réseau local (HPLMN ou Home PLMN ou bien *Home Routed*) on utilise l'interface S8.
Ces interfaces utilisent un protocole appelé GTP-U (GPRS Tunneling Protocol-User plane).

S4 : elle relie le SGSN à la S-GW, elle traite à la fois les transferts de signalisation et de charge utile, et permet également à la S-GW d'ancrer le transfert inter-3GPP. Elle est basée sur les protocoles GTP-U et GTP-C

SGi : elle relie la P-GW au PDN qui peut être Internet ou un réseau privé d'une entreprise.

Gn/Gp : elle relie la P-GW et le MME au SGSN.

Gi : elle relie un GGSN au PDN.

La figure 2.4 illustre les interconnexions entre les nœuds SGSN-MME et l'EPG.

SGSN (Serving GPRS Support Node) : c'est un nœud qui gère la signalisation dans le réseau cœur GPRS, il peut notamment gérer plusieurs terminaux dans une zone donnée.

GGSN (Gateway GPRS Support Node) : c'est la passerelle dans le réseau cœur du GPRS qui nous permet d'accéder à Internet, elle permet aussi aux paquets de données d'êtres acheminés vers l'équipement SGSN du destinataire. On retrouve également ces deux nœuds (SGSN, GGSN) dans le réseau cœur de l'UMTS**.**
L'ensemble des équipements SGSN et GGSN forme ce qu'on appelle «le réseau fédérateur» ou *Backbone*.

SGSN et GGSN définis, on peut maintenant décrire les fonctions des nœuds SGSN-MME et EPG. En effet certains constructeurs comme Ericsson proposent des solutions cœur paquet multi accès (2G, 3G ,4G, etc.) et Co-localisent les fonctions logiques sur les mêmes plateformes physiques.

SGSN-MME : le SGSN-MME fournit les fonctionnalités du SGSN et du MME, il est notamment possible d'utiliser le SGSN-MME pour les fonctionnalités du SGSN ou du MME ou bien des deux à la fois. Le SGSN-MME nous permet de gérer les utilisateurs à multi-souscription, telles que GSM, WCDMA et la LTE, le contrôle de signalisation de l'UE, etc.

EPG : l'EPG quant à lui fournit les fonctions du GGSN,S-GW et du P-GW, il est notamment possible d'utiliser l'EPG pour remplir les fonctions du GGSN ou de la S-GW ou bien de la P-GW, on peut l'utiliser également pour les fonctions des S-GW et P-GW. Comme on peut l'utiliser pour les trois fonctionnalités à la fois. Notamment l'application de la QoS, fonction DPI etc. [25]

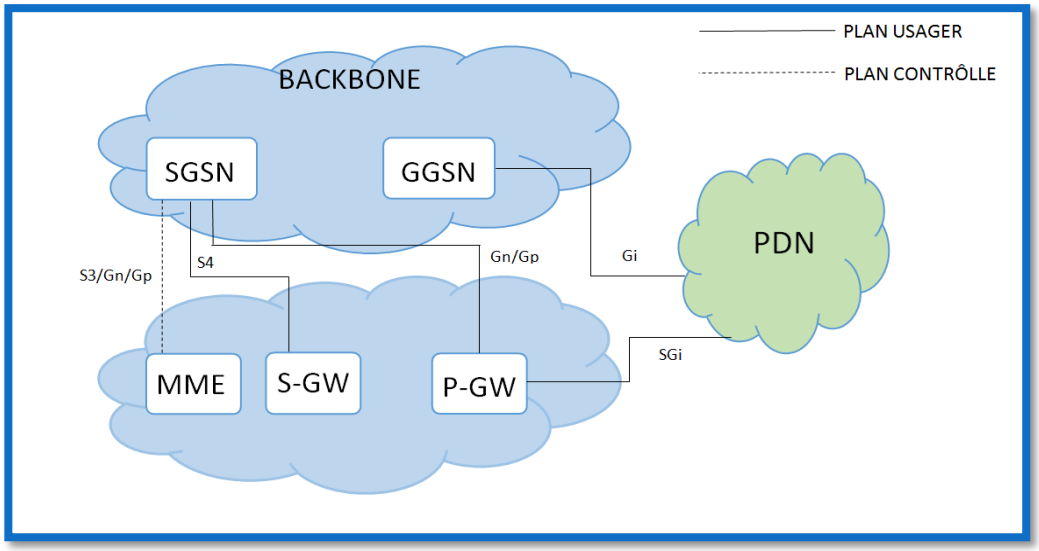

Figure 2.4 Interfonctionnement des nœuds SGSN-MME et EPG

2.5 Le Call flow d'un appel data 4G :

Ci-dessous, les différentes procédures d'établissement d'un appel 4G, notamment l'établissement d'une session EPS (LTE/EPC) :

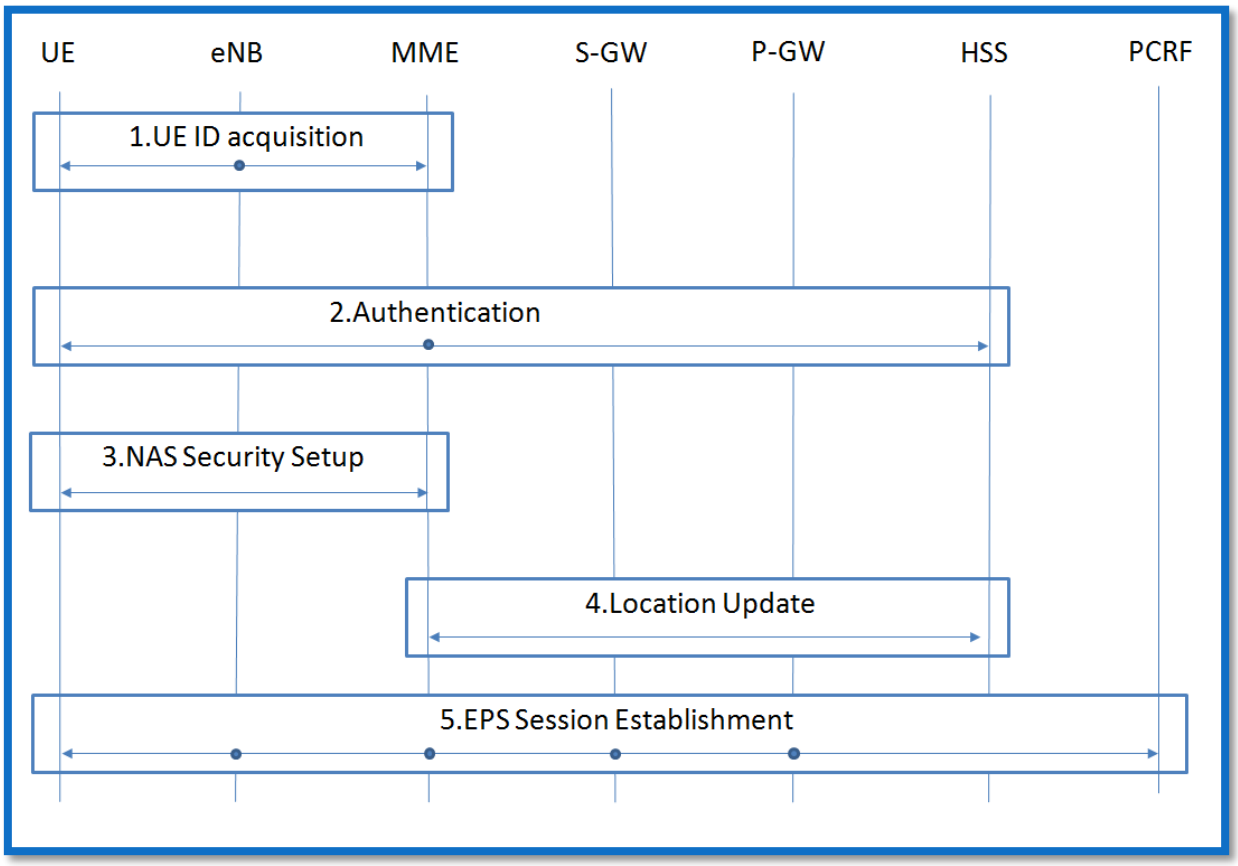

Figure 2.5 Call flow d'un appel data 4G

Décrivons les différentes étapes d'établissement du bearer EPS [9] :

2.5.1 UE ID acquisition (l'acquisition de l'IMSI de l'UE) :

Le MME obtient un IMSI de l'UE. Initialement l'UE tente de se connecter au réseau en envoyant un message **Attach Request** au MME contenant l'IMSI. Cette étape peut être divisée en deux sous-étapes : l'UE se trouve dans l'état « initiale » après une synchronisation de la liaison radio, en suite l'UE établie une connexion ECM (EPS Connection Management) pour qu'il puisse délivrer un message **Attach Request** au MME. Pour établir une connexion ECM, une connexion **RRC** (Radio Resource Control) et une connexion de **signalisation S1** sont nécessaires.

-Etat initial : après la synchronisation de la liaison radio ;
Pour que l'UE puisse envoyer un message **Attach Request** au réseau, la communication avec l'eNB est primordiale, L'UE choisit une eNB (cellule) en sélectionnant un PLMN et entame les procédures de recherche de cellules, l'UE obtient une liaison radio synchronisée. Désormais l'UE peut communiquer avec l'eNB, mais il est dans un état EMM-Deregisterd, ECM-Idle, RRC-Idle.

-Etablissement d'une connexion ECM :
Sur la couche NAS, l'UE envoie un message **Attach Request** (contenant l'IMSI et la capacité réseau de l'UE) demandant une première liaison à la couche NAS du MME. Pour que l'**Attach Request** soit délivré, une connexion ECM est nécessaire entre l'UE et le MME.

La couche NAS ou Non Access Stratum c'est l'ensemble des protocoles permettant l'échange d'informations en l'UE et le réseau cœur. Le protocole NAS permet entre autre l'enregistrement au réseau, la mise à jour de localisation, la sécurité etc.

L'ECM quant à elle, exige une connexion RRC entre l'UE et l'eNB et une signalisation S1 entre l'eNB et le MME :

Voici la figure résumant les procédures d'acquisition de l'IMSI :

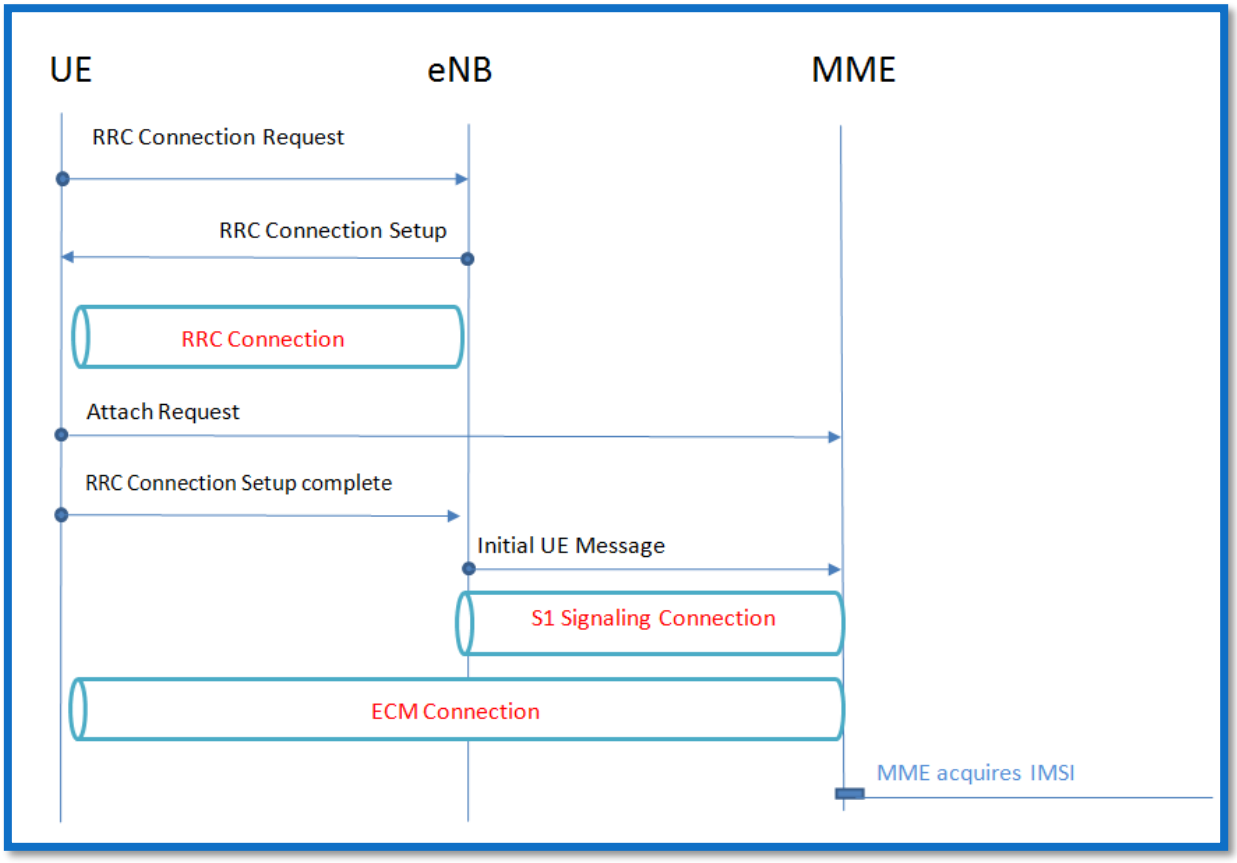

Figure 2.6 Procédure d'acquisition de l'IMSI

2.5.1.1 Etablissement d'une connexion RRC (Radio Resource Control) :

Voici les étapes nécessaires pour l'établissement d'une connexion RRC:

[UE →eNB] Demande de connexion RRC :

L'UE envoie un message **RRC Connection Request** à l'eNB. Le message est envoyé sur le SRB0 (Signal Radio Bearer) et le CCCH (Common Control Channel).

[UE ←eNB] Configuration de connexion RRC :

L'eNB alloue un bearer SRB (SRB1) dédié à l'UE en lui envoyant un message **RRC Connection Setup**, qui est délivré sur le SRB0 et le CCCH. Les ressources Uplink/Downlink de l'UE sont contrôlées par l'eNB.

[UE →eNB] Configuration de connexion terminée :

L'UE informe l'eNB que la configuration de la connexion RRC est terminée en envoyant un message **RRC Connection Setup Complete** sur le SRB1 et le DCCH (Dedicated Control Channel).

2.5.1.2 Etablissement de la connexion de signalisation S1 :

Les messages de contrôle entre l'eNB et le MME sont envoyés sur l'interface S1-MME, ils sont intégrés dans les messages S1-AP. Les connexions de signalisation S1 sont définies par la paire d'identifiants (eNB UE S1-AP ID, MME UE S1-AP ID) alloués par l'eNB et le MME pour l'identification des UEs.

L'**Attach Request** arrive à l'eNB avant l'établissement de connexion de signalisation, ainsi l'eNB alloue un identifiant (eNB UE S1-AP ID) pour l'établissement de connexion de signalisation S1, et envoie au MME l'**Attch Request** en l'encapsulant dans un message dit **Initial UE Message**. Le message **Initial UE Message** est constitué d'éléments suivants :

Initial UE Message(eNB UE S1-AP ID, NAS-PDU, TAI, ECGI, RRC Establishment Cause)

- eNB UE S1-AP ID : identifie les UEs dans l'eNB sur l'interface S1-MME.
- NAS-PDU : message NAS (Attach Request).
- TAI (Tracking Area Identifier) : indique la TA (Tracking Area) sur laquelle l'UE se trouve (zone d'enregistrement).
- ECGI (Evolved Cell Global Identifier):indique la cellule sur laquelle l'UE se trouve.
- RRC Establishment Cause : indique la signalisation générée par l'UE.

Quand le MME reçoit le message **Initial UE Message** de l'eNB sur l'interface S1-MME, il alloue un identifiant MME UE S1-AP ID, la paire d'identifiants (MME UE S1-AP ID, eNB UE S1-AP ID) permet l'établissement de la connexion de signalisation S1.

2.5.1.3 Etablissement de connexion ECM S1 :

Après l'établissement de connexion RRC et de signalisation S1, la connexion ECM entre les couches NAS de l'UE et du MME est établie à son tour. L'UE passe à l'état EMM-Registred, ECM-Connected et RRC-connected.

2.5.1.4 L'acquisition de l'IMSI :

La couche NAS du MME reçoit donc l'IMSI de l'UE à partir de l'**AttachRequest** envoyé par la couche NAS de l'UE.

2.5.2 Authentication (l'authentification entre l'UE et le MME) :

Ce processus est réalisé en deux étapes :
-Le MME reçoit des informations d'authentification du HSS pour l'UE.
-L'authentification mutuelle, durant laquelle le MME et l'UE sont mutuellement authentifiés.

La première étape est réalisée sur l'interface S6a en utilisant le protocole Diameter.
La deuxième étape est réalisée sur l'UE et le MME en utilisant le protocole NAS.

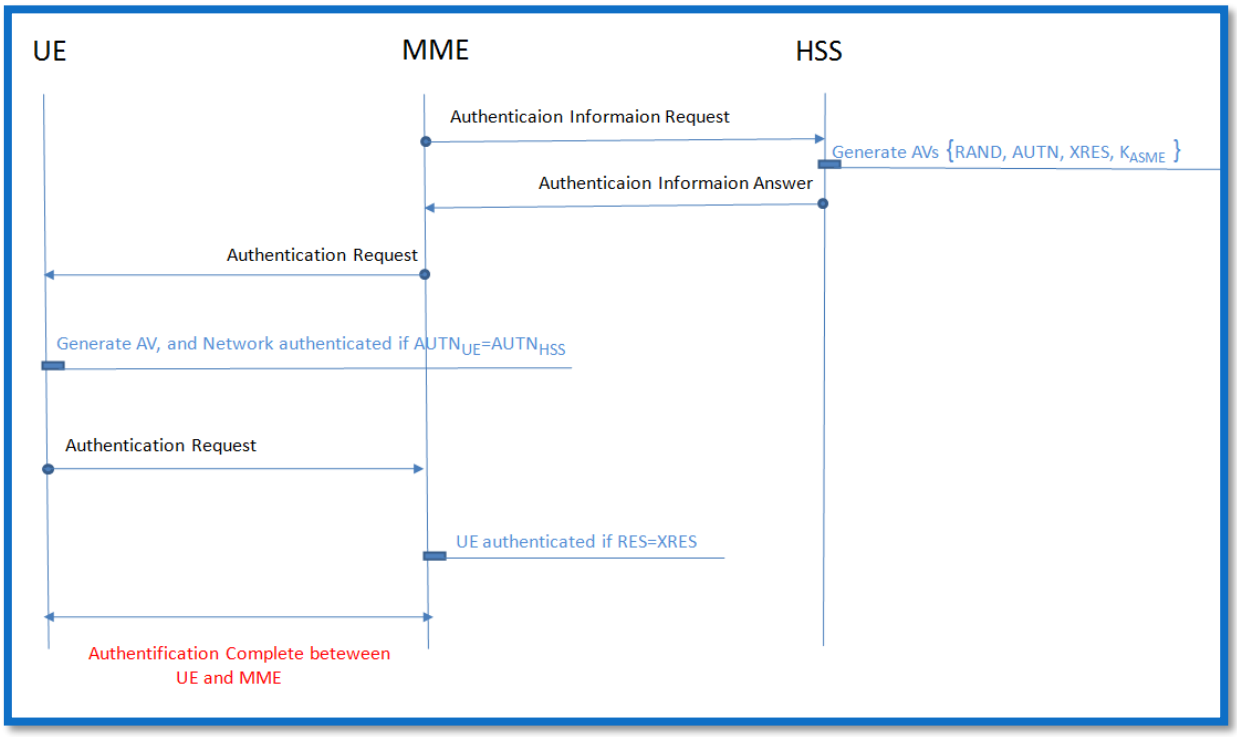

Figure 2.7 Procédure d'authentification

2.5.2.1 L'acquisition des vecteurs d'authentification :

[MME → HSS] Demande d'information d'authentification :

Le MME envoie un message **Authentication Information Request** au HSS, demandant les vecteurs d'authentification (AV) pour l'UE. Il inclut dans ce message l'identifiant SN ID (Serving Network ID), l'IMSI de l'UE, et s'assure que la HSS reflète les informations sur le réseau de desserte actuel pour l'UE (à savoir le PLMN que l'UE utilise).

[HSS] Génération de vecteurs d'authentification :

Le HSS génère les vecteurs d'authentification en utilisant le *LTE master Key* (LTE Key) dans l'IMSI et SN ID de l'UE. Les AVs sont générés en deux étapes :

-la première : le HSS génère la SQN et le RAND puis saisie les valeurs {LTE K, SQN, RAND} dans la fonction de chiffrement (crypto function) pour générer les valeurs {XRES, ATUN, CK, IK},dans la KDF (Key Derivation Function) pour obtenir la K_{ASME} ;

-{XRES, ATUN, CK, IK}=crypto function {LTE K, SQN, RAND}.

-K_{ASME}=KDF {SQN, SN ID, CK, IK}, voir la figure ci-dessous :

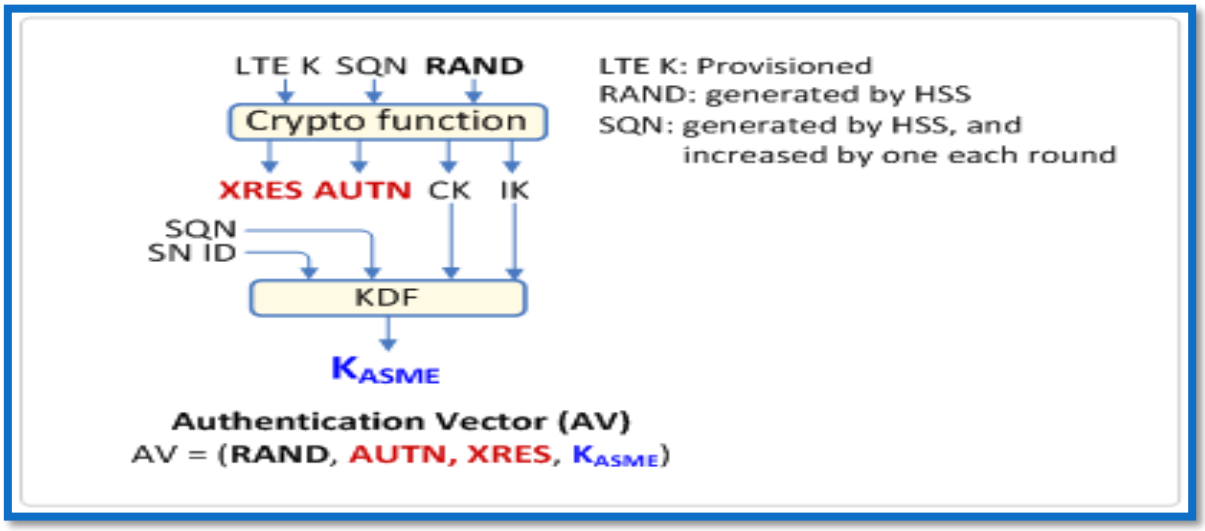

Figure 2.8 Génération de vecteurs d'authentification [9]

Au final on retrouve dans le vecteur d'authentification les éléments suivants {RAND, AUTN, XRES, K_{ASME}}. Décrivons le rôle de chacun de ces éléments :

-RAND : c'est un nombre aléatoire (Random) généré par le HSS et délivré à l'UE, il l'utilise afin de générer ces vecteurs d'authentification.

-AUTN : est un jeton d'authentification généré par la HSS et aussi délivré à l'UE. L'UE après avoir générer ces vecteurs d'authentification il compare la valeur de ce jeton avec celui qu'il a généré lui-même pour l'authentification du réseau.

-XRES : est une valeur générée par le HSS. Le MME garde cette valeur pour lui sans l'envoyer à l'UE, puis la compare avec le RES reçu de l'UE après l'authentification du réseau pour authentifier un usager.

-K_{ASME} : c'est la clé de niveau supérieur dans le réseau d'accès, c'est la clé mère, générée par l'UE et le HSS au MME pour l'utiliser dans le réseau d'accès. Elle sert comme clé de base pour le MME et l'UE quand les clés de sécurité NAS sont générées.

[MME ← HSS] Délivrance de vecteurs d'authentification :

Le HSS envoie les vecteurs d'authentification au MME, ils sont inclus dans le message **Authentication Information Answer**. Le MME les utilise ensuite pour effectuer l'authentification mutuelle avec l'UE.

2.5.2.2 Authentification mutuelle :

Le LTE exige une authentification mutuelle entre l'UE et le réseau (MME). Une fois que le MME reçoit les vecteurs d'authentification {RAND, AUTN, XRES, K_{ASME}} à partir du HSS, il envoie le RAND et le AUTN à l'UE de telle sorte que l'UE puisse générer les vecteurs d'authentification et authentifie le réseau. Toutefois, le MME garde le XRES et la K_{ASME} pour l'authentification des usagers et la sécurité NAS.

K_{ASME} n'est pas transmise à l'UE, mais la KSI_{ASME}, une clé index de la K_{ASME}, est transmise à ça place. Voici les procédures d'authentification mutuelle entre l'UE et le MME :

[UE ← MME] Demande de la MME pour l'authentification de l'abonné :

Le MME envoie le message **Authentication Request** (RAND, AUTN, KSI_{ASME}) à l'UE.

[UE] L'utilisateur authentifie le réseau :

Une fois le message **Authentication Request** reçu, l'UE génère d'abord la SQN pour l'AUTN, puis les AVs (authentification vectors) que le HSS a produit.
L'UE compare ensuite ses AUTN ($AUTN_{UE}$) avec ceux reçus du MME ($AUTN_{HSS}$) pour authentifier le réseau.

[UE → MME] L'UE délivre le RES au MME :

Après l'authentification du réseau en comparant les valeurs AUTN, l'UE envoie ses valeurs RES au MME, incluses dans le message **Authentication Response** (RES), le MME peut désormais authentifier l'utilisateur.

[MME] Le réseau authentifie l'UE :

Après la réception du message **Authentication Response** de l'UE, le MME compare la valeur RES générée par l'UE avec la valeur XRES reçue du HSS, pour authentifier l'utilisateur.

On a désormais une authentification complète entre l'UE et le réseau (MME).

2.5.3 NAS Security Setup (la configuration de la sécurité NAS) :

Le MME engage la procédure NAS Security Setup afin que les messages NAS puissent êtres échangés en toute sécurité entre les deux entités (l'UE et le MME). Voici les procédures de configuration de sécurité :

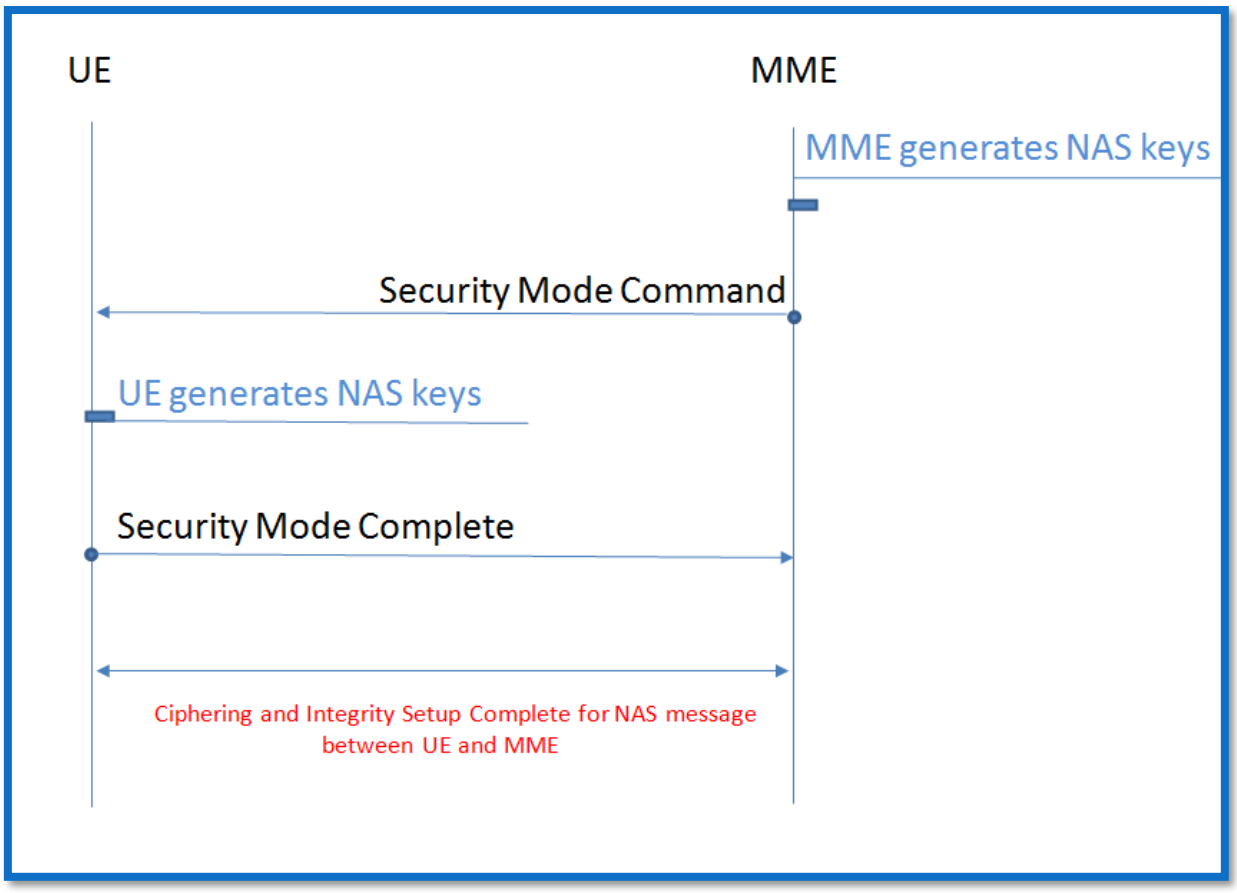

Figure 2.9 Procédure de configuration de sécurité NAS

[MME] Génère les clés de sécurité NAS :

Le MME sélectionne les algorithmes de chiffrement et d'intégrité à appliquer aux messages NAS de l'**Attach Request** reçu de l'UE, puis il délivre une clé dite *NAS integrity Key* (K_{NASint}) et une autre clé dite *NAS encryption Key* (K_{NASenc}) à partir de la clé mère K_{ASME} pour être appliquées aux messages NAS.

[UE ← MME] Aide l'UE pour générer les NAS Security Keys :

Le MME informe l'UE à propos des algorithmes de sécurités sélectionnées, en les incluant dans un message **Secutity Mode Command** (KSI_{ASME}, Security Algorithm, NAS-MAC) pour aider l'UE à générer les clés de sécurité NAS (*NAS Security Keys*).

[UE] Génère les clés de sécurité NAS :

Quand l'UE reçoit le message **Security Mode Command**, l'UE génère les clés de sécurité NAS (K_{NASint} et K_{NASenc}) en utilisant un algorithme de sécurité (NAS Security Algorithm que le MME a sélectionné) et effectue la validation d'intégrité sur le message **Security NAS Command** en utilisant la clé (K_{NASint}).

[UE → MME] Génération de clés de sécurité NAS est terminée :

L'UE informe le MME que la génération de clés de sécurité NAS est réussie en envoyant un message **Security Mode Complete** (NAS-MAC), après l'avoir chiffré et protégé l'intégrité en utilisant les clés générées.

2.5.4 Location Update (mise à jour de la localisation) :

Une fois que les procédures d'authentification et NAS Security Setup sont terminées, le MME doit enregistrer l'abonné dans le réseau, et savoir quels sont les services auxquels l'abonné peut accéder. A cette fin, le MME avise le HSS que l'abonné est inscrit dans le réseau, Puis il accède aux informations de l'abonné à partir du HSS. Pour ce faire des procédures de mise à jour et protocole Diameter sur l'interface S6a entre le MME et le HSS sont mise en place.

Voici les procédures nécessaires :

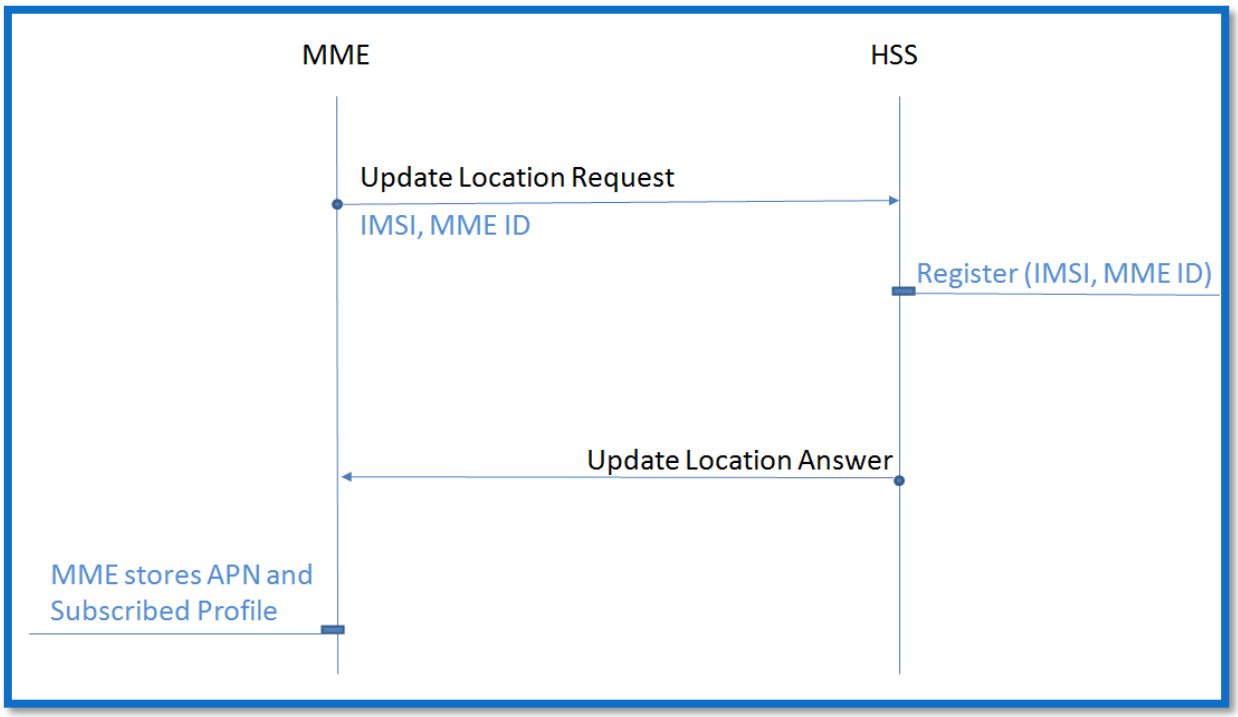

Figure 2.10 Procédure de mise à jour de la localisation

[MME → HSS] Notifie l'emplacement de l'UE :

Le MME envoie un message **Update Location Request** (IMSI, MME ID) au HSS afin de l'informer de l'enregistrement de l'UE et obtient donc les informations de la souscription de l'UE.

[HSS] Mise à jour de localisation de l'UE :

Le HSS enregistre l'identifiant du MME (MME ID) pour indiquer dans quel MME l'UE se trouve.

[MME ← HSS] Délivre les informations de l'abonné :

Le HSS envoie au MME les informations de souscription de l'abonné, ces informations sont inclus dans un message **Update Location Answer** pour que le MME puisse créer un bearer EPS par défaut pour l'abonné. Voici les informations de souscription incluses dans l'**Update Location Answer** :

Update Location Answer (IMSI, Subscribed APN, Subscribed P-GW ID, SubscribedQoS Profile).

-Subscribed APN : l'APN sur lequel l'usager est souscrit (e.g. Service d'Internet)
-Subscribed P-GW ID : un identifiant pour la P-GW à travers laquelle l'UE peut accéder à l'APN souscrit.
- SubscribedQoS Profile : (UE-AMBR (UL/DL), QCI, ARP, APN-AMBR(UL/DL)) ;
UE-AMBR (UL/DL) : c'est la bande passante globale de tous les bearers non-GBR qu'un UE peut avoir, elle est déterminée par le MME et contrôlée par l'eNB.
QCI, ARP, APN-AMBR(UL/DL) :QoS appliquée à l'APN souscrit.

[MME] Stockage d'informations d'abonnement :

Le MME reçoit le message **Update Location Answer** à partir du HSS, et enregistre les informations de souscription se trouvant dans le message.

2.5.5 EPS Session Establishment (établissement de session EPS):

Le MME établit une session EPS par défaut (non dédiée) pour l'utilisateur en se basant sur les informations de souscription. En faisant cela le MME alloue les ressources (réseau/radio) pour fournir à chaque utilisateur la QoS selon le profil souscrit.

Voici les procédures d'établissement d'une session EPS :

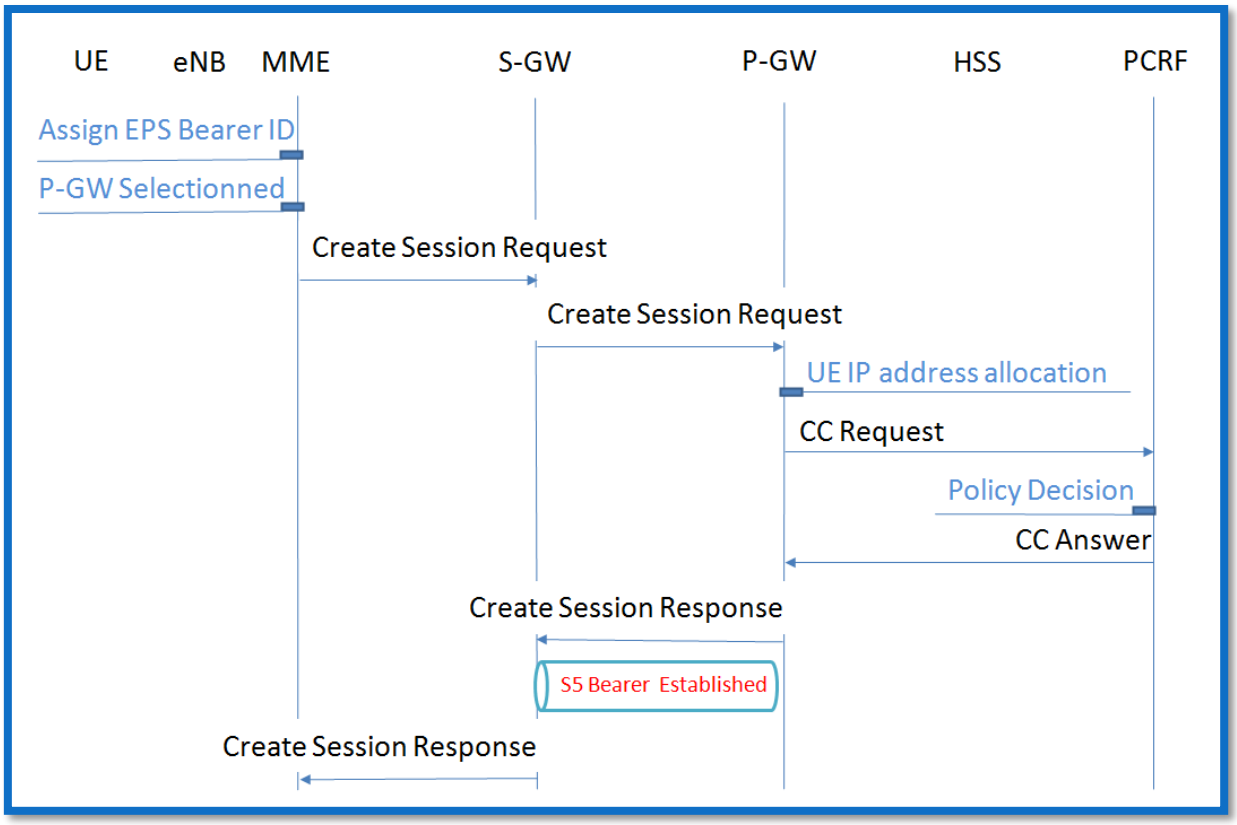

Figure 2.11 Procédure d'établissement d'une session EPS (1)

[MME] Attribue un EPS Bearer ID :

Le MME sélectionne une valeur et l'alloue comme identifiant de bearer EPS (EPS Bearer ID), afin d'établir une session EPS par défaut pour l'utilisateur qui vient d'être attaché.

[MME] Sélection de P-GW :

Le MME vérifie l'APN (Access Point Network) reçu à partir du HSS, et décide sur quelle P-GW se connecter pour l'accès à l'APN. Cette décision peut être basée sur les informations de la souscription reçues du HSS (Spécifiquement le P-GW ID). Le MME ensuite choisit la S-GW à travers laquelle il peut atteindre la P-GW sélectionnée.

[MME → S-GW] Demande de création d'une session EPS :

Le MME et la S-GW communiquent à travers l'interface S11 (plan de contrôle) en utilisant le protocole GTP-C (GPRS Tunneling Protocol-Control plane). Le MME envoie un message **Create Session Request** à la S-GW sélectionnée précédemment. Ce message contient les paramètres suivants :
Create Session Request (IMSI, EPS Bearer ID, P-GW IP, APN, Subscribed Profile, ECGI, TAI).

[S-GW → P-GW] Demande de création de session EPS :

La S-GW et la P-GW communiquent sur l'interface S5 sur le plan usager, utilisant le protocole GTP (GTP-U).La S-GW alloue un identifiant de tunnel GTP sur l'interface S5 en liaison descendante S5 TEID (S5 S-GW TEID) pour établir un tunnel S5 GTP à la P-GW indiquée dans le message **Create Session Request**. Ensuite, elle envoie à la P-GW l'identifiant ainsi que d'autres paramètres, inclus dans le message **Create Session Request**.

[S5 Bearer:Downlink] :

Une fois que l'étape précédente terminée, le downlink S5 GTP-U est crée. Ci-dessous les étapes d'établissement du bearer S1 sont décrites.

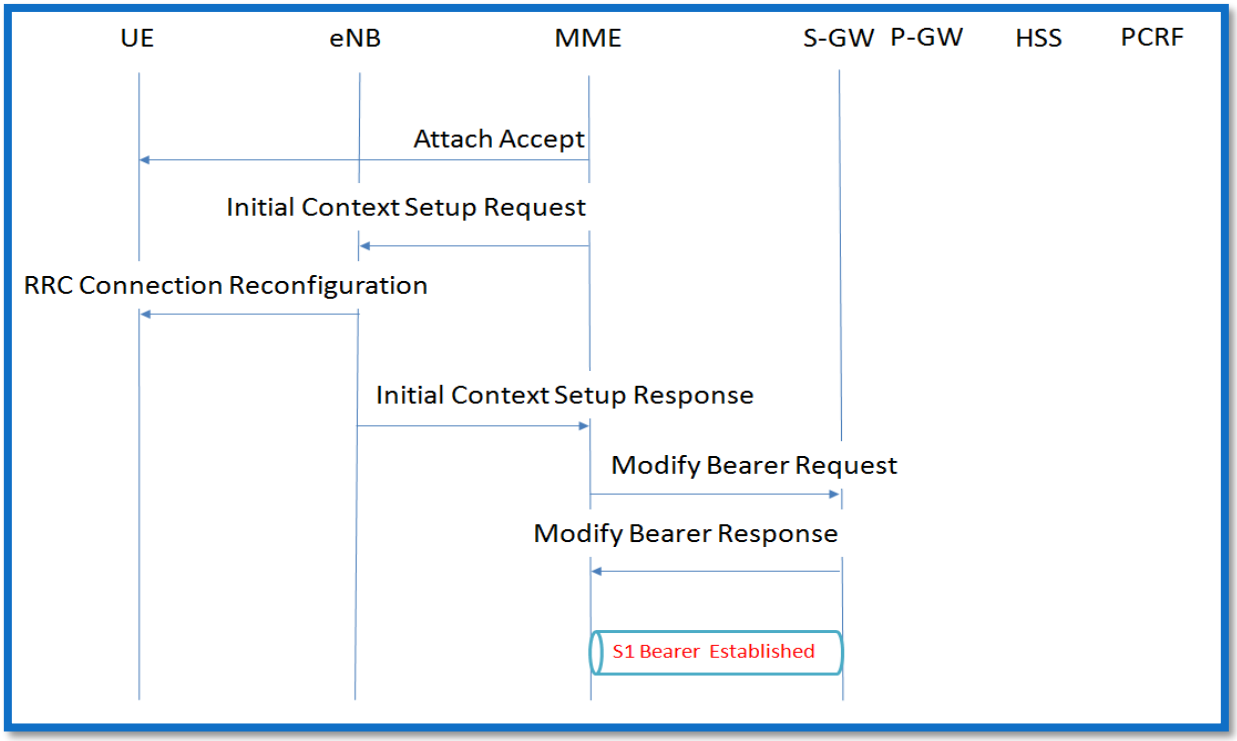

Figure 2.12 Procédure d'établissement d'une session EPS (2)

[P-GW] Allocation d'adresse IP pour l'utilisateur :

La P-GW, à la réception du message **Create Session Request**, réalise que l'usager tente d'accéder au réseau. Elle alloue donc une adresse IP à l'UE pour qu'il puisse se connecter à un APN. A partir d'un serveur DHCP interne. IL est aussi possible d'utiliser un serveur DHCP externe que la P-GW interrogera pour recevoir l'adresse IP.

[P-GW → PCRF] Notification de configuration de Session EPS :

La P-GW et le PCRF communiquent via l'interface Gx utilisant le protocole Diameter. Durant la création d'une session EPS pour l'utilisateur, l'allocation des ressources et le contrôle de QoS pour l'utilisateur doivent se faire en se basant sur les services que propose

la souscription. C'est le PCRF qui prend en charge les politiques de contrôle concernant tous les usagers ayant l'accès au réseau. Ainsi la P-GW fournit au PCRF les informations des souscriptions de chaque utilisateur, et obtient donc les autorisations du PCRF pour l'allocation des ressources tout en étant en accord avec les politiques du réseau de l'opérateur. A partir des informations de l'abonnement de l'utilisateur reçues de la MME, la P-GW rassemble les informations requises pour que le PCRF puisse prendre des décisions imposées par la politique de l'opérateur, elle les envoie donc au PCRF sur le message **CCR (CC-Request**).

CCR (IMSI, UE IP, PDN ID (APN), Subscribed QoS Profile (QCI, ARP, APN-AMBR(UL/DL), ECGI, TAI).

[P-GW ← PCRF] Accorde l'établissement de la session EPS :

Le PCRF délivre à la P-GW les règles **PCC** (Policies and Charging Conrtrol) encapsulées dans le message **CCA (CC-Answer)**.

Voici un exemple de message **CCA** :
CCA (IMSI, PCC Rule (SDF Filter, QCI, ARP, APN-AMBR (UL/DL), Charging=Offline, Change Reporting Action (Start Reporting ECGI, TAI)).

PCC Rule : c'est les règles de charging et de contrôle
SDF Filter :c'est un filtre de session de flux de données
Change Reporting Action : permet la mise à jour de localisation

[S-GW ← P-GW] Réponse de création de Session EPS :

La P-GW alloue un identifiant de tunnel GTP sur l'interface S5 en liaison montante (Uplink S5 TEID) ou (S5 P-GW TEID) pour l'établissement d'un S5 GTP à la S-GW. La P-GW répond donc à la S-GW un message **Create Session Response** en incluant dedans le S5P-GW TEID et le profile de QoS à appliquer au bearer EPS (S5 Bearer).

[MME ← S-GW] Réponse de création de Session EPS :

Après avoir reçu le **Create Session Response** message, la S-GW prend l'Uplink S5 TEID (S5 P - GW TEID) qui sera utilisé pour le trafic de liaison montante, et alloue unuplink S1 TEID (S1 S-GW TEID) pour le tunnel S1-GTP qui sera utilisé pour le S1 bearer. Après le traitement du message, la S-GW ajoute au message traité le S1 S-GW TEID alloué précédemment et l'envoie ensuite au MME comme message de réponse au message **Create Session Request.**

[UE ← MME] Accepte la liaison :

Le MME envoie un message **AttachAccept** à l'UE incluant dedans les informations telles que : l'adresse IP de l'UE allouée par la P-GW, le GUTI (identifiant temporaire pour l'UE), liste TAI (Tracking Area Identifier), identifiant de bearer EPS (EPS Bearer ID), la valeur

UE-AMBR (Aggregate Maximum Bit Rate), et les paramètres de QoS reçus de la S-GW. Ce message est inclus dans l'**Initial Context Setup Request** sur la connexion de signalisation S1 puis dans le message **RRC Connection Reconfiguration** sur la connexion RRC.

[eNB← MME] Demande de configuration E-RAB (E-UTRAN Radion Access Bearer) :

Le MME envoie l'**Initial Context Setup Request** pour que l'eNB puisse établir un bearer S1 avec la S-GW et un DRB (Data Radio Bearer) avec l'UE. Le message **Initial Context Setup Request** est constitué de :

Initial Context Setup Request (UE-AMBR (UL/DL),E-RAB ID, E-RAB QoS (QCI, ARP), S1 S-GW TEID, K_{eNB}, UE Security Algorithm, NAS-PDU).

[UE ←eNB] Reconfiguration de connexion RRC :

L'eNB alloue les identifiants uplink/downllink des DRB et configure les paramètres de QoSdu E-RAB afin d'établir un DBR et un bearer EPS sur la liaison radio. Ensuite elle envoie le message de reconfiguration **RRC Connection Reconfiguration** à l'UE sur la connexion RRC sécurisée. La connexion RRC est déjà établie auparavant quand l'UE a envoyé l'**Attach Request** au réseau. Suite à l'autorisation à l'UE d'accéder au réseau, il doit être reconfiguré puisqu'il a besoin de configurer les paramètres en fonction des ressources allouée par le réseau. La couche RRC de l'UE alloue les ressources radio en se basant sur les paramètres de configurations obtenus à partir du **RRC Connection Reconfiguration**, ensuite elle retire de se message l'**Attach Accept** et l'envoie à la couche NAS.
Une fois que la couche NAS de l'UE reçoit l'**Attach Accept**, elle obtient l'adresse IP pour l'UE et le GUTI, et l'utilise pour une future communication.

[eNB→ S-GW] Réponse de configuration E-RAB :

L'eNB alloue une liaison descendante S1 TEID (S1 eNB TEID) pour un bearer S1. Ensuite elle inclut l'identifiant dans le message **Initial Context Setup Response** et l'envoie au MME comme réponse au message **Initial Context Setup Request**, le MME peut désormais l'envoyer à la S-GW.

[MME → S-GW] Demande de modification de Bearer S1 :

Le MME envoie le Downlink S1 TEID (S1 eNB TEID) reçu de l'eNB pour la S-GW sur le message **Modify Bearer Request**.

[MME ← S-GW] Réponse à la demande de modification de bearer S1 :

La S-GW envoie au MME un message **Modify Bearer Response**, la S-GW est prête pour délivrer le trafic downlink S1.

[S1 Bearer:Downlink] : configuration de bearer S1 terminée :

Avec l'établissement du bearer S1 l'eNB et la S-GW peuvent s'échanger le trafic entre eux. Maintenant le bearer EPS de l'UE à la P-GW est enfin établi, allouant les ressources **réseau/radio**, uplink/downlink pour les communications entre l'UE et la P-GW.

2.6 Conclusion :

A l'issu de ce chapitre on a pu passer en revue les différentes étapes de développement qu'a connu la téléphonie mobile. On a étudié les différentes générations des réseaux mobiles en passants du mode analogique au mode circuit numérique, ensuite au mode paquet.

On a aussi vu comment les objets peuvent communiquer entres eux et comment les piloter à distance grâce à Internet.

En fin, on a étudié en détail l'architecture EPC d'un réseau 4G, notamment les nœuds et les interfaces standard constituant le réseau cœur, et expliqué les différentes procédures permettant l'établissement d'un bearer EPS.

3 La virtualisation dans les réseaux

3.1 Introduction :

La virtualisation consiste à découper le matériel du logiciel. La virtualisation a eu lieu déjà dans le monde informatique il y a quelques années et commence à se concrétiser dans les réseaux télécoms avec des déploiements commerciaux qui sont entrain de se mettre en place.

Dans ce chapitre nous allons introduire les éléments qui ont permis l'arrivé de la nouvelle génération de réseaux à savoir les réseaux logiciels. Ces éléments se caractérisent par le Cloud, SDN (Software-Defined Networking) et enfin la virtualisation des fonctions réseaux qui a pour nom NFV (Network Function Virtualization). Ces technologies représentent le symbole des réseaux d'aujourd'hui et de demain.

3.2 Définition de la virtualisation :

La virtualisation est un mécanisme informatique qui nous permet de faire fonctionner sur une même machine physique plusieurs systèmes, serveurs ou applications comme s'ils fonctionnaient sur des machines physiques distinctes. Comme on le voit à la figure 3.1.

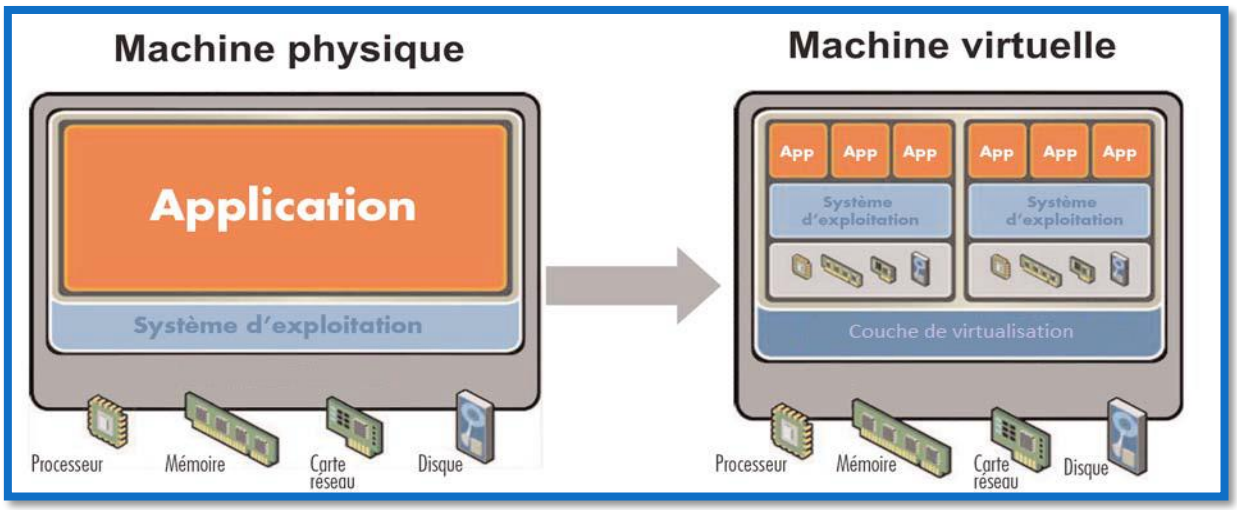

Figure 3.1 Concept de la virtualisation [10]

La virtualisation repose sur le mécanisme suivant :

- Un système d'exploitation principal appelé « système hôte » est installé sur un serveur physique unique. Ce système sert d'accueil à d'autres systèmes d'exploitation.

- Un logiciel de virtualisation appelé « hyperviseur » est installé sur le système d'exploitation principal. Il permet la création d'environnements clos et indépendants sur lesquels seront installés d'autres systèmes d'exploitation « systèmes invités ». Ces environnements sont des « machines virtuelles ».

- Un système invité est installé dans une machine virtuelle qui fonctionne indépendamment des autres systèmes invités dans d'autres machines virtuelles. Chaque machine virtuelle dispose d'un accès aux ressources du serveur physique (mémoire, espace disque, CPU…) qui sont allouées dynamiquement par l'Hyperviseur.

La virtualisation consiste à virtualiser complètement l'environnement matériel c'est-à-dire, mettre le processeur, la mémoire vive, le disque dur, le réseau et les divers autres périphériques d'entrées/sorties au sein d'une machine virtuelle pour qu'elle puisse accueillir un système d'exploitation au complet.

Une machine virtuelle se comporte donc comme un ordinateur physique et contient ses propres ressources qui sont alors virtuelles (basées sur du logiciel).
L'autonomie de chaque machine virtuelle rend la solution complètement transparente pour l'utilisateur, toute action telle que le redémarrage ou installation d'application ne perturbent pas le fonctionnement des autres machines virtuelles en marche pour autant sur la même ressource physique.

3.2.1 Le rôle de la couche de virtualisation (hyperviseur) :

L'hyperviseur permet de supporter les fonctionnalités suivantes :

- Assure le contrôle du processeur et des ressources de la machine hôte.

- Alloue à chaque machine virtuelle les ressources dont elle a besoin.

- S'assure que les VM n'interfèrent pas l'une avec l'autre.

3.2.2 Type d'hyperviseur :

Il y a d'innombrables manières de placer des machines virtuelles sur des équipements matérielles. On peut les classer selon trois grandes catégories décrites aux figures 3.2, 3.3, et 3.4.

3.2.2.1 La paravirtualisation :

Un hyperviseur de type paravirtualisation appelé également *baremetal*, est un logiciel qui s'exécute directement sur une plate-forme matérielle. Cette plate-forme permet de supporter des systèmes d'exploitation invités avec leurs pilotes. On appelle

également ces logiciels des hyperviseurs de type 1. On retrouve plusieurs exemples sur le marché : VMware vSphere, VMware ESX, Microsoft Hyper-V Server, BareMetal et KVM.

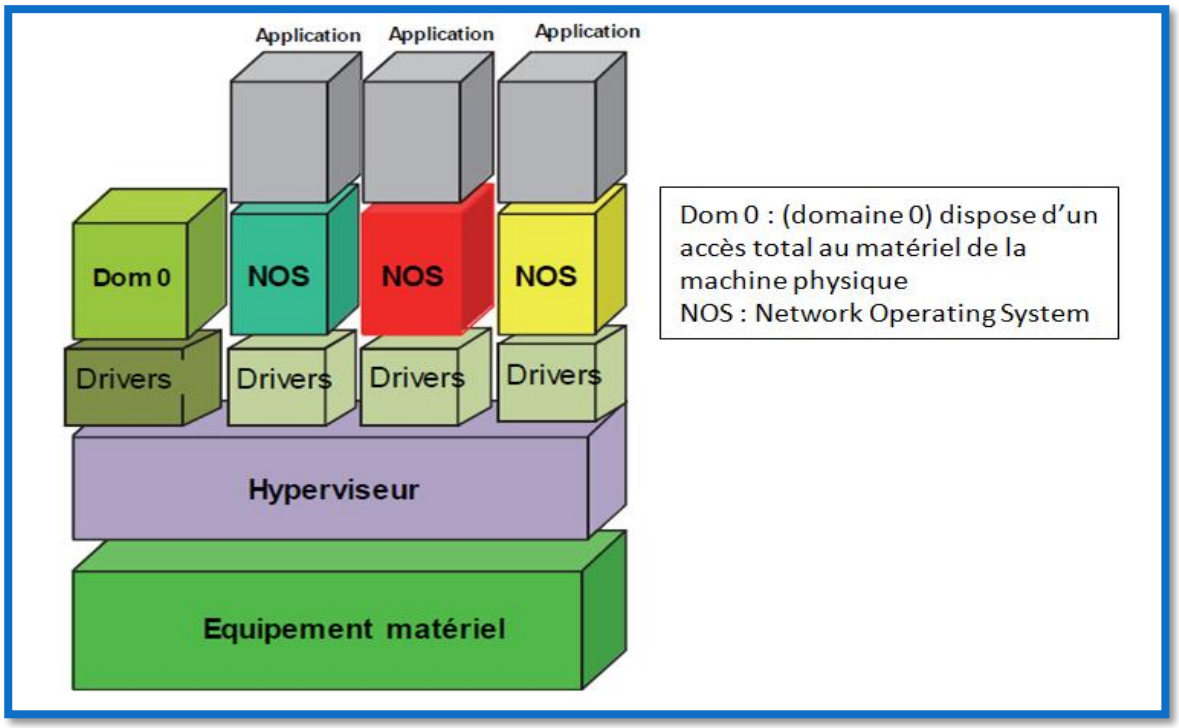

Figure 3.2 La Paravirtualisation [3]

3.2.2.2 La virtualisation par émulation :

Le type 2 d'hyperviseur, est un logiciel qui s'exécute à l'intérieure d'un autre système d'exploitation. Un système d'exploitation invité s'exécute au-dessus du matériel et demande un émulateur (logiciel qui va imiter le comportement physique du matériel) pour s'exécuter sur le système d'exploitation de l'hôte. On peut citer les exemples suivants : Microsoft VirtualPC, VMware Fusion, Parallels Desktop, Oracle VM VirtualBox.

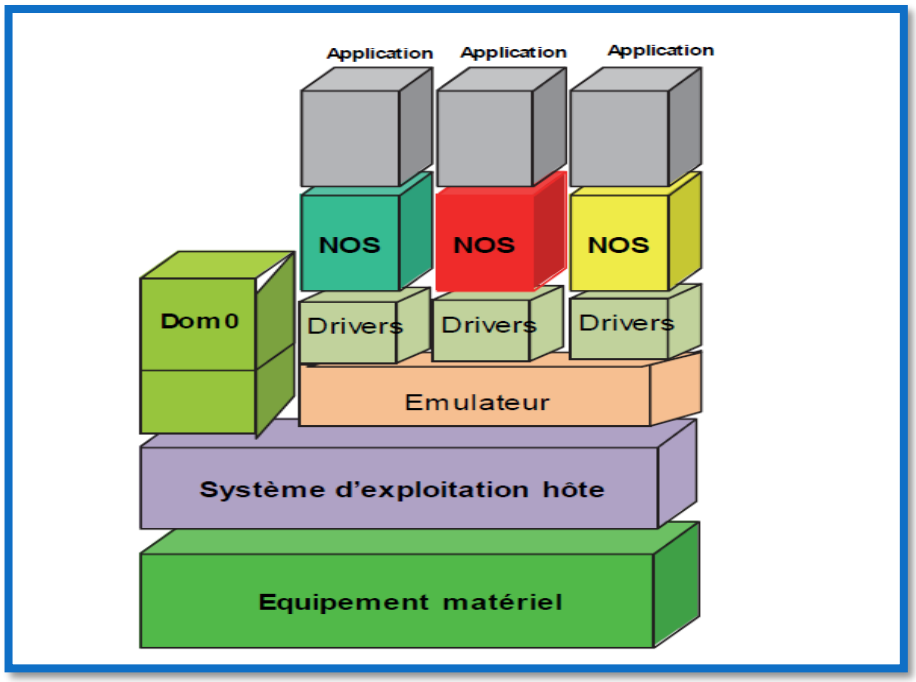

Figure 3.3 Virtualisation par émulation [3]

3.2.2.3 La virtualisation par zone d'exécution

Le troisième type s'éloigne des systèmes d'hypervision précédents pour faire tourner plusieurs machines simultanément. On parle plutôt d'isolateur. Un isolateur est un logiciel qui permet d'isoler l'exécution des applications dans un environnement appelé contexte ou zone d'exécution. Cette solution est très performante car elle n'introduit pas de surcharge mais les environnements sont plus difficiles à isoler. Dans cette catégorie on peut citer Linux-Vserver, BSD Jail, Open VZ.

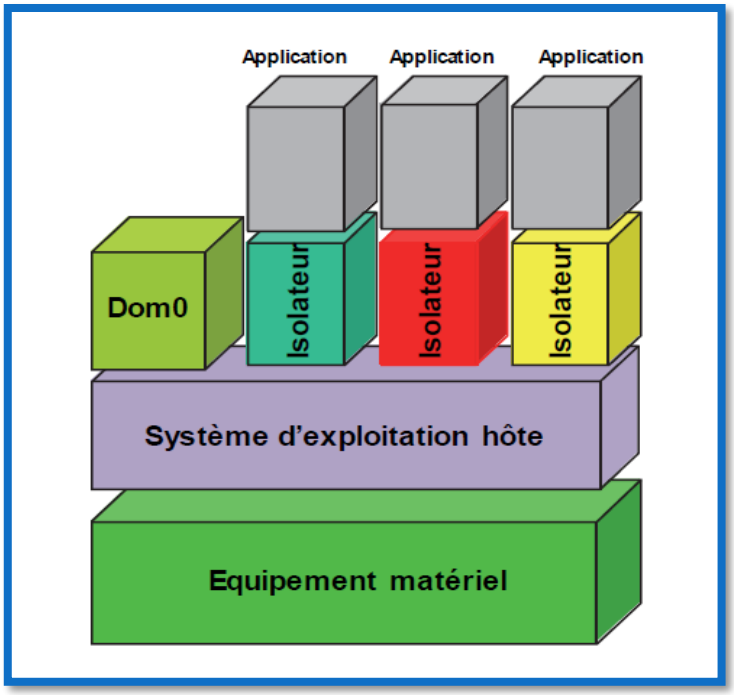

Figure 3.4 Virtualisation par zone d'exécution [3]

3.2.3 Avantages de la virtualisation :

La virtualisation offre une multitude d'avantages voici quelque uns :

- Possibilité de faire tourner sur un même serveur plusieurs application diverses
- Rationalisation des coûts de matériels informatiques
- Possibilité d'installer plusieurs systèmes (Windows, Linux) sur une même machine
- Portabilité des serveurs : une machine virtuelle peut être déplacée d'un serveur physique vers un autre (lorsque celle-ci a, par exemple, besoin davantage de ressources)
- Accélération des déploiements de systèmes et d'applications en entreprise
- Administration simplifiée de l'ensemble des serveurs
- Réduction de la facture d'électricité, en diminuant le nombre de serveurs physiques
- Disponibilité des services en tout temps même lors de maintenance (migration des VM).

3.3 Les réseaux logiciels :

La réalisation de réseaux logiciels (virtuels) se fait à l'aide des machines virtuelles. Pour cela il faut les interconnecter comme on l'aurait fait pour des machines physiques. Il faut ainsi partager les circuits de communications entre les multiples réseaux logiciels. La figure 3.5 représente un ensemble de réseaux logiciels bâtit sur un seul et unique réseau physique.

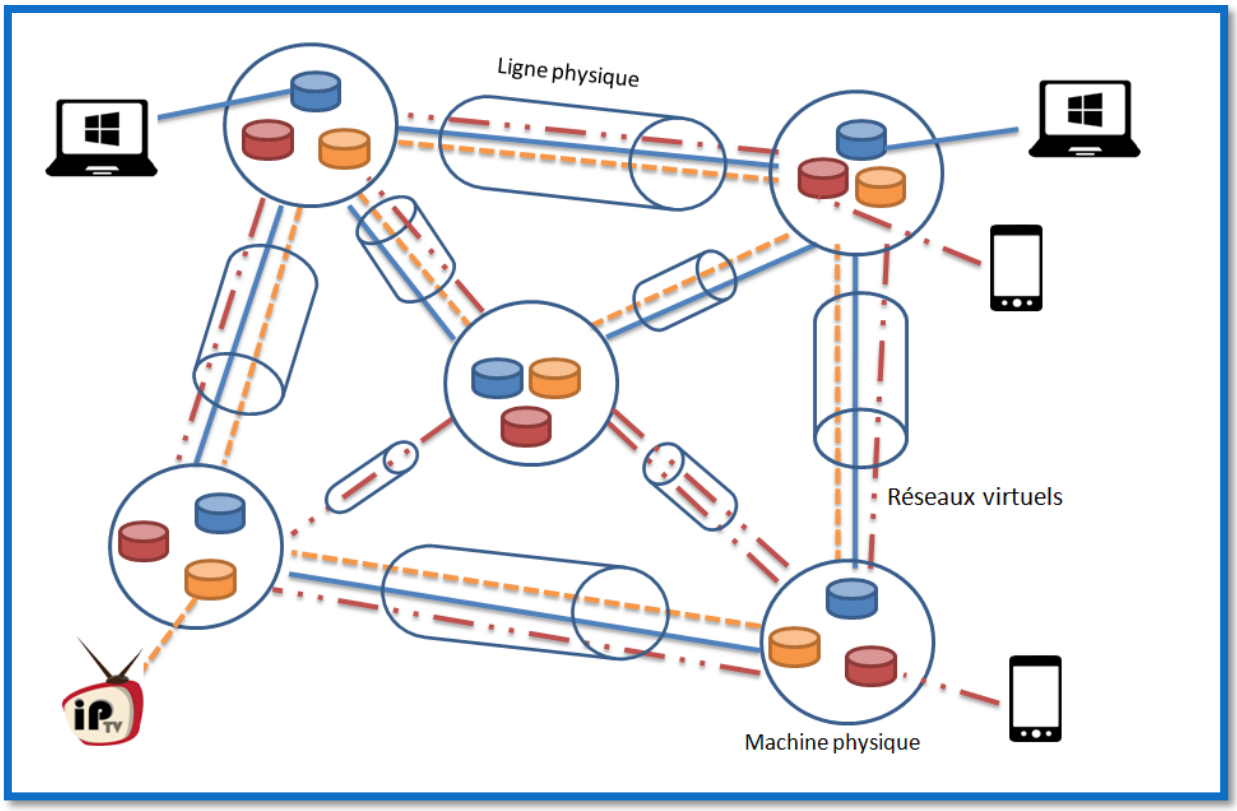

Figure 3.5 Réseaux logiciels sur un seul réseau physique

Chaque réseau virtuel peut avoir ses propres caractéristiques et sa propre architecture. Un réseau logiciel peut être destiné à un service ou une application particulière, par exemple un réseau logiciel dévolu à un service de VoIP (Voice over IP) réseau en rouge sur la figure ci-dessus, un autre à de la IP-TV, réseau en orange sur la figure, et un troisième réseau pour le transport de données, réseau en bleu. De manière générale on peut faire un réseau logiciel pour chaque utilisateur. Le réseau logiciel est créé au moment ou l'utilisateur se connecte et il est détruit lorsqu'il se retire. Mais aujourd'hui on se limite à un nombre de réseaux logiciels compatibles avec la capacité du matérielle de l'infrastructure physique sous-jacente. Chaque réseau virtuel se voit allouer des ressources en fonctions des demandes et des droits des utilisateurs.

Les nœuds virtuels qui sont à la base de la constitution des réseaux logiciels, se trouvent dans des datacenters qui peuvent être plus ou moins importants : cela va des gros datacenters centraux aux petits datacenters (femto-datacenters) en passant par d'autres tailles intermédiaires.

Un des avantages de ces réseaux est de pouvoir faire migrer des machines virtuelles d'un équipement physique à un autre et d'un datacenter à un autre, car on est désormais sur du logiciel. La migration peut être automatisée si par exemple un nœud de transfert est surchargé, montre des signes de faiblesse ou bien tombe en panne. En réalité lorsqu'on réalise la migration d'un nœud, on ne procède pas au transport de tout le code de la machine, ce qui serait un peu lourd dans certains cas. En général, le logiciel à transporter se trouve déjà présent dans le nœud distant mais il est dans un état de veille. Il suffit de mettre

en route le logiciel et de lui envoyer la configuration du nœud à déplacer. Cela demande que peu de données à transférer et une latence faible avant l'ouverture de la machine migrée.

L'isolation est une propriété importante que doivent posséder ces réseaux, il ne faut pas qu'un problème sur un réseau logiciel puisse entacher les autres réseaux. L'isolation est complexe, car il faut à la fois partager les ressources communes et être sûr que chaque réseau ait à tout moment l'accès à ses propres ressources.

3.3.1 Equipements virtuels :

Pratiquement tous les équipements peuvent être virtualisés à l'exception de ceux qui doivent prendre en charge la réception de signaux (électromagnétiques, pression atmosphérique, température …). Par exemple une antenne ou un thermomètre ne peuvent pas être remplacés par un logiciel. Mais toute la partie qui concerne le traitement de signal peut être gérée dans une machine virtuelle.

Tous les équipements des réseaux sont virtualisés ou en cours de virtualisation, que ce soit la partie traitement des Node-B des réseaux mobile 3, 4 et dans pas longtemps 5G, les bases de données HLR, VLR, HSS, les routeurs, commutateurs, firewalls, load balancer etc. De plus, ces machines peuvent être partitionnées pour s'exécuter sur plusieurs machines en parallèle.

C'est ici qu'on voit toute l'importance des datacenters qui forment le Cloud puisque ce sont des environnements où la puissance de traitement est disponible avec un vaste espace de stockage pour les machines virtuelles et tout un ensemble d'informations liées aux réseaux, aux clients et aux algorithmes de traitement.

3.4 Le Cloud :

Littéralement le Cloud est un ensemble de ressources (ordinateurs centraux, serveurs, baie de stockage, équipements de réseaux et de télécommunication, etc.) que l'on déplace de l'entreprise ou du particulier vers Internet. En effet, on rassemble les ressources dans des centres de données ou datacenters, on parle alors de délocalisation de ressources. Il s'agit de déporter sur un serveur éloigné, le traitement informatique qui jusqu'ici s'effectue sur la machine de l'utilisateur ou du moins sur le serveur de l'entreprise. C'est une évolution majeure de l'informatique qui fait que les utilisateurs ou les entreprises ne sont plus gérants de leurs serveurs informatiques. Ils accèdent de façon souple et évolutive à de nombreux services en ligne sans avoir à gérer l'infrastructure. Les données de l'entreprise et les logiciels sont déportés de l'ordinateur vers le serveur distant, on ne sait où, d'où l'expression "dans le nuage". [12]

Figure 3.6 Le Cloud [11]

L'avantage du Cloud provient de la puissance des datacenters qui permettent de prendre en charge un grand nombre de machines virtuelles et de leur donner la puissance nécessaire à leurs exécutions. Les datacenters vont servir de base pour les réseaux logiciels et le support des machines virtuelles pour les créer. C'est ce qui a poussé de nombreux opérateurs de télécommunications à créer des sociétés qui fournissent des services Cloud pour eux-mêmes et également pour leurs clients.

3.4.1 Catégories de Cloud :

Le monde du Cloud est assez divers, par rapport aux multitudes de fonctionnalités qu'il peut apporter. On retrouve trois catégories principales de Cloud comme le montre la figure 3.7.

- Le Cloud SaaS (Software as a Service)
- Le Cloud PaaS (Platform as a Service)
- Le Cloud IaaS (Infrastructure as a Service).

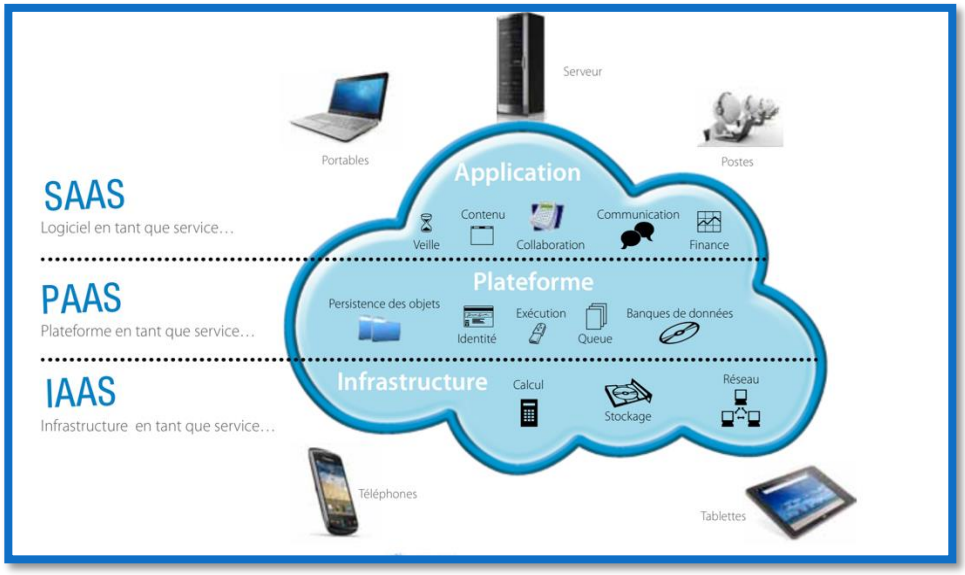

Figure 3.7 Les trois principales catégories de Cloud [12]

La première solution, le SaaS (Software as a Service) appelé également le Cloud Computing, offre le plus de potentiel, en effet il met à diposition tous les services à l'utilsateur que ce soit du calcul, du stockage ou du réseau. De façon plus précise, le SaaS permet au fournisseur de Cloud de proposer en plus de l'infrastucture et de la plate-forme, les applications elles-mêmes. Il ne reste plus rien dans l'entreprise, si ce n'est que les términaux permettant l'accès à Internet. Notamment cette solution extériorise pratiquement l'ensemble de ressources de l'entrepise.

La deuxième soluton ou le PaaS (Platform as a Service), laisse les applications à l'initiative de la société. Le fournisseur de Cloud propose une plate-forme complète et ne laisse à l'entreprise que la gestion des applications. Notamment les serveurs de l'entreprise ne prennent en compte que les applications.

Enfin, la troisième solution IaaS (Infrastructure as a Service), laissant nettement plus d'initiatives à l'entreprise. Dans ce cas le fournisseur offre toujours le stockage, le calcul et le réseau mais laisse à la société le choix des applications et les environnements nécessaires aux applications tels que les systèmes d'exploitation et les bases de données. [3]

Pour comprendre plus les fonctions des différents types de Clouds, la figure ci-dessous compare ces catégories au model classique que l'on trouve souvent aujourd'hui.

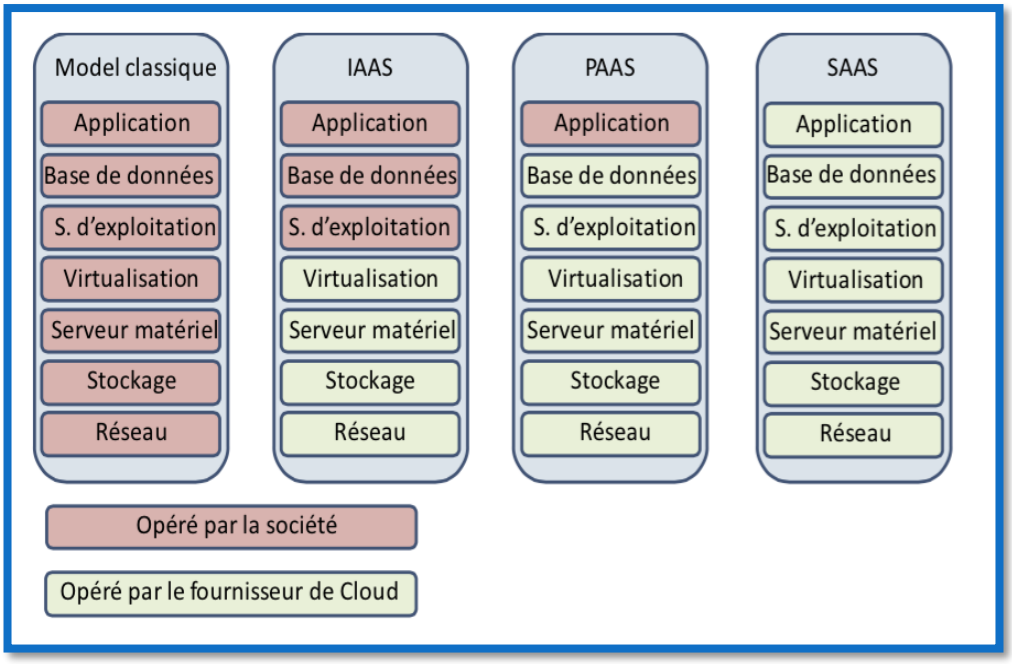

Figure 3.8 Les différents types de Clouds [3]

Le problème majeur que craignent les entreprises est la sécurité. En effet, rien n'empêche les fournisseurs de Cloud d'aller jeter un cout d'œil aux données de leurs clients ou encore plus les intercepter. Pour palier ce problème, des Clouds de sécurité sont nécessaires, on les appelle aussi les Clouds souverains, de quoi rassurer les clients et gagner un peu plus leurs confiances.

Les Clouds souverains contiennent de nombreuse machines virtuelles de sécurité comme des serveurs d'authentification, des serveurs d'autorisation, on peut trouver également des firewalls, des DPI (Deep Packet Inspection) etc.

L'une des techniques que l'on verra dans la suite est le SDN (Software-Defined Networking), qui permet de définir plusieurs tables de transferts, et seule la puissance des datacenters sera capable de faire tous les calculs nécessaires.

3.5 Le SDN (Software-Defined Networking) :

Le SDN (Software-Defined Networking) est une approche du réseau dans laquelle le contrôle est séparé du matériel et transféré vers une application logicielle appelé contrôleur. Le SDN isole l'infrastructure sous-jacente du réseau afin de pouvoir la traiter comme une entité logique ou virtuelle. Jusqu'à présent les tables de transfert étaient calculé de façon distribuée dans chaque équipement de type routeur ou commutateur, mais désormais avec cette nouvelle architecture les plans de contrôle et de transfert du réseau sont séparés pour pouvoir optimiser chacun d'eux plus facilement et offrir une vue centralisée sur le réseau distribué.

3.5.1 Objectif du SDN:

L'objectif du SDN est d'abaisser les coûts par la virtualisation, l'automatisation, et la simplification. Pour atteindre ces objectifs le SDN permet une personnalisation des réseaux, un temps de mise en route très court et un déploiement du réseau avec la bonne qualité de service et non pas une qualité de service générale.

3.5.2 Architecture du SDN :

Aujourd'hui, pour constituer un système d'information et d'opération complet pour une entreprise il faut mettre en place cinq domaines essentiels à savoir : le stockage, le calcul, le réseau, la gestion et le contrôle et enfin la sécurité. Ces domaines peuvent se mettre en place par l'intermédiaire de machines virtuelles associées à chacun des domaines. L'environnement d'information et d'opération peut donc être contenu dans le Cloud sous forme de VMs distribuées dans des datacenters.

On ajoute à l'environnement des applications qui peuvent être de deux types : applications business et des applications qui permettent le pilotage ou l'orchestration de l'environnement lui-même. La figure 3.9 résume l'environnement complet de l'architecture générale des systèmes d'informations et d'opérations des entreprises.

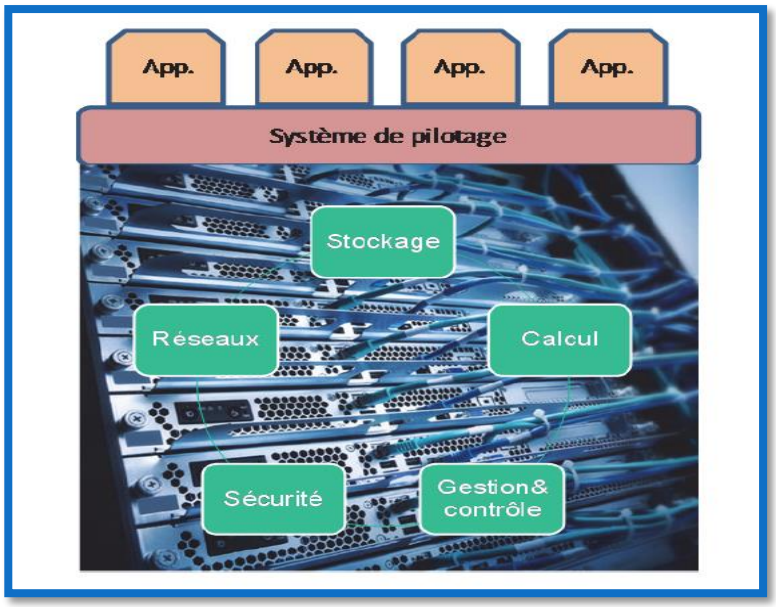

Figure 3.9 Environnement complet d'un système d'information et d'opération [3]

3.5.3 Architecture ONF (Open Network Foundation) :

L'ONF a été chargé de la normalisation de l'architecture SDN. L'architecture proposée par l'ONF est composée de trois couches comme le décrit la figure 3.10.

- La couche la plus basse ou le ***plan infrastructure*** : cette couche permet de découpler le hardware du software et se charge du transport de données. Elle comporte les algorithmes et les protocoles qui permettent aux paquets IP d'avancer dans le réseau.

- La deuxième couche ou le ***plan de contrôle*** : ce plan contient les contrôleurs qui donnent des ordres au plan de données pour que l'acheminement des paquets se fasse au mieux. Cette architecture permet de centraliser le contrôle pour permettre la récupération de nombreuses informations sur tous les abonnés et d'obtenir une sorte d'intelligence. Les contrôleurs se répartissent les infrastructures à prendre en charge, ils opèrent sur un ensemble de fonctions comme le provisionnement de l'infrastructure, la répartition ou non de charge sur les différents équipements du réseau.

- La couche supérieure ou ***plan application*** : ce plan est responsable des applications nécessaires et de leurs exigences en matière de réseau, de stockage, de calcul, de sécurité et de gestion. Cette couche introduit la programmabilité des applications et permet de faire descendre vers le contrôleur tous les éléments nécessaires pour la mise en place du réseau logiciel personnalisé aux besoins des applications (actions réalisés par l'orchestrateur). Tout nouveau service peut être introduit rapidement et donnera naissance à un réseau spécifique s'il ne peut pas s'implémenter sur un réseau déjà existant.

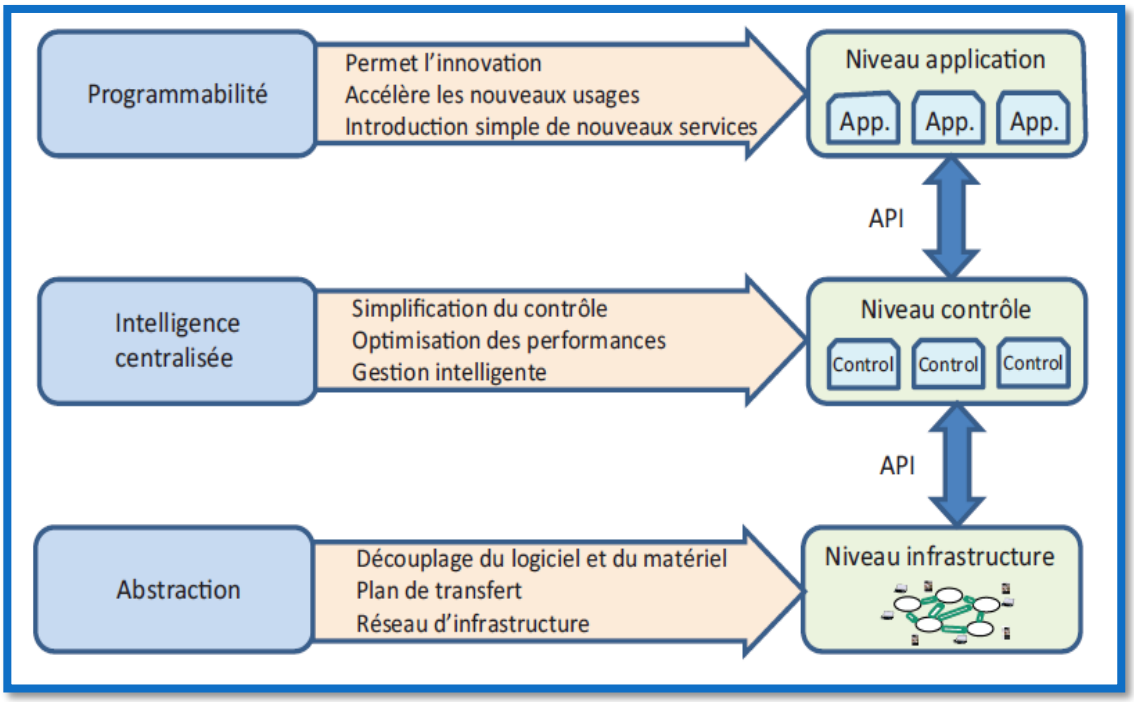

Figure 3.10 Architecture de l'ONF [3]

On va désormais voir l'architecture SDN plus en détail comme le montre la figure 3.11.

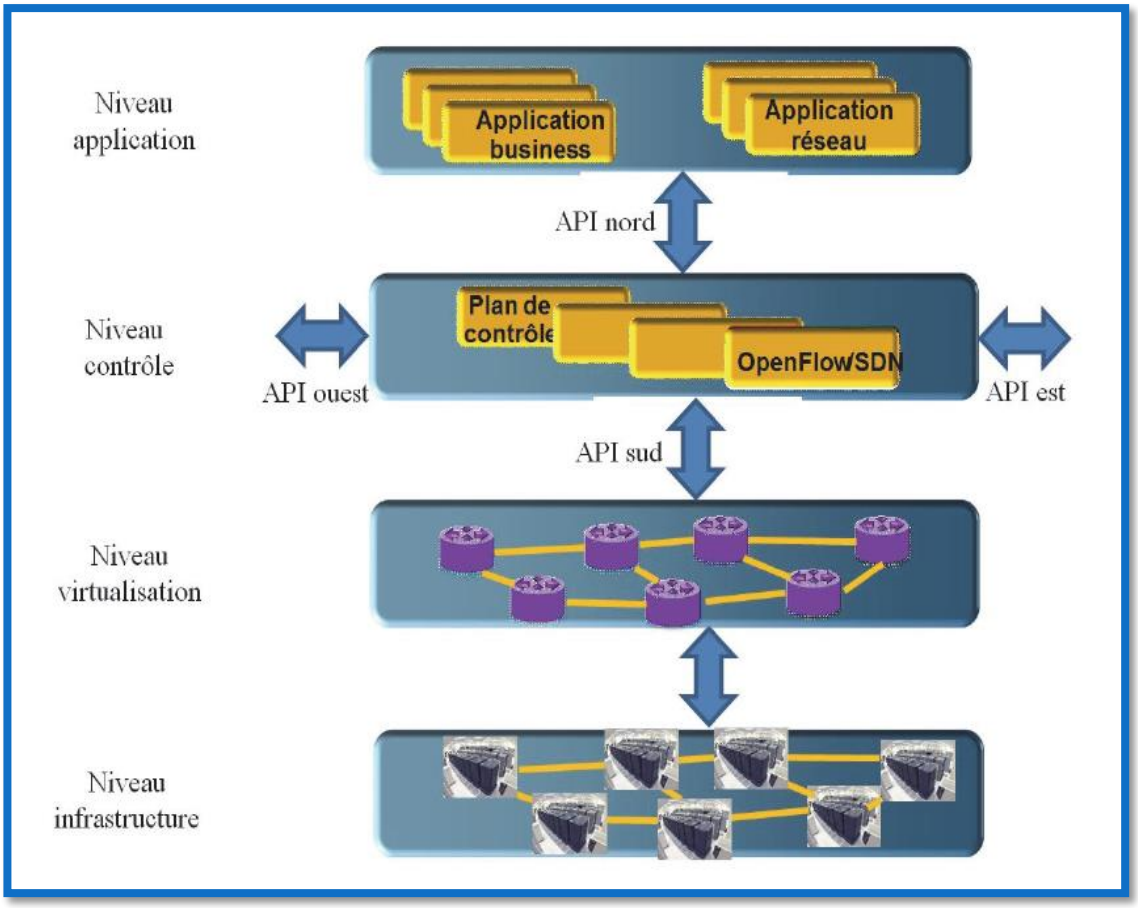

Figure 3.11 Architecture SDN [3]

Le niveau infrastructure est partagé en deux plans, le plan physique et plan logique. Le plan physique se charge de l'ensemble des équipements matériels de manière générale de l'infrastructure physique pour réaliser un réseau. Le plan logique concerne la mise en place des réseaux logiciels construits à base de machines virtuelles et se partageant l'infrastructure physique suivant des règles qui proviennent des couches supérieures.

Dans l'architecture présentée à la figure 3.11 on retrouve les trois couches cité un peu plus haut, ces couches communiquent entre elle via des interfaces appelées API (Application Programming Interface) elles sont au nombre de quatre : API nord (northbound), sud (southbound), est (eastbound) et ouest (westbound).

L'interface nord permet la communication entre le niveau applicatif et le contrôleur. Elle a pour objectif de décrire les besoins de l'application et de faire passer les commandes pour orchestrer le réseau. L'interface sud décrit la signalisation nécessaire entre le plan de contrôle et la couche de virtualisation. Pour cela il faut que le contrôleur puisse déterminer les éléments qui formeront le réseau logiciel dont il s'occupe. Dans l'autre sens, les statistiques d'occupations des ressources du réseau doivent être remontées pour que le contrôleur ait une vue la plus complète possible de l'utilisation des ressources. Les interfaces est et ouest permettent la communication entre les contrôleurs pour prendre des décisions ensemble.

L'interface sud est souvent connue au travers du terme OpenFlow, qui est une signalisation entre l'infrastructure et le contrôleur. C'est un protocole permettant le transport des informations qui définissent proprement le flot dont il est question pour lui ouvrir, modifier ou fermer le chemin associé. OpenFlow détermine également les actions à exécuter dans un sens ou dans l'autre de l'interface. Enfin, il permet la remontée d'informations de type mesures effectuées sur les différents ports de communications pour que le contrôleur ait une vue précise du réseau.

Le contrôleur a pour objectif de contrôler le plan de données et de recevoir du plan applicatif les éléments nécessaires pour déterminer le contrôle à exercer. Le contrôleur doit donc recevoir des règles de politiques à respecter et en partant de la description des applications à prendre en compte, il en déduit les actions à exercer sur les équipements de réseau. Les actions peuvent s'exécuter sur des routeurs, des commutateurs, des firewalls, des équilibreurs de charge, des VPN virtuels et d'autres équipements physiques.

Le contrôleur contient des modules prenant en charge différentes fonctions nécessaires à la bonne marche du réseau. Parmi ces fonctions, une des plus importantes correspond à l'équilibreur de charge (load balancer). C'est un ensemble d'algorithmes déterminant les meilleurs chemins à suivre dans le plan de données, il doit décider, en fonction des statistiques reçues, des nœuds de l'infrastructure de réseau par lesquels doivent transiter les paquets. Ce choix doit optimiser les demandes utilisateurs ou plus précisément les applications des utilisateurs.

Le plan applicatif est essentiellement formé de Clouds qui retiennent les machines virtuelles applicatives. Ces machines peuvent être de type business ou de type gestion d'éléments réseau comme la gestion des handovers ou la détermination du meilleur accès, à tout moment, pour un terminal. Dans cette couche se trouve essentiellement les systèmes d'exploitation de Cloud.

Pour résumer, les parties hautes et basses concernent le Cloud et les réseaux physiques et logiques. Entre ces deux niveaux, la gestion et le contrôle du réseau et des applications doivent être mis en place. Du coté application business, on retrouve les ensembles de modules de logiciels permettant de déployer des infrastructures de Cloud Computing (IaaS). De l'autre coté, on trouve les applications de mise en place de structure virtualisée de réseau avec les commandes nécessaire pour prendre en charge les applications business.

3.6 La virtualisation des fonctions réseaux NFV :

La virtualisation des fonctions réseau (Network FunctionsVirtualization) est une initiative destinée à virtualiser des fonctions réseau précédemment gérées par du matériel dédié. C'est une nouvelle façon de concevoir, déployer et gérer les services réseau, le NFV dissocie les fonctions réseau des systèmes matériels propriétaires, pour les exécuter au niveau du logiciel.

Le NFV exploite les technologies de virtualisation d'entreprise standard pour consolider de nombreux types d'équipement réseau sur des serveurs, des commutateurs et des systèmes de stockage standards. Elle réduit de ce fait le matériel, l'alimentation et les besoins d'espace du data center.

3.6.1 Architecture fonctionnelle du NFV :

Cette architecture est constituée :

- d'une couche comprenant **les fonctions de réseau virtuelles** (Virtual Network Function) ;
- **d'une couche d'infrastructure** (calcul, stockage et réseau) dans laquelle les fonctions seront exécutées ;
- **une couche pour la gestion et l'orchestration**.

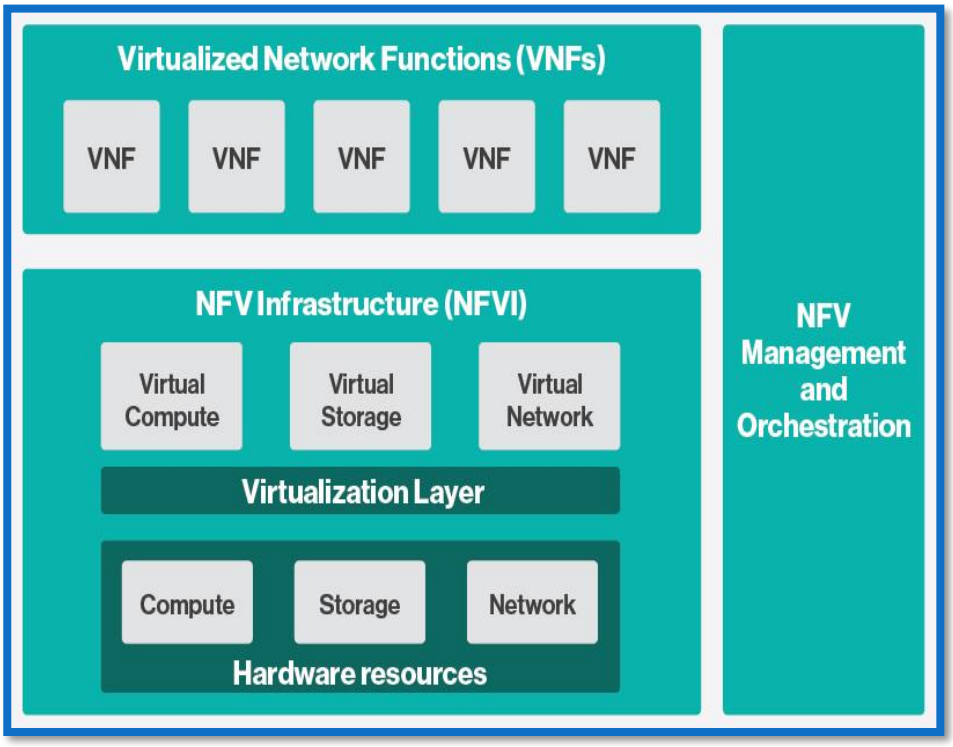

Figure 3.12 Architecture fonctionnelle du NFV [13]

Cette architecture permet le déploiement et l'exécution de fonctions réseau virtualisées (VNF) sur une infrastructure Cloud dénommée « NFV Infrastructure » (NFVI).

L'infrastructure NFVI est composée de ressources matérielles de base (pour le calcul, le stockage et la mise en réseau) qui sont partitionnées et partagées au moyen d'une couche logicielle de virtualisation. Cette couche logicielle peut par exemple correspondre à un hyperviseur, où une VNF pourra être déployée sur une seule machine virtuelle au sein du NFVI.

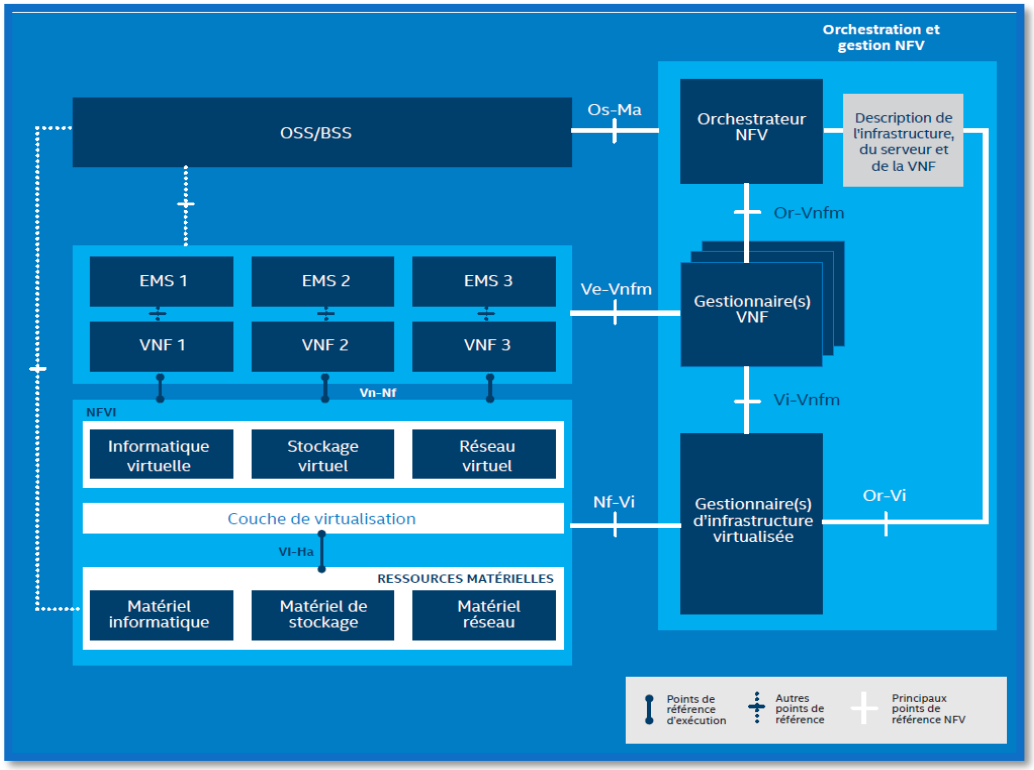

Figure 3.13 Les éléments constituants l'architecture NFV [14]

Le déploiement, l'exécution et l'exploitation des VNFs dans l'infrastructure NFVI sont pilotés par des fonctions de gestion et d'orchestration MANO (Management And Network Orchestration) comprenant :

- un orchestrateur NFV (NFVO) en charge du cycle de vie des services réseau ;
- un gestionnaire (VNFM) en charge du cycle de vie des VNFs ;
- un gestionnaire (VIM) en charge de la gestion des ressources du NFVI.

3.6.2 Eléments de l'architecture NFV [25] :

L'architecture NFV est constituée d'éléments suivants :

3.6.2.1 NFV Infrastructure (NFVI) :

Cet élément comprend l'ensemble des composants matériels (matériel informatique, stockage et matériel réseau) et logiciels (machines virtuelles) de l'environnement dans lequel les VNFs sont déployées, gérées et exécutées.

Pour une VNF la couche de virtualisation et les ressources matérielles ne forment qu'une seule entité qui leur fournit des ressources virtualisées nécessaires.

Cette architecture (NFVI) comprend trois couches qui sont les suivantes :

- **La couche matérielle (Hardware Resources) :** cette partie contient les différentes ressources matérielles nécessaires à l'exécution des fonctions réseau. On retrouve les ressources informatiques (serveurs, RAM…), les ressources de stockage (disque dur, NAS…) et les ressources réseau (routeurs, commutateur, firewall…).
- **La couche de virtualisation :** cette couche de virtualisation découple le logiciel du matériel. Elle permet ainsi au logiciel d'évoluer indépendamment du matériel. Elle alloue de façon dynamique les ressources matérielles aux différentes machines virtuelles.
- **Les ressources virtualisées :** elle comporte les ressources informatiques, de stockage et de réseau virtualisées pouvant être utilisée par les machines virtuelles.

3.6.2.2 Virtualized Network Functions (VNF) :

Cette couche contient les blocs de base (les fonctions réseau virtualisées) de l'architecture NFV. Une VNF est une fonction réseau qui est désormais virtualisée. Pour virtualiser une fonction réseau qui était autrefois représenté par du matériel, il suffit d'écrire un code qui effectue exactement ce que fait le matériel. Ainsi on passe du concret au logiciel.

Les VNFs peuvent être connectées ou être combiner entre elles pour offrir des services de communications réseau à grande échelle. C'est ce qu'on appelle le « Service Chaining »

Exemple de VNF : vRouter, vFirewall, vSGSN-MME, vEPG.

3.6.2.3 Element management system (EMS) :

Un EMS gère un ou plusieurs types spécifiques d'éléments réseaux de télécommunication. Typiquement, l'EMS gère les fonctions et les capacités au sein de chaque élément réseau mais ne gère pas le trafic entre ces éléments dans le réseau. Dans notre cas il gère différentes VNFs.

3.6.2.4 Management and Network Orchestration (MANO) :

Elle se compose de trois parties :

3.6.2.4.1 Virtualized Infrastructure Manager (VIM) :

Le gestionnaire d'infrastructure virtualisée comprend les fonctionnalités qui sont utilisées pour contrôler et gérer l'interaction des VNFs avec les différentes ressources informatique, de stockage et réseau, sous son autorité ainsi que leur virtualisation.

3.6.2.4.2 VNF Manager (VNFM) :

Il permet la gestion du cycle de vie des instances VNF, il est responsable de :

- L'initialisation
- La mise à jour
- Les tests (Query)
- La mise à l'échelle
- La résiliation (terminate).

Plusieurs VNFM peuvent être déployé pour gérer une ou un ensemble de VNFs.

3.6.2.4.3 L'orchestrateur :

Prend en charge le cycle de vie des services réseau, incluant :

- La gestion globale des ressources, la validation et l'autorisation des demandes de ressources de la part de la NFVI ;
- Politique de gestion des instances des services réseau ;
- Mesures et surveillance des performances KPI (Key Performance Indicator).

3.6.2.5 La couche OSS (Operations Support System)/BSS (Business Support System) :

L'OSS s'occupe da la:

- Gestion du réseau
- Gestion des pannes
- Gestion de la configuration
- Gestion des services.

Le BSS s'occupe de la :

- Gestion des abonnés
- Gestion des commandes
- Gestion de la facturation et des revenus.

Les plates-formes BSS et OSS sont liées dans le besoin d'appuyer différents services de bout en bout. Chaque domaine possède ses propres responsabilités liées aux données et aux services.

3.6.3 SDN et NFV :

Mutuellement bénéfiques, sans être dépendants, le SDN et le NFV partagent une approche basée sur le logiciel pour le support des réseaux plus évolutifs, agiles et innovants. Le SDN a cependant une portée plus vaste en matière de contrôle des flux de trafic et de gestion du réseau. Le NFV est plusse concentre sur la virtualisation et l'optimisation de fonctions et de services réseaux tels que les routeurs, les contrôleurs de distribution des applications, les équilibreurs de charge et les pare-feu.

Ces éléments ont permis l'apparition des réseaux cœur virtualisés vEPC que l'on va voir en détail dans les lignes à venir.

3.7 LE vEPC (virtual Evolved Packet Core)

3.7.1 Définition du vEPC :

L'EPC virtuel fait abstraire et décompose les différentes fonctions de l'EPC classique et leur permet une exécution dans des combinaisons uniques dans des serveurs COTS (Commercial Off-The-Shelf).

3.7.2 Le passage de l'EPC vers le vEPC :

L'architectures EPC traditionnelle est de plus en plus limitée elle n'optimise plus du tout les coûts. De plus, elle n'est pas flexible. Le temps du déploiement est trop long et donc une introduction au marché tardive.

Le vEPC utilise la technologie NFV (Network Functions Virtualization) pour virtualiser les composants d'un système EPC classique, on obtient donc un vSGSN-MME, vEPG, vPCRF etc. Cette solution permet aux fournisseurs d'accélérer le déploiement et d'accroitre le nombre des services, et enfin d'abaisser les coûts de développement en diminuant le nombre d'équipements et les coûts de maintenance. Ci-dessous l'architecture d'un réseau vEPC est représentée.

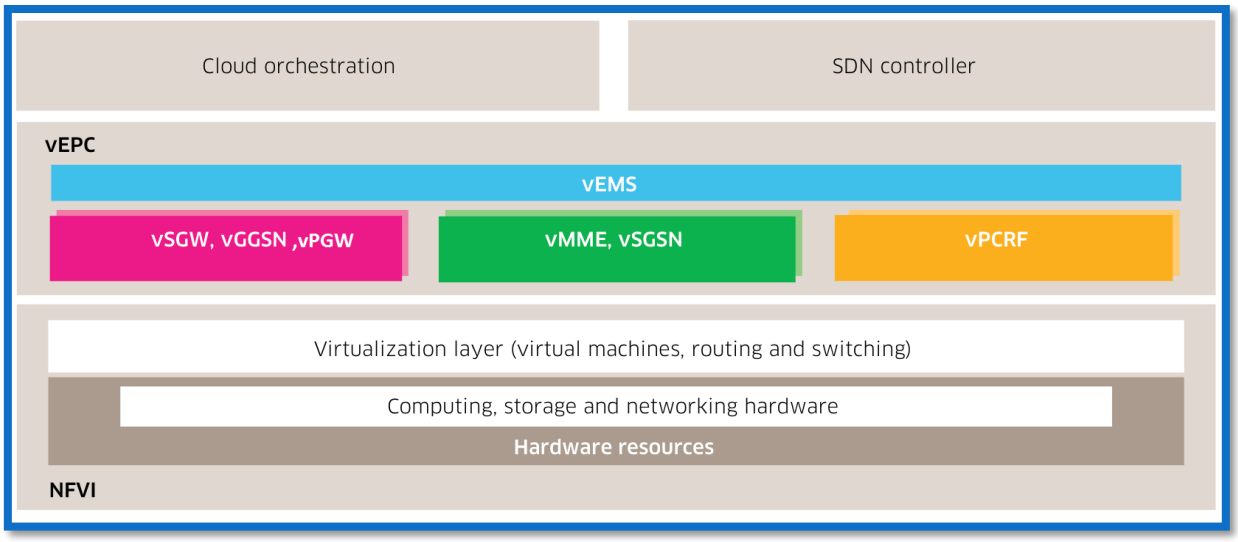

Figure 3.14 Architecture vEPC [15]

3.7.3 Les avantages du déploiement d'un vEPC :

La virtualisation est synonyme de simplification, en effet c'est une consolidation de plusieurs fonctions réseau dans une seule plate-forme. L'adoption du vEPC est donc avantageuse, citons quelques avantages :

- Réduction des coûts d'acquisition : le vEPC peut couter beaucoup moins cher que l'EPC traditionnel.
- Réduction des coûts de maintenance : le vEPC peut réduire les coûts conception, nécessite moins d'espace et plus facile à maintenir.
- Flexibilité : le vEPC permet l'introduction rapide de nouveaux services.
- Agilité : le vEPC offre aux fournisseurs une mise à l'échelle de services élastique en fonction de trafic réseau et demandes des clients.

3.7.4 Le vEPC et l'IoT :

Le vEPC permettra d'importantes nouvelles opportunités commerciales pour les operateurs. Il participe notamment à la croissance du marché IoT.

Les applications IoT ont des exigences réseau très différentes que les Smartphones et tablettes qui prédominent dans les réseaux actuels. Toutefois les fournisseurs commencent à tirer parti du NFV pour construire des sections IoT spécifiques dans leurs réseaux mobiles avec de nouveaux vEPCs.

L'EPC virtuel est composé de plusieurs sous-éléments, les quels vont être utilisés dans différentes combinaisons pour les applications IoT spécifiques (SpecificIoT applications). Le vEPC donne aux operateurs la possibilité de personnaliser de manière rentable leurs réseaux pour les différents clients (particulier, industriels), et applications qui sont critiques dans le monde diversifié de l'IoT.

3.7.5 Le vEPC et autres applications :

Plusieurs autres applications intéressantes rendues capables par l'EPC virtuel, citons d'ailleurs quelques unes :

- Réseaux mobiles spécifiques pour les entreprises
- Données mobiles haut débit
- L'apparition d'operateurs MVNOs (Mobile Virtual Network Operators).

3.7.6 Challenges de mise en œuvre :

Comme plusieurs nouvelles technologies complexes, l'EPC virtuel crée des chalenges pour les operateurs. Traditionnellement, les operateurs mobiles sont reliés à un ou deux grands fournisseurs (ERICSSON, NOKIA, Alcatel-Lucent etc.) pour leurs déployer des réseaux cœurs. Ces derniers sont typiquement implémentés comme systèmes intégrés sur des plate-fromes hardwares optimisées.

L'intégration de nouveaux vEPCs avec les systèmes Mobile Core et les back-offices (OSS/BSS) existants sera difficile et peut nécessiter une personnalisation importante. Plusieurs des grands operateurs de téléphonie mobile ont déjà construit de nouveaux réseaux cœurs à haute capacité pour leurs déploiement 4G LTE, à noter que la plupart des déploiements vEPC seront soit pour des réseaux mobiles vierges ou pour des nouvelles applications, telles que IoT, distinct du réseau de téléphonie mobile traditionnel qui est optimisé pour le trafic Smartphone.

3.8 Description des paramètres de trafic du vEPC :

3.8.1 Ps subscribers :

C'est le nombre d'abonnés qui dispose d'un service de données par paquets. On retrouve différentes type de souscriptions : 2G, 3G et 4G.

3.8.2 Simultaneously Attached Users (SAU) :

Dans le dimensionnement des nœuds, SAPC (nom commercial du PCRF chez ERICSSON), SGSN-MME et du EPG, le SAU représente le nombre maximum d'abonnés attachés simultanément que peuvent assumés ces nœuds.

Par ailleurs le SAU est utilisé pour déterminé le nombre minimum des nœuds requis pour bâtir le réseau cœur.

3.8.3 IP sessions :

C'est le nombre d'IP Sessions pour la 2G, 3G, 4G comportant le contexte PDP des 2G/3G plus les bearers LTE par défaut et dédié.

3.8.4 KPPS :

C'est le nombre de paquets par seconde portés par les nœuds vEPC.
Les deux tableaux ci-dessous définissent les rapports qu'on a utilisés dans notre application:

kSAU/VNF	La capacité SAU en utilisant le nombre de VM:s déclarés
kIP Sessions/VNF	La capacité d'IP Session en utilisant le nombre de VM:s déclarés
Gbps/VNF	La capacité de débit de données en utilisant le nombre de VM:s déclarées
Kpps/VNF	La capacité de debits de paquets en utilisant le nombre de VM:s déclarées

kSAU/VM	Le nombre SAU supporté par une VM
kIP Sessions/ VM	La nombre d'IP Session supporté par une VM
Gbps/ VM	Le débit de données supporté par une VM
Kpps/ VM	Le débit de paquets supporté par une VM

On va également définir quelques termes :

VM : Virtual Machine en anglais, est un container logiciel bien isolé pouvant exécuter son propre système d'exploitation et des applications comme s'ils tournés sur un ordinateur physique. Pour une VM les ressources virtuelles telles que le CPU(s), RAM, disque(s) et les cartes d'interface réseaux sont attribuées, qui sont crées par un logiciel appelé hyperviseur. L'hyperviseur permet la création et exécution de l'ensemble des machines virtuelles dans une machine physique.

VNF : Virtual Network Function (terme de l'ETSI), c'est la virtualisation des fonctions réseau qui est un élément réseau déployé dans un environnement virtuelle. Exemple : le vEPG, le vSGSN-MME, vSAPC etc.

3.9 Conclusion :

La virtualisation a permis de révolutionner le monde des réseaux et des télécommunications, par le passage du matériel au logiciel. On peut ainsi créer des machines virtuelles contenant diverses applications et fonctionnant sur une même machine physique. Ces machines virtuelles permettent la mise en œuvre des réseaux logiciels appelés aussi réseaux virtuels par l'interconnexion de ces différentes VM.

Nous avons vu dans ce chapitre les différents éléments qui permettent l'arrivé de ces nouveaux réseaux à savoir le Cloud qui contient les différentes VM, l'architecture SDN et NFV et ses différents éléments qui permettent le déploiement et l'exécutions des fonctions réseau désormais virtualisées.

4 Conception et réalisation de l'outil de dimensionnement de réseaux Packet Core Virtualisé

4.1 Introduction :

Dans ce dernier chapitre dédié à la conception et à la réalisation de notre application de dimensionnement de réseau cœur vEPC, nous allons décrire les différents besoins fonctionnels et non fonctionnels que doit avoir notre application, puis passer aux choix logiciels et matériels qui nous ont permis sa réalisation, enfin nous allons présenter les fonctionnalités de l'application et ses différentes interfaces à l'aide de capture d'écran.

4.2 Détermination des besoins :

Dans cette partie nous allons énumérer les différents besoins nécessaires à la réalisation de notre outil de dimensionnement de réseaux Packet Core Virtualisé, plus exactement le dimensionnement des nœuds : vEPG, vSGSN-MME, vSAPC (vPCRF), et décrire les étapes qui ont permis l'aboutissement de cet outil.

4.2.1 Les besoins fonctionnels :

Les besoins fonctionnels doivent spécifier toutes les fonctionnalités que doit contenir l'application afin de permettre aux utilisateurs de dimensionner leur réseau cœur paquet virtuel vEPC.

L'application qu'on va développer doit satisfaire les fonctionnalités suivantes :

- ***L'authentification à l'application :*** pour utiliser l'application, le client doit tout d'abord s'authentifier par l'insertion d'un nom d'utilisateur (login) et d'un mot de passe. Le système vérifie les informations introduites et permet ou non l'accès à l'application et détermine le rôle de chaque utilisateur.

- ***Importer des paramètres depuis une base de données :*** l'application à la possibilité de sauvegarder et/ou extraire des informations depuis une base de données.

- ***Insertion de données :*** l'utilisateur se doit d'insérer des données (inputs) pour pouvoir dimensionner son réseau cœur virtuel vEPC. Dans notre application on distingue deux types de données à introduire : en premier lieu les paramètres du trafic réseau et en second lieu les caractéristique du Hardware que veut utiliser l'opérateur de l'application (l'application se veut dynamique).

- ***Affichage des outputs :*** l'application fait des calculs en exploitant les données entrées en inputs ainsi que des informations se trouvant dans la base de données, puis affiche le résultat de ses calculs qui permet le dimensionnement d'un vEPC.

- ***Administration de l'outil :*** l'administrateur de l'application à la possibilité d'ajouter, supprimer, et de modifier le rôle de chaque utilisateur (opérateur) de l'application.

- ***Sauvegarde :*** l'outil permet la sauvegarde et la consultation des informations saisie par l'utilisateur.

4.2.2 Les besoins non fonctionnels :

Tous les systèmes informatiques doivent considérer des besoins non fonctionnels. En ce qui concerne notre réalisation, on distingue les besoins non fonctionnels suivants :

- ***Extensibilité :*** En cas d'apport de nouvelles fonctionnalités, la mise à jour de l'application doit être réalisée facilement.

- ***Performance :*** l'application ne doit présenter aucune faille, proposer des résultats correctes dans un des délais de temps moindre.

- ***Simplicité :*** les interfaces de l'application doivent être simple et à la porter de tout utilisateur pour qu'ils puissent manipuler ces fonctionnalité aisément et l'exploiter de manière optimale.

- ***Ergonomie :*** l'application se veut présentable et conviviale, assurant ainsi une communication entre l'utilisateur et la machine sans encombre.

4.2.3 Types d'utilisateurs :

On distingue deux types d'utilisateur de l'application :

- ***L'utilisateur ou opérateur client :*** son rôle se limite à entrer les données qui caractérise le trafic de son réseau, ainsi les spécifications du Hardware qu'il veut utiliser.

- ***L'administrateur*** : comme son nom l'indique a pour rôle d'administrer l'application. Il gère ainsi tous les composants de l'application, peut ajouter ou supprimer des opérateurs et désigner d'autres administrateurs.

4.2.4 Présentation conceptuelle de l'application:

Pour présenter notre application d'un point de vue conceptuelle, nous avons choisit de réaliser différents diagrammes afin d'aider le lecteur à mieux comprendre les étapes de conception et d'utilisation de l'application :

4.2.4.1 Diagramme de cas d'utilisation coté utilisateur :

Ce diagramme montre le comportement du système lorsque l'utilisateur (opérateur) se sert de l'application. L'utilisateur va devoir introduire des données en entrée nécessaire pour le calcul et pour le dimensionnement du réseau vEPC. Le résultat sera sur une interface dédiée indiquant les ressources à déployer.

La figure ci-dessous représente le diagramme de cas d'utilisation coté utilisateur :

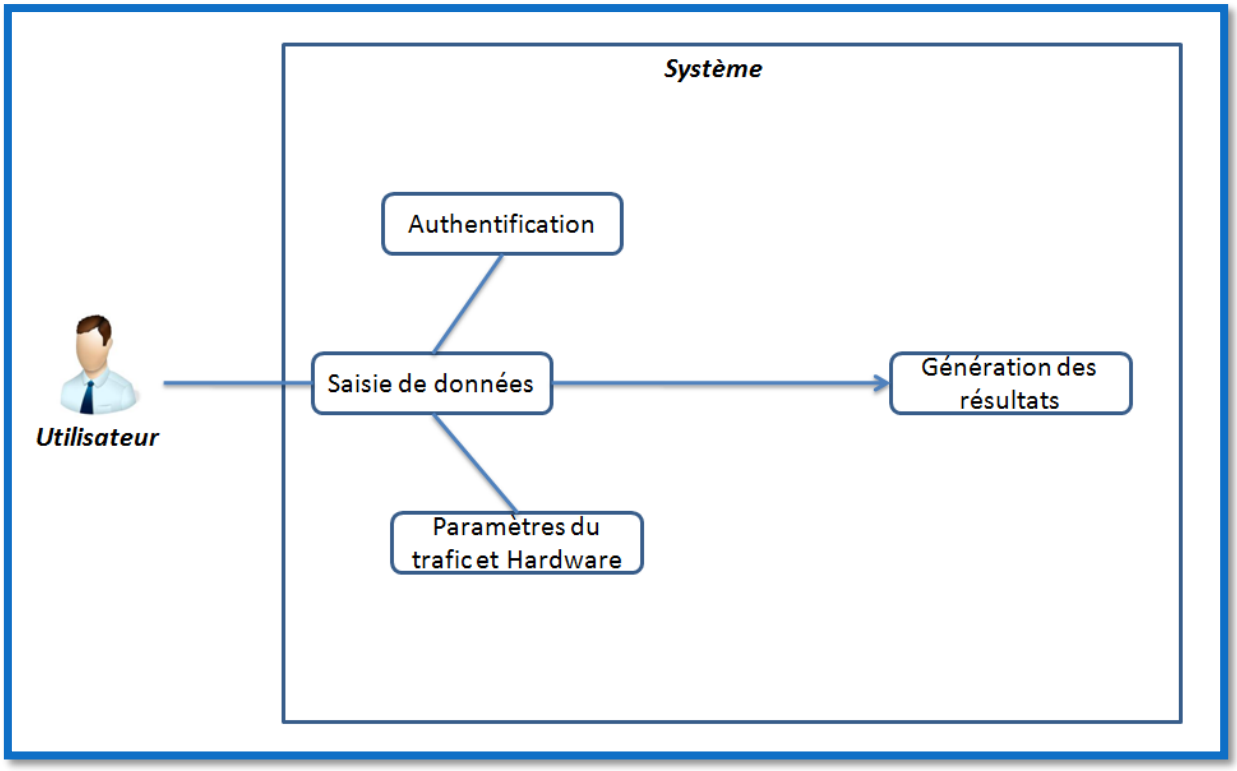

Figure 4.1 Diagramme de cas d'utilisation coté utilisateur

4.2.4.1.1 Description textuelle de cas d'utilisation :

	Saisie de données
Objectif	La saisie de données permet le calcul des différents paramètres du réseau afin de réaliser le dimensionnement du réseau vEPC.
Acteur	Utilisateur
Pré-Condition	L'utilisateur doit s'authentifier en saisissant son login (nom d'utilisateur) et son mot de passe afin d'accéder à l'interface des Inputs du trafic et du Hardware.
Scénario nominal	- L'utilisateur s'authentifie. - Il sélectionne les paramètres de son réseau ainsi du matériel qu'il veut utiliser. - L'application génère des résultats pour le dimensionnement du réseau.
Scénario d'exception	L'utilisateur n'accède pas à l'application (login et/ou mot de passe erroné(es)).

Figure 4.2 Tableau qui décrit le cas d'utilisation de l'application coté utilisateur

4.2.4.2 Diagramme de cas d'utilisation coté administrateur :

Le diagramme ci-dessous permet de décrire le comportement du système du coté administrateur. L'administrateur aura accès à toutes les fonctionnalités du système, telles que la modification, l'ajout ou la suppression des utilisateurs, des données et mise à jour du système.

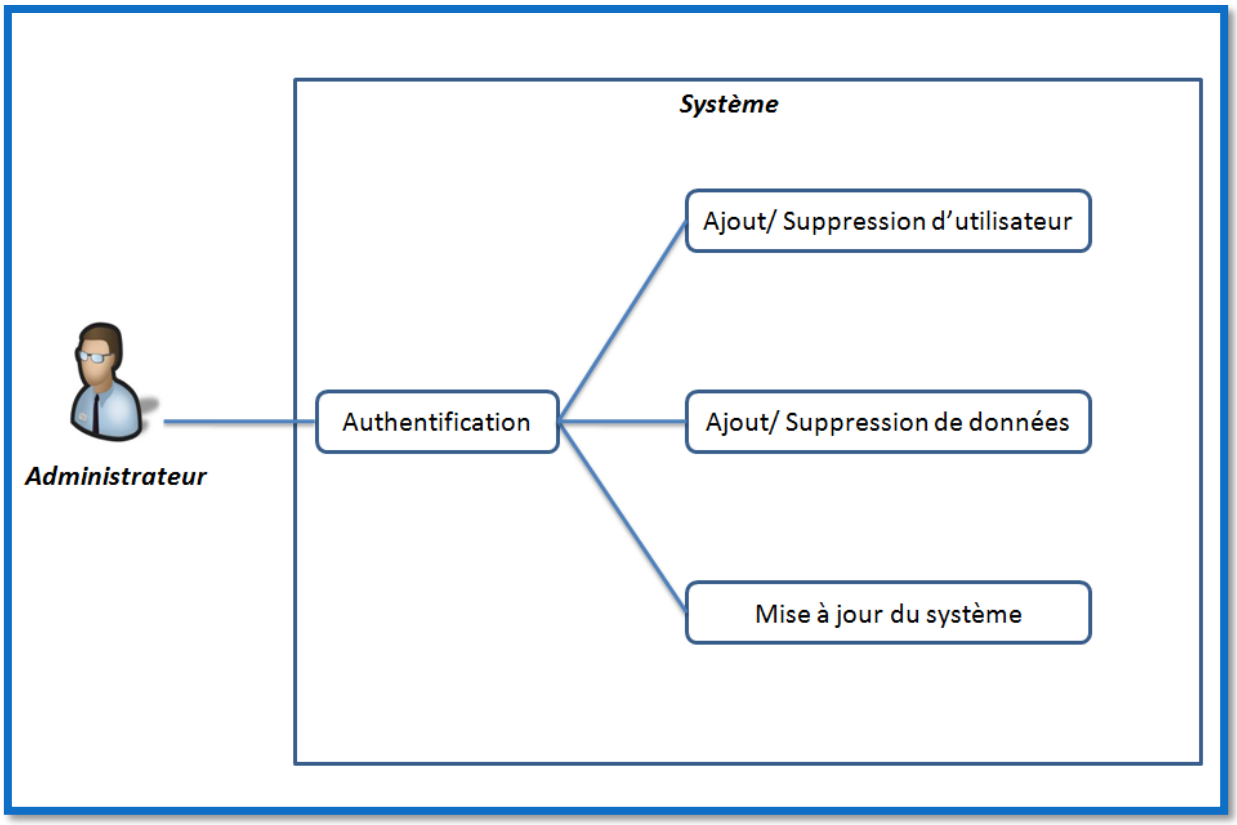

Figure 4.3 Diagramme d'utilisation coté administrateur

4.2.4.2.1 Description textuelle de cas d'utilisation :

	Ajout/Suppression
Objectif	Administrer le système : Ajout/Suppression d'utilisateur Ajout/Suppression de données Mise à jour du Système.
Acteur	Administrateur
Pré-condition	L'administrateur doit s'authentifier avec un login et un mot de passe afin d'accéder à l'application.
Scénario nominal	- L'administrateur s'authentifie - Il accède à la base de données contenant les informations relatives à l'application.
Scénario d'exception	L'administrateur n'accède pas à l'application (login ou mot de passe erroné(es)).

Figure 4.4 Tableau qui décrit le cas d'utilisation coté administrateur

4.2.4.3 Diagramme des séquences :

Le diagramme des séquences permet de décrire les interactions entre l'utilisateur (l'opérateur) et le système dans le temps. La figure ci-dessous représente le diagramme des séquences.

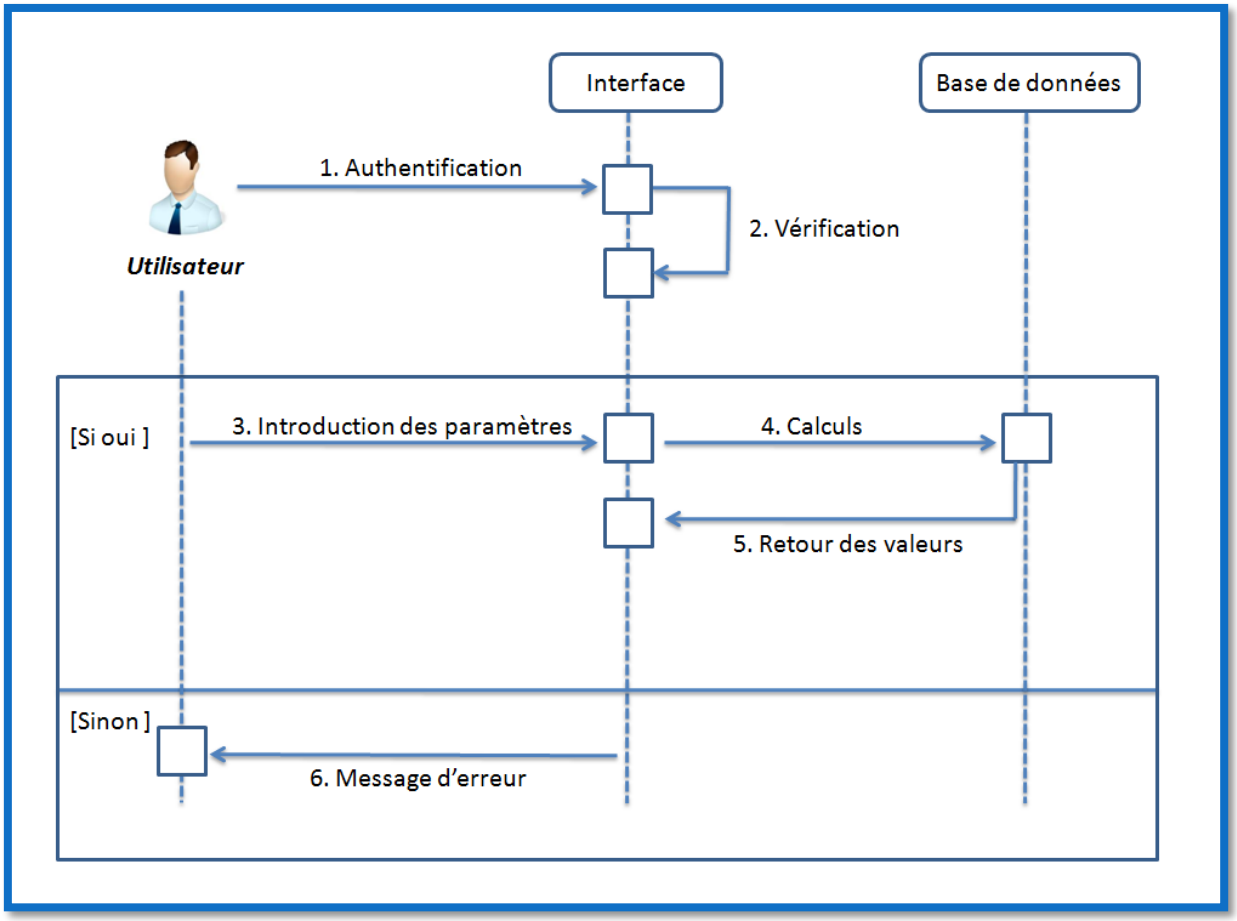

Figure 4.5 Diagramme des séquences

4.2.4.4 Diagramme d'activité :

Le diagramme d'activité permet de présenter le déroulement des événements en fonctions des états du système. Le diagramme suivant permet de décrire les différents états de notre application.

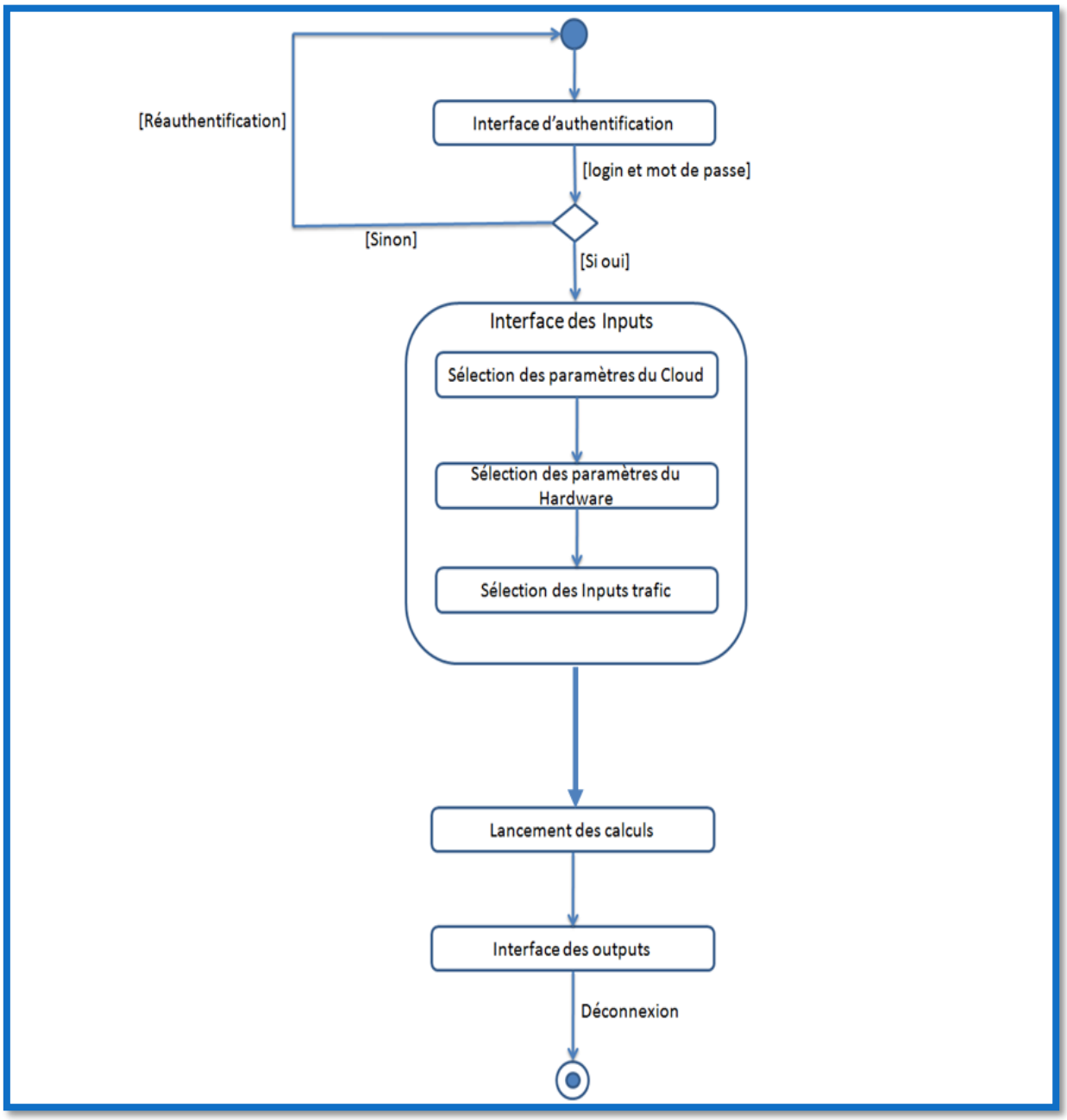

Figure 4.6 Diagramme d'activité

4.3 Réalisation de l'application :

Dans cette partie dédiée à la conception de l'application, que l'on a nommé DimTool pour Dimensioning Tool, servant au dimensionnement d'un vEPC, nous allons préciser les environnements matériels et logiciels du travail réalisé, ensuite mettre en exergue nos choix techniques et enfin nous allons exposer les différentes interfaces qui constitue l'application à travers des captures d'écran.

4.4 Environnement de travail :

Dans cette section présente l'environnement matériel nécessaire à la réalisation de ce projet ainsi que l'environnement logiciel qui a permis l'élaboration et l'achèvement de l'outils de dimensionnement.

4.4.1 Environnement matériel :

La réalisation de cette application web a été conçue à l'aide d'un ordinateur portable ayant les caractéristiques suivant :

- Pc portable 1 : LENOVO Z50-70
- Processeur : Intel® Core™ i5-4210U CPU @ 1.70GHz 2.40GHz
- OS : Windows 7 professionnel
- Mémoire RAM : 6.00 Go
- Disque Dur : 1 To.
- Pc portable 2 : Apple MacBook pro
- Processeur : 2.5 GHz Intel Core i5
- OS : Mac OS X Yosemite
- Mémoire RAM : 8 Go 1600 MHz DDR3
- Disque Dur : 128 Go SSD.

4.4.2 Environnement logiciel :

Les lignes suivantes nous renseignent sur les outils logiciels utilisées lors de la phase de développement de l'application DimTool :

- Langage de développement : PHP 5.4.6
- Environnement de développement : EasyPHP 14.1
- Serveur HTTP : Apache 2
- Système de gestion de base de données : MySQL
- Outil de rédaction du projet : Word office 2007 et 2016.

4.5 Choix techniques :

Cette partie donne quelque définition et particularité des outils logiciels que nous avons choisit.

4.5.1 Choix d'EasyPHP :

EasyPHP est un logiciel de développement Web sous le système d'exploitation Windows pour des applications Web de nature dynamique en utilisant le serveur Appache2, le langage de programmation PHP et d'une base de données MySQL. Il possède l'application PhpMyAdmin pour gérer plus aisément les bases de données.

Parmi les éléments qui composent EasyPHP on retrouve :

- **Apache :** on le retrouve généralement dans des serveurs Web, Apache est un logiciel apte à traiter les requêtes HTTP que l'on envoie pour demander une page Web.
- **MySQL :** c'est un système de gestion de base de données
- **PHP :** c'est un langage de programmation libre, principalement utilisé pour produire des pages Web dynamique via un serveur HTTP, mais pouvant également fonctionner comme n'importe quel autre langage de façon locale. PHP est un langage orienté objet.
- **PhpMyAdmin :** c'est une interface pratique permettant d'exécuter, très facilement et sans grande connaissances en base de données, des requêtes comme la création de table de données, mise à jour, suppression et modification de structure de la base de données.

EasyPHP permet de gérer d'autres fonctionnalités telles que :

- La gestion des services propres à Apache et MySQL
- Installation est mise à jour des versions Apache, MySQL et PHP
- Gestion des paramètres de configuration des serveurs
- Accéder aux fichiers de configuration
- Accéder aux fichiers logs
- Créer des alias.

4.5.2 *Langage de programmation PHP :*

PHP est un langage de programmation qui s'intègre dans les pages HTML. Il permet de rendre automatiques des tâches répétitives, notamment grâce à la communication avec une base de données.

L'un des avantages le plus important de PHP est qu'il est simple, mais il offre aussi des fonctionnalités avancées pour les experts dans ce domaine.

Bien que le développement de PHP s'articule autour de la programmation des sites Web, il est possible d'en faire bien d'autres usages. Il y a trois domaines où PHP peut s'illustrer :

- **Langage de script coté serveur.** C'est l'utilisation traditionnelle, et aussi le principal objet de PHP. Il existe trois composants pour l'exploiter : un analyseur PHP (module serveur), un serveur Web et un navigateur Web. Le serveur Web doit être exécuté en corrélation avec PHP. L'accès au programme se fait à l'aide du navigateur Web.

- **Langage de programmation en ligne de commande.** On peut écrire des scripts PHP et les exécuter en ligne de commande, sans l'aide du serveur Web et d'un navigateur. Il suffit de disposer de l'exécutable PHP.

- **Ecrire des applications clients graphiques.** On peut utiliser PHP-GTK pour écrire de tels programmes. Il est possible d'écrire des applications très portables avec ce langage. PHP-GTK est une extension de PHP non fournie dans la distribution de base.

4.5.3 *Choix de MySQL :*

Pour la réalisation de l'application DimTool on a choisi de travailler avec la base de données MySQL qui est gérée par l'interface PhpMyAdmin.

Les critères de cette base de données sont les suivants :

- **Performances :** MySQL est un système rapide et très performant.

- **Gratuité :** MySQL est disponible gratuitement sur internet sous une licence open-source.

- **Simplicité :** l'installation de MySQL est très simple à installer.

- **Portabilité :** MySQL peut fonctionner convenablement sur plusieurs systèmes d'exploitation tels que Windows et Unix.

- **Disponibilité du support :** MySQL est open-source, la documentation permettant son apprentissage est abondante. Plusieurs livres, tutoriels et site spécialisés sont disponible pour permettre une bonne formation et apprentissage de ce dernier.

4.6 Interfaces graphiques de l'application :

Dans cette partie nous allons présenter le travail que nous avons réalisé, c'est-à-dire la conception et le développement de notre application de dimensionnement de réseaux cœur vEPC. Pour cela on a pris plusieurs captures d'écran pour montrer les multiples interfaces que contient l'application et ses fonctionnalités.

4.6.1 Interface d'authentification :

C'est la première interface qui apparait lors de l'exécution de l'application. Cette interface permet à l'utilisateur de s'authentifier à l'aide d'un login (nom d'utilisateur) et d'un mot de passe. Cela permet de différencier entre les utilisateurs lambda et l'administrateur qui a tous les droits d'accès à l'application.

L'interface d'authentification est présentée à la figure 4.7.

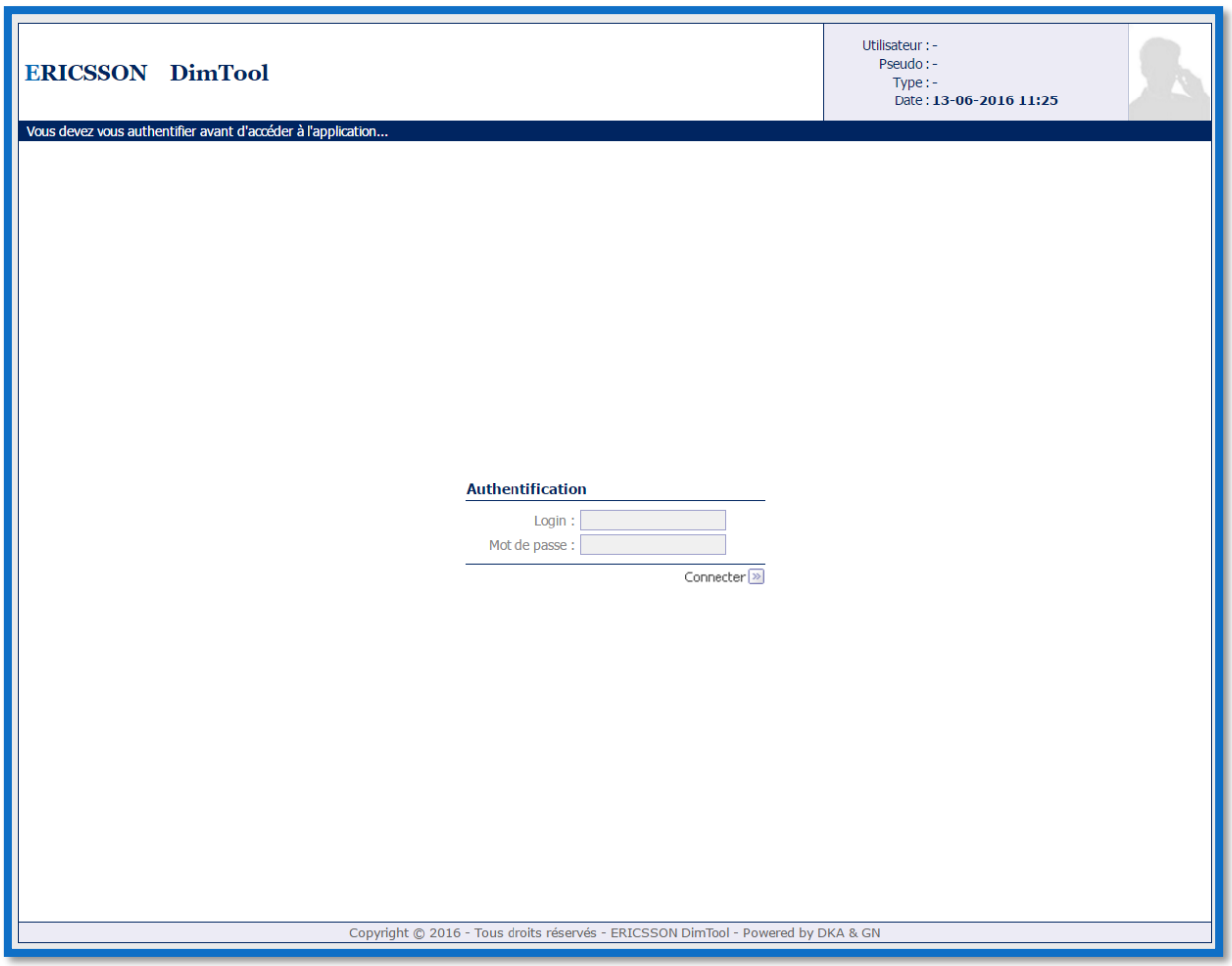

Figure 4.7 Interface d'authentification de l'application DimTool

Si le login et/ou le mot de passe sont erroné(s) un message d'erreur va s'afficher indiquant que les informations saisies sont faux et donne droit à une réauthentification. Comme le montre la figure suivante.

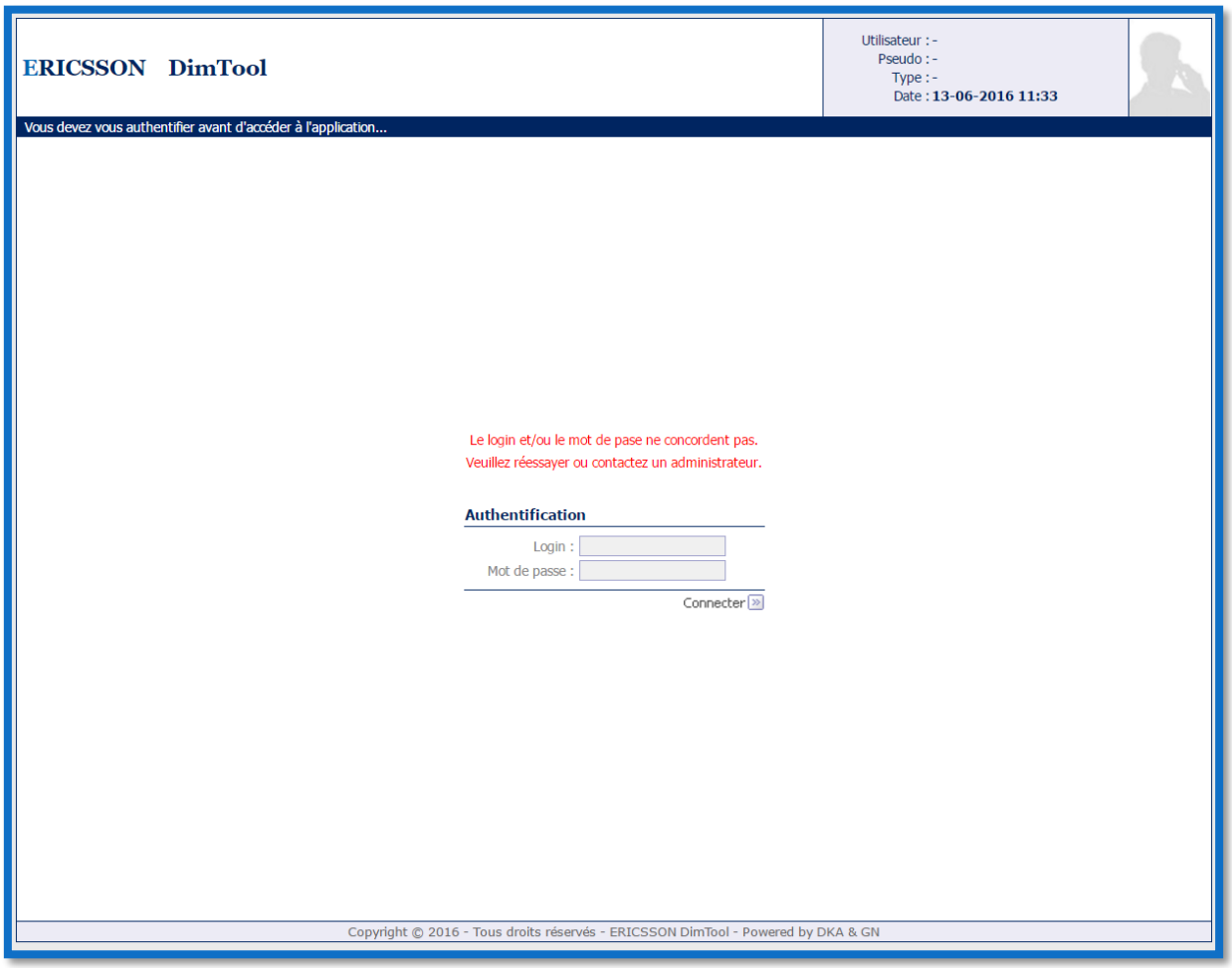

Figure 4.8 Interface d'authentification (message d'erreur)

4.6.2 Interface d'accueil :

Après l'introduction de login et de mot de passe correctes, l'utilisateur est orienté vers une interface d'accueil de l'application. Cette interface contient plusieurs menus qui sont les suivants :

- Menu Inputs : ce menu contient différentes entrées à introduire, on retrouve les paramètres du trafic et les paramètres du hardware qu'on souhaite utiliser.

- Menu Outputs : dans ce menu, on retrouve les résultats de calculs après l'introduction des Inputs. On retrouve les interfaces de sorties du trafic (total d'abonnés, total trafic en Gbit/s…), et les interfaces des outputs vEPG, vSGSN-MME et vSAPC (nombre de machines virtuels, nombre de serveur…).

- Menu administration (lorsqu'on se connecte en tant qu'administrateur) : dans ce menu on retrouve une liste déroulante contenant la liste des utilisateurs, elle permet de gérer les utilisateurs de l'application (supprimer ou modifier le rôle des utilisateurs), nouvel utilisateur pour créer un nouvel utilisateur.

- Menu Mon compte : ce Menu permet à l'utilisateur de gérer son compte, par exemple changer de login ou de mot de passe.

- Menu Help : dans ce menu servant à aider l'utilisateur de DimTool on retrouve le FAQ (Frequently Asked Questions), ce sont les questions que peux se poser l'utilisateur suivi de réponses claires et précises. On retrouve aussi dans ce menu le manuel utilisateur contenant toutes les informations nécessaires pour bien utiliser l'application que l'on peut télécharger sous format PDF.

  La figure 4.9 représente l'interface d'accueil de l'application et ses différents menus.

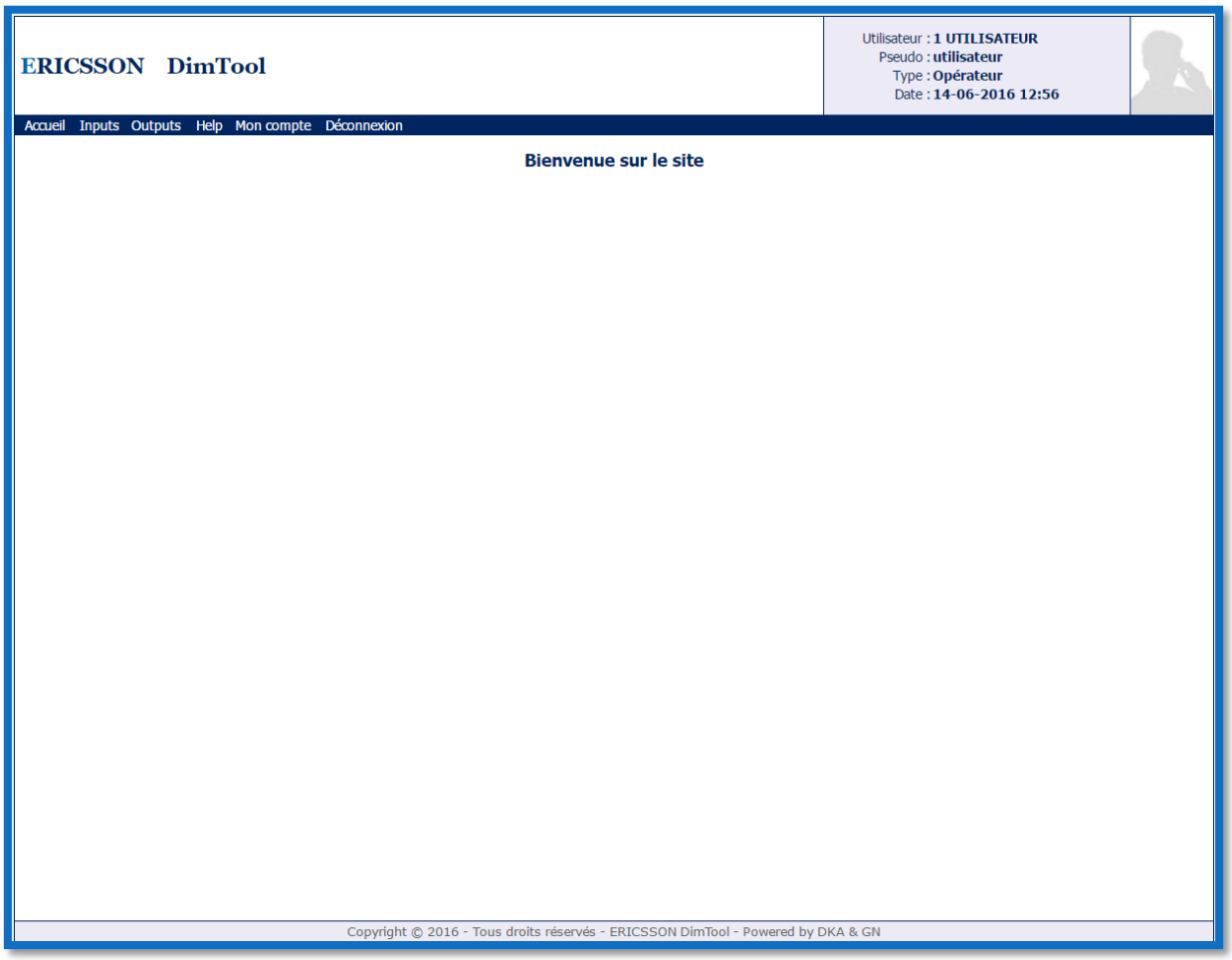

Figure 4.9 Interface d'accueil de l'application

4.6.3 Interface des Inputs trafic :

Cette interface permet à l'utilisateur d'insérer des paramètres concernant le trafic de son réseau, afin de réaliser des calculs pour avoir en sortie les ressources nécessaires pour le dimensionnement des nœuds vEPG, vSGSN-MME et vSAPC (vPCRF) du réseau cœur vEPC.

La figure 4.10 représente l'interface des Inputs pour les paramètres du trafic réseau.

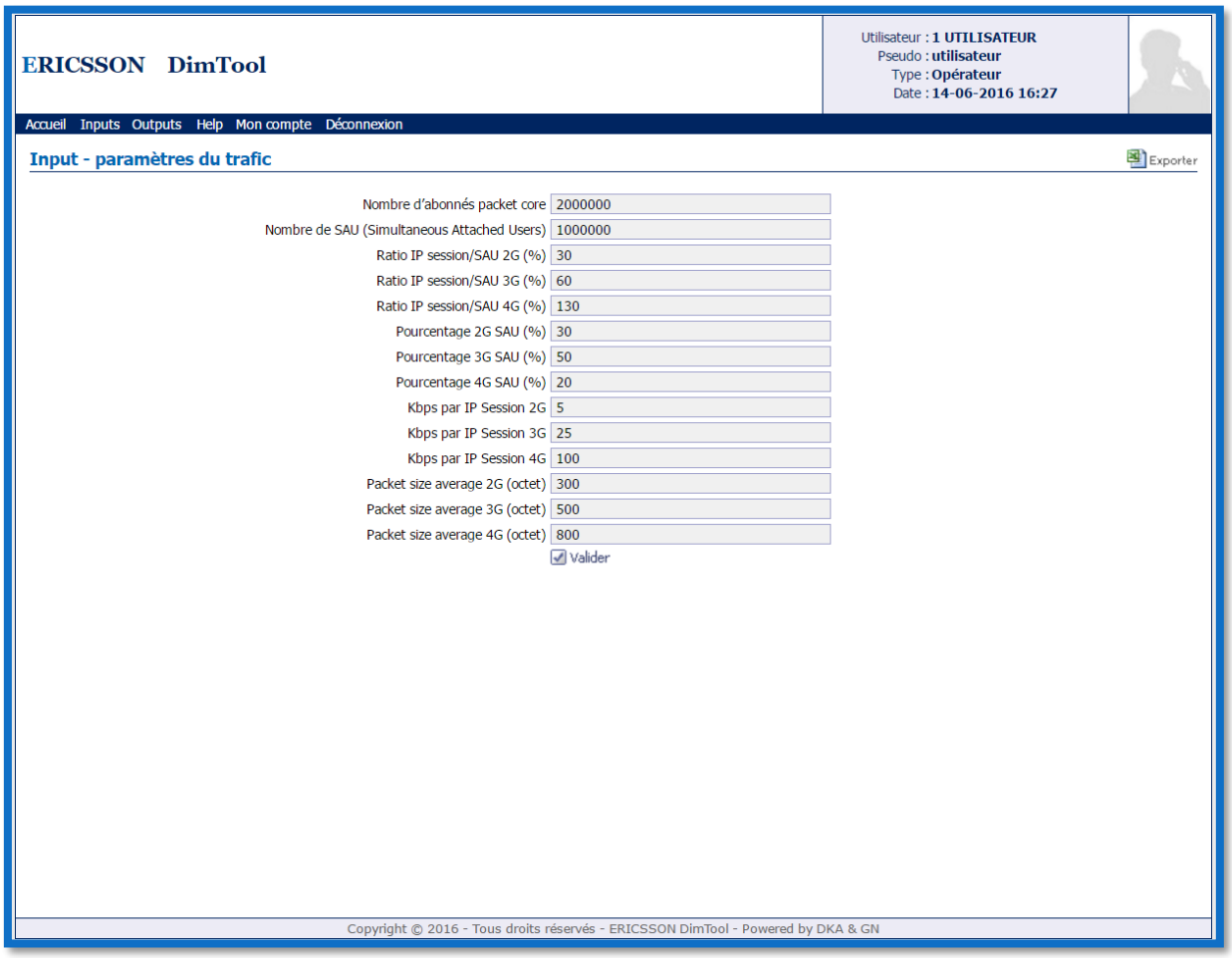

Figure 4.10 Interface des Inputs (paramètres du trafic).

Les paramètres du trafic à saisir sont les suivants :

- **Nombre d'abonnées packet core :** il s'agit du nombre total d'abonné du réseau.
- **Nombre de SAU (Simultaneous Attached Users) :** il représente le nombre d'abonné attaché simultanément (qui utilise le réseau en même temps).
- **Ratio IP session/SAU 2G, 3G, ou 4G :** représente le nombre de session IP établies par les abonnés attachés simultanément pour chacune des trois générations (2G, 3G, 4G).
- **Pourcentage 2G, 3G et 4G SAU :** représente le pourcentage d'abonnés attachés simultanément pour les trois générations précédentes.
- **Kbps par IP session 2G, 3G et 4G :** c'est le débit binaire pour chaque session IP pour les trois générations.
- **Taille moyenne des paquets 2G, 3G, 4G :** représente la taille moyenne que peut avoir un paquet.

4.6.4 *Interface choix du Hardware :*

Dans cette interface l'utilisateur à la possibilité de choisir entre trois types de Hardware dont les caractéristiques sont différentes pour chacun deux. Ces trois types de machines sont les suivantes :

- HP BL 460c
- HP DL 380c
- DELL R630.

L'utilisateur à également la possibilité d'insérer manuellement ses propres caractéristiques du Hardware qu'il veut utiliser.

La figure ci-dessous représente l'interface du choix du Hardware.

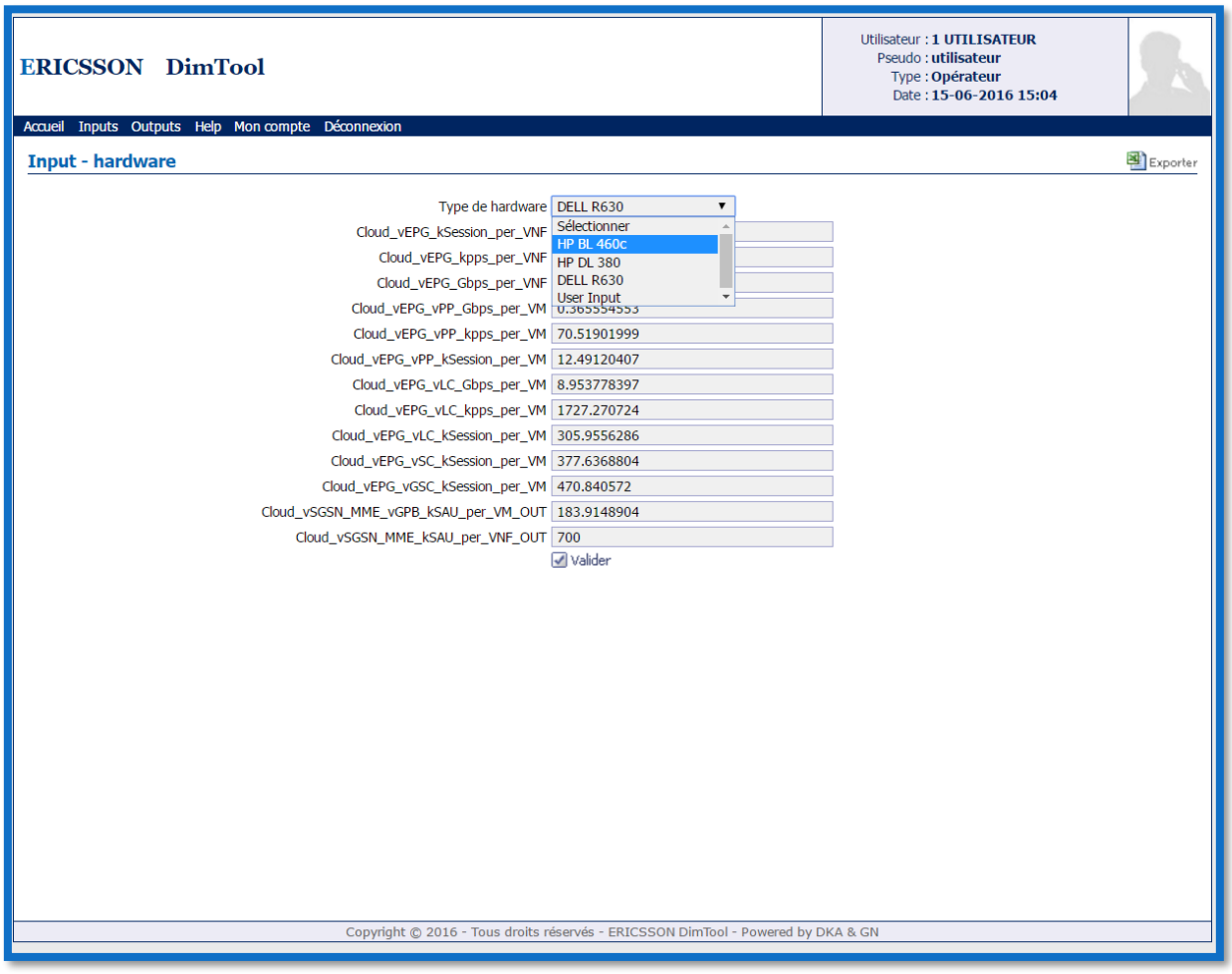

Figure 4.11 Interface du choix de hardware

Lorsqu'un Hardware est sélectionné ses paramètres sont alors pris en compte, pour les calculs dimensionnement.

Lorsque c'est l'utilisateur qui veut insérer ses propres paramètres du Hardware, c'est l'interface présenté à la figure 4.12 qui apparait.

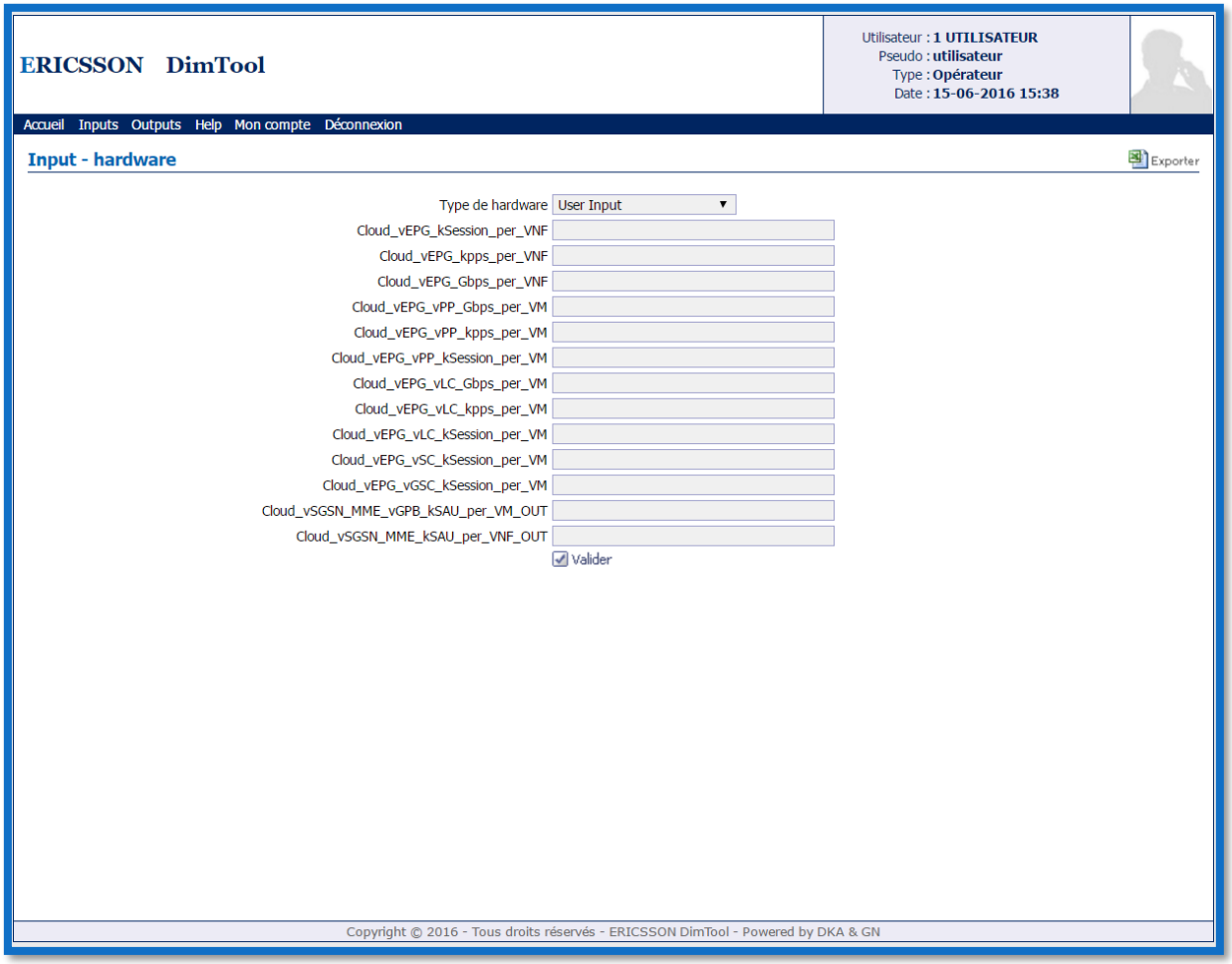

Figure 4.12 Interface choix du Hardware (paramètres insérés par l'utilisateur)

4.6.5 Interface des Outputs :

Après avoir introduits les paramètres du trafic dans l'interface Inputs trafic, et sélectionné le choix du Hardware que l'on souhaite utilisé dans l'interface du choix du Hardware, le système procède aux calculs et fournit des résultats qui se trouvent dans l'interface des outputs. On retrouve deux types d'outputs :

- Outputs qui concernent les paramètres du trafic.
- Outputs qui concernent le dimensionnement des nœuds vEPG, vSGSN-MME, vSAPC.

La figure suivante représente l'interface des outputs trafic :

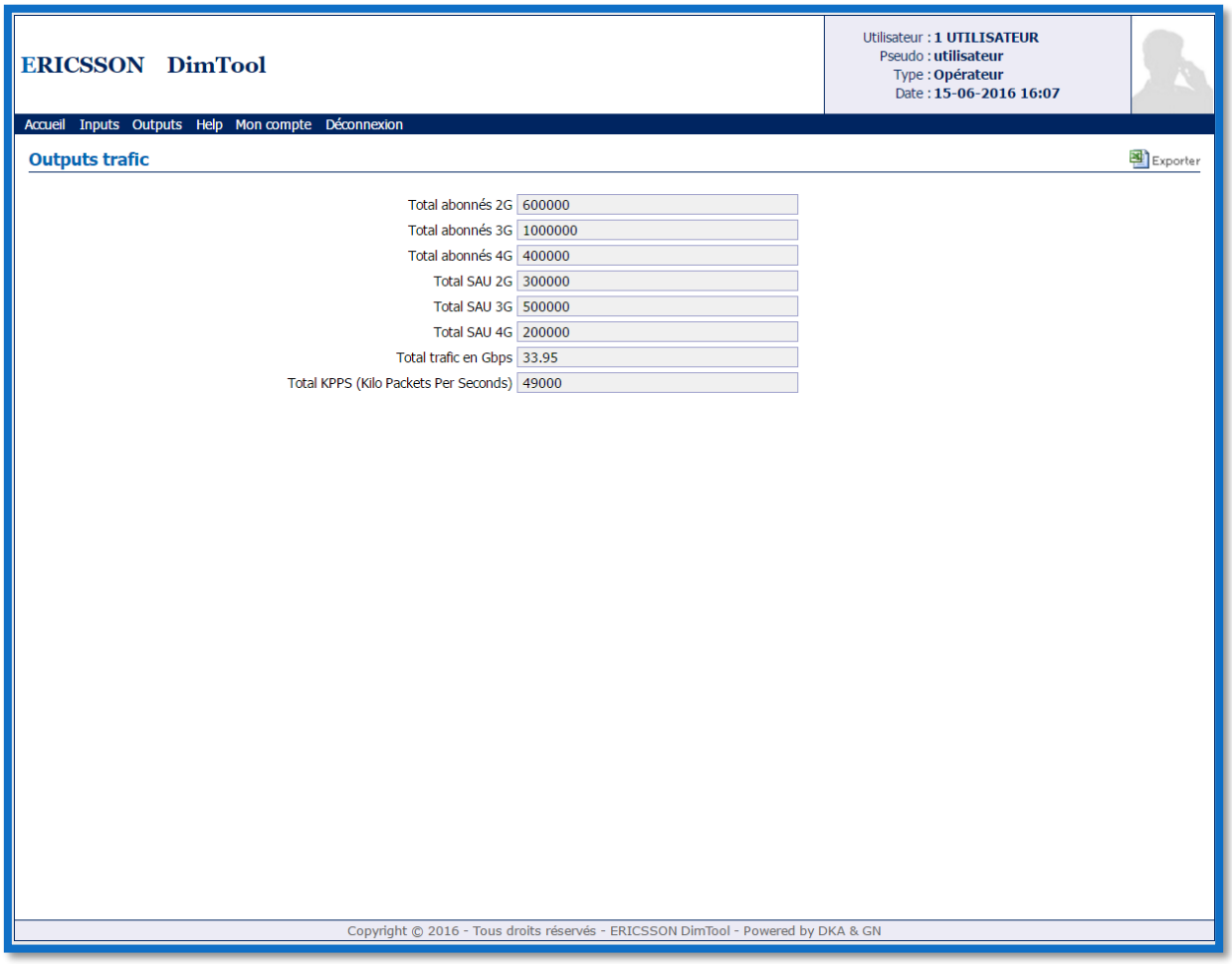

Figure 4.13 Interface des Outputs trafic

Dans cette interface on retrouve les sorties suivantes :

- Total abonnés 2G, 3G, 4G : représente le nombre total d'abonnés utilisant chacune des trois générations précédentes.
- Total SAU 2G, 3G, 4G : représente le nombre total d'abonnés attachés simultanément pour les générations 2G, 3G et 4G.
- Total trafic en Gbps : représente le total du trafic généré par les abonnés en Giga bit par seconde.
- Total Kpps : représente la charge du trafic généré par les abonnés en kilo paquet par second.

La figure 4.14 représente l'interface des Outputs pour le nœud vEPG :

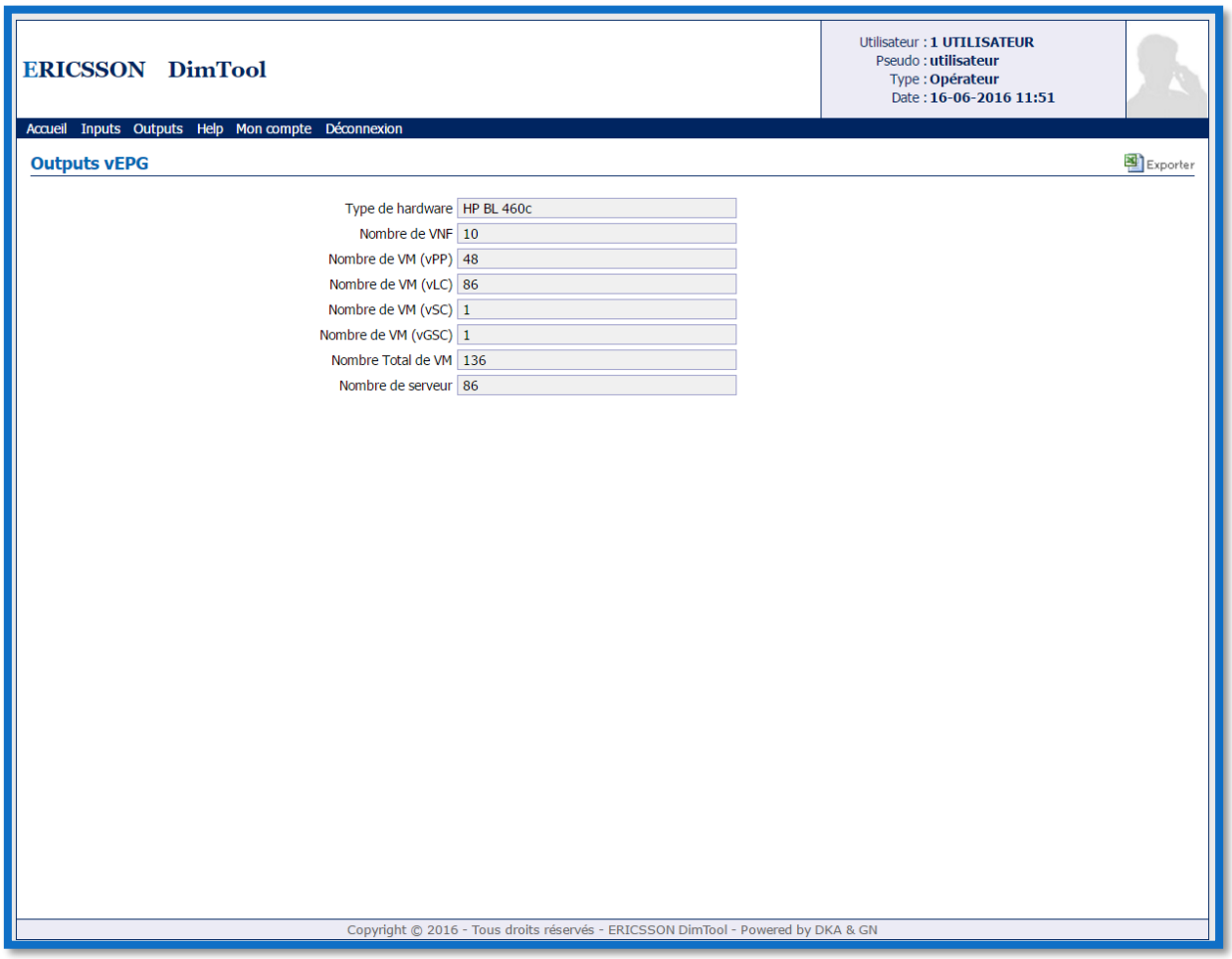

Figure 4.14 Interface des Outputs du nœud vEPG

Dans cette interface on retrouve les sorties suivantes :

- Type du hardware : représente le Hardware choisit pour les calculs de dimensionnement.
- Nombre de VNF : représente le nombre de fonctions réseau virtualisées nécessaires pour réaliser un vEPG.
- Nombre de VM vPP, vLC, vSC, vGSC : représente le nombre de machines virtuelles nécessaires pour contenir chacune des quatre fonctions du vEPG.
- Nombre Total de VM : représente le nombre total de machines virtuelles, nécessaires à la réalisation du vEPG.
- Nombre de serveurs : représente le nombre serveurs nécessaires pour contenir tous les machines virtuelles.

Pour les interfaces des Outputs nous retrouvons les mêmes sorties c'est-à-dire, le type de hardware choisit, le nombre de VNF, le nombre de VM pour chaque fonction du vSGSN-MME et du vSAPC, et le nombre de serveurs nécessaires.

4.6.6 Menu Help:

Le menu Help, permet à l'utilisateur d'avoir de l'aide concernant l'utilisation de l'application et ses diverses fonctionnalités. Ce menu contient deux volets : le volet FAQ et un manuel utilisateur téléchargeable sous format PDF.

La figure 4.15 représente l'interface FAQ de l'application :

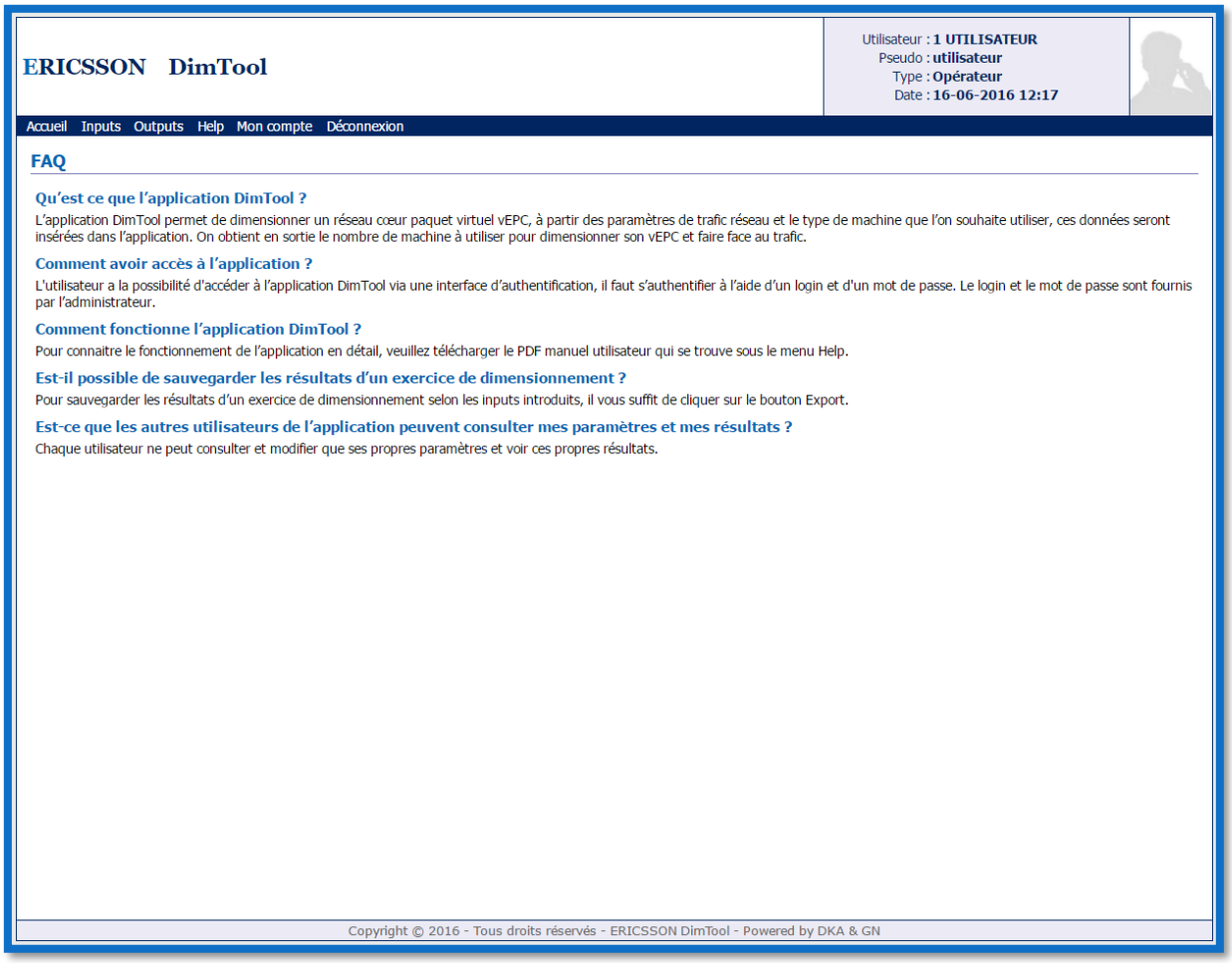

Figure 4.15 Interface FAQ de l'application

La figure 4.16 représente le manuel utilisateur de l'application DimTool :

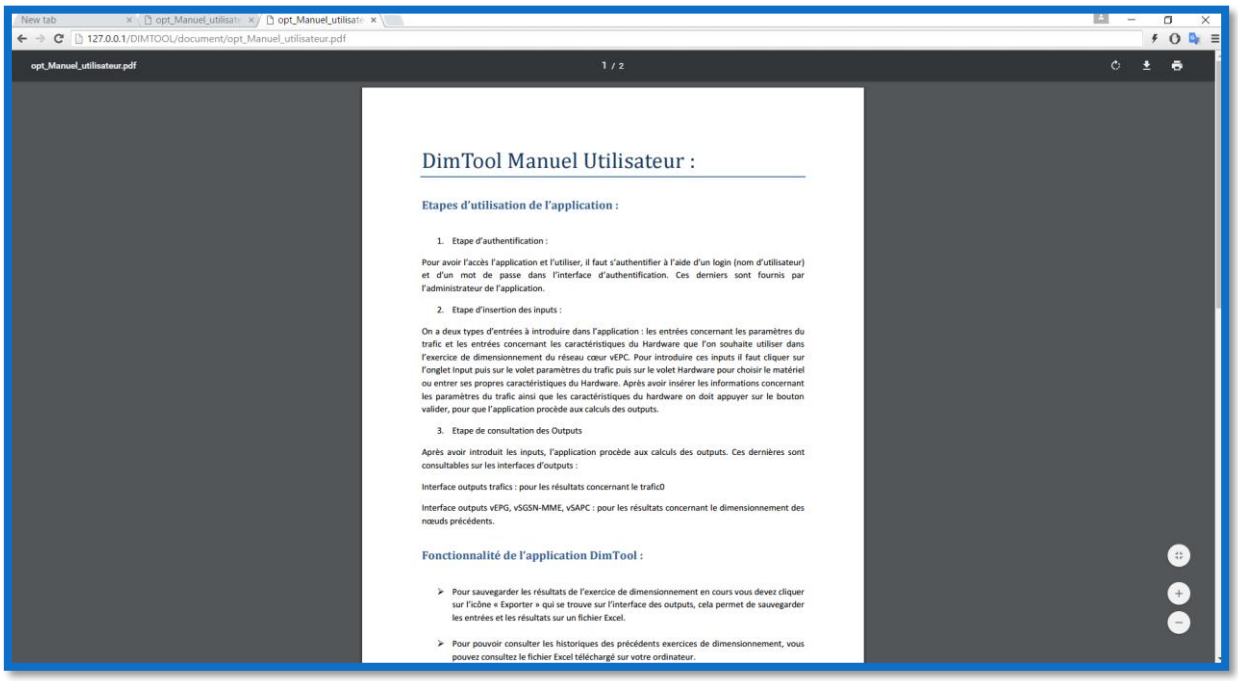

Figure 4.16 Manuel utilisateur de l'application

Suite au développement de l'application on a pu vérifier les résultats générés par l'application par rapport à des valeurs réels vérifiés par le constructeur dans son laboratoire. Les résultats dégagés sont alignes avec les observations faites dans le monde de l'industrie par le constructeur Ericsson.

4.7 Etude pratique de l'application:

Dans cette partie, nous allons utiliser notre application pour deux cas d'utilisation. Le premier concerne le mobile Broadband, le deuxième cas est une application IoT « le Smart Metering » ou compteur intelligent, c'est du télé-prélèvement. Nous allons entrer en Input les différents paramètres des deux cas d'utilisation, puis constater les résultats obtenus pour dimensionner les nœuds vEPG et vSGSN-MME.

4.7.1 Cas d'utilisation n°1 : le mobile Broadband :

Les différents paramètres introduits en entrées et les résultats obtenus sont illustrés dans les figures suivantes.

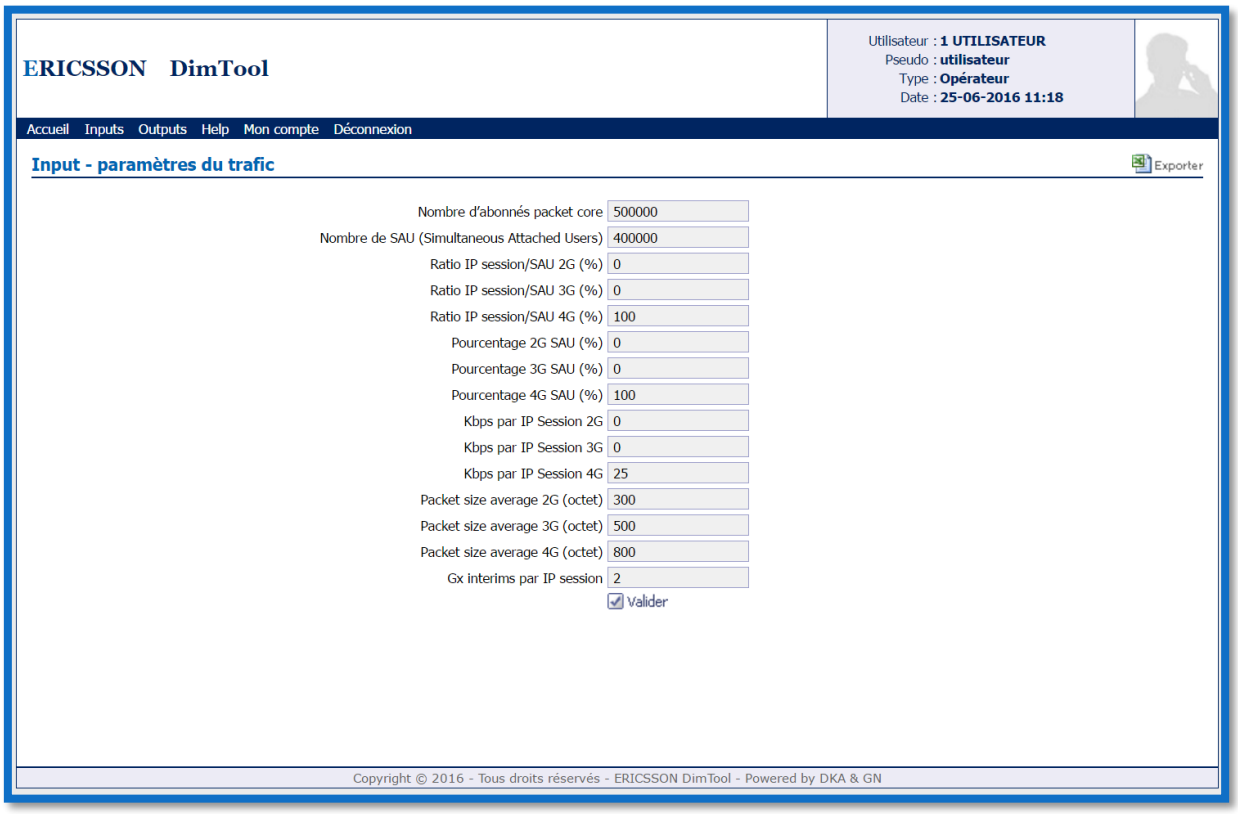

Figure 4.17 Inputs trafic du cas d'utilisation "mobile BroadBand"

Dans cette exemple, on prendre 500000 abonnés et dont 40000 utilisent simultanément le réseau 4G. A partir de ces paramètres le système va calculer le trafic que génèrent ces abonnées, et le nombre de hardware nécessaire pour le dimensionnements des nœuds vEPC.

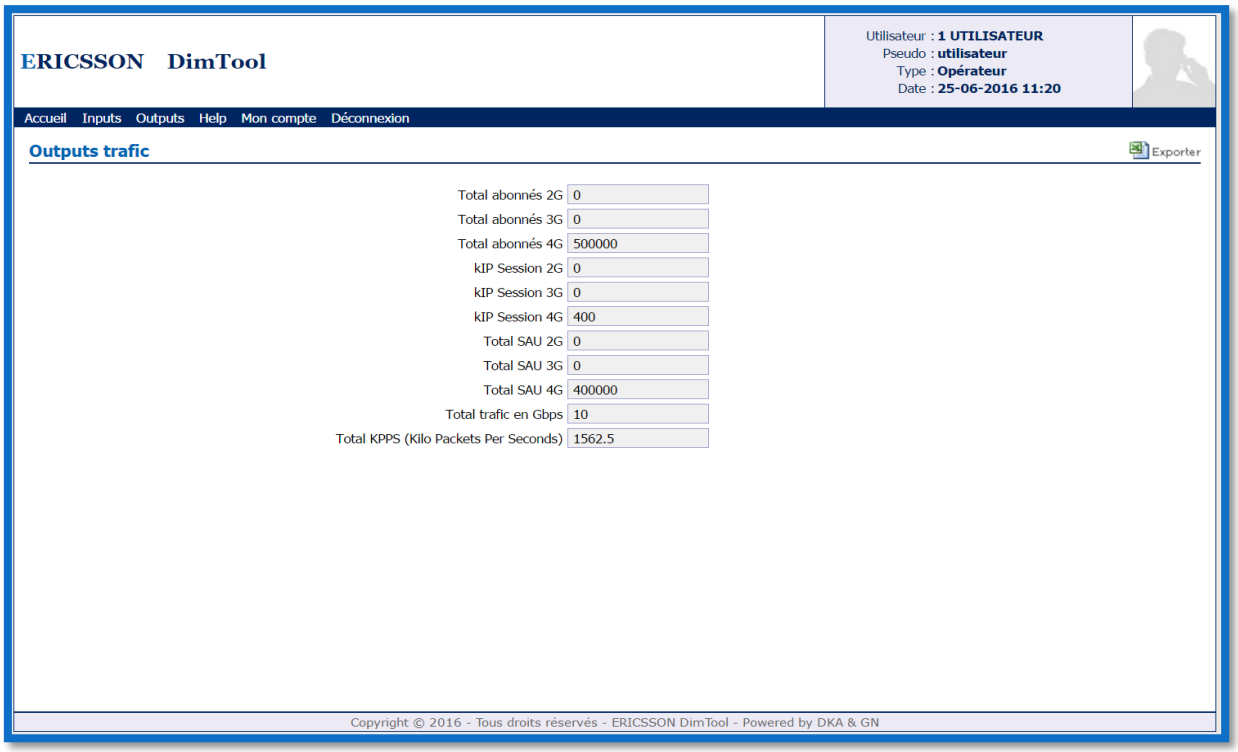

Figure 4.18 outputs trafic

Le trafic généré est de 10 Gbps et de 1562.6 KPPS pour le nombre d'abonnés précédent.

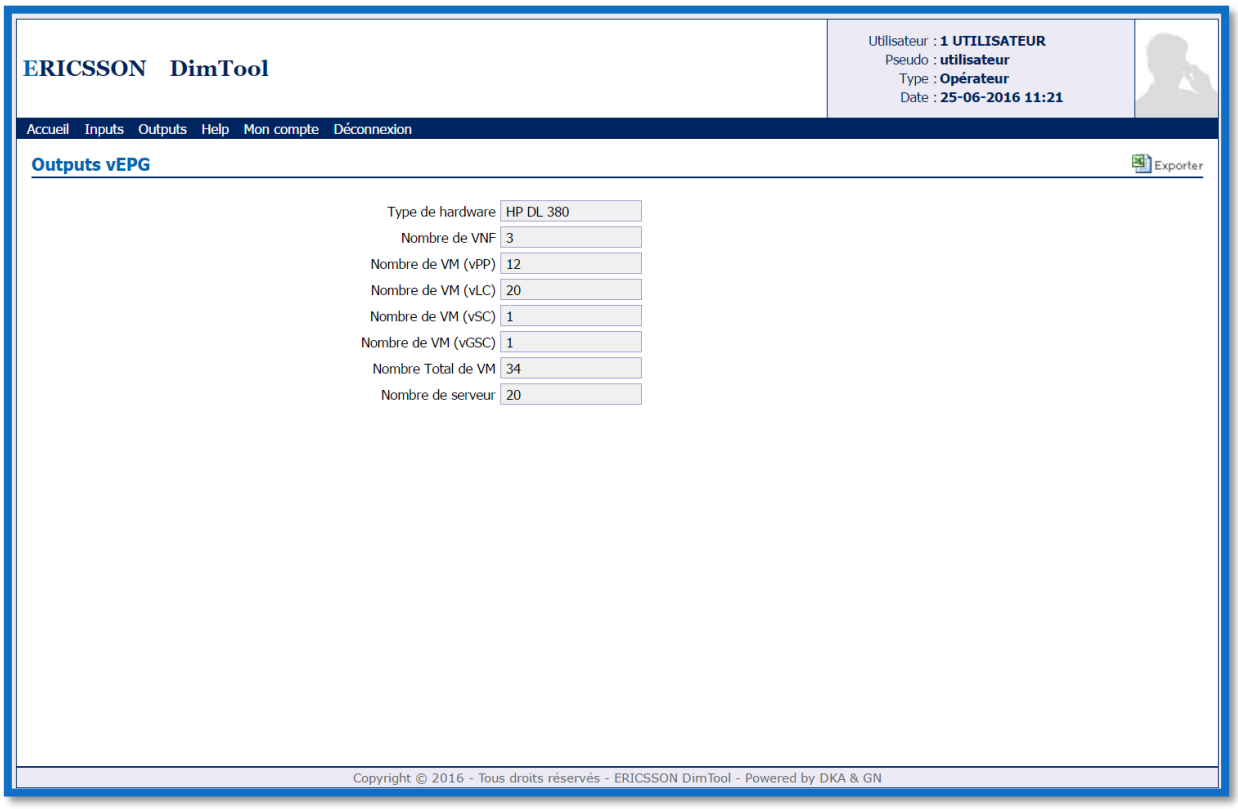

Figure 4.19 Outputs vEPG

La figure 4.19 représente les outputs pour le dimensionnement d'un vEPG pour le cas d'utilisation du Mobile Broadband.

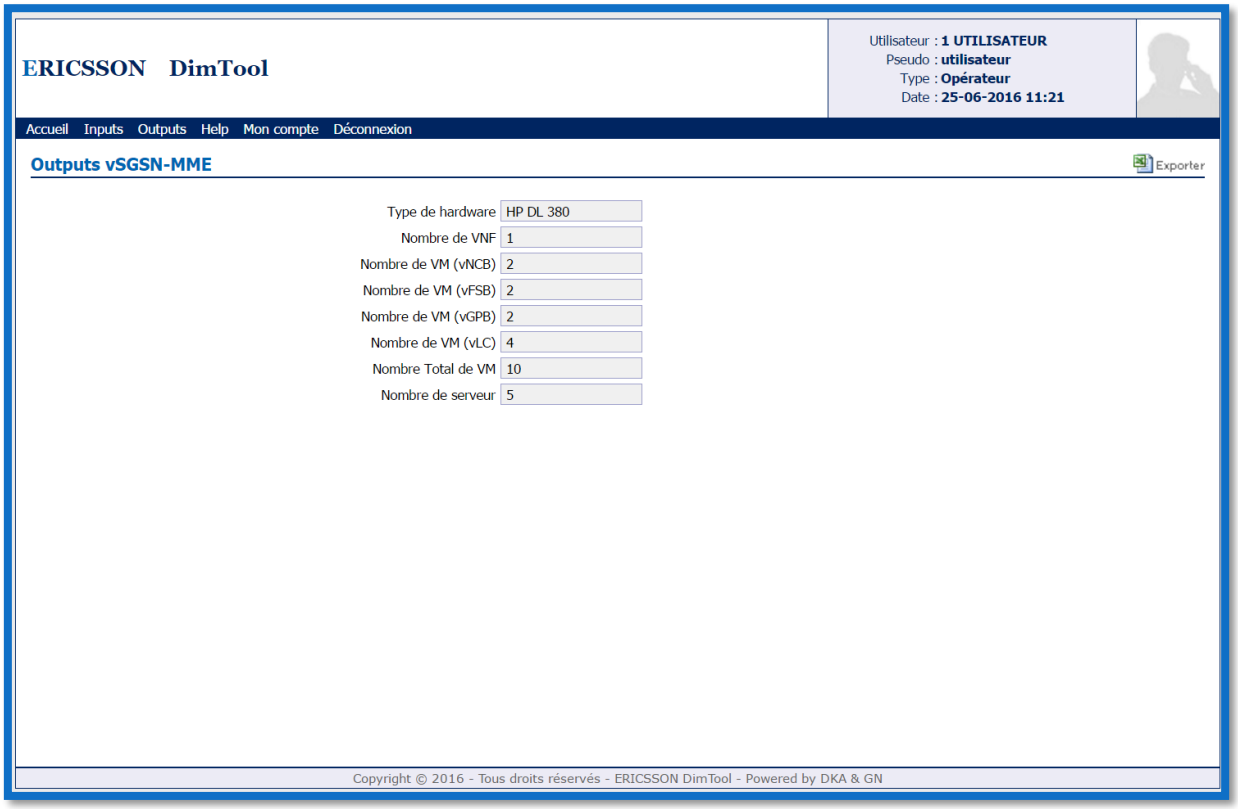

Figure 4.20 Outputs vSGSN-MME

La figure 4.20 représente les outputs pour le dimensionnement d'un vSGSN-MME pour le cas d'utilisation du Mobile Broadband.

4.7.2 Cas d'utilisation n°2 : Le Smart Metering :

Les différents paramètres introduits en entrées et les résultats obtenus sont illustrés dans les figures suivantes.

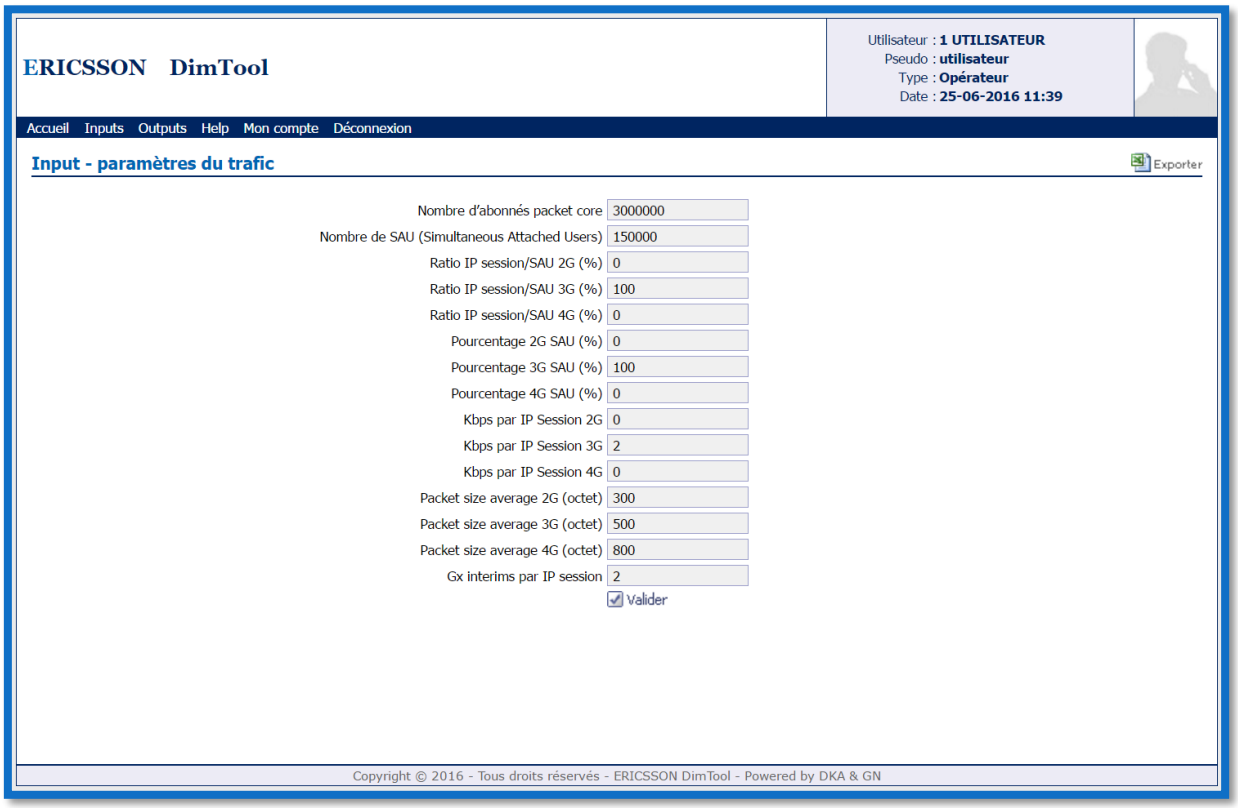

Figure 4.21 Inputs trafic du cas d'utilisation "Smart Metering"

Dans cette exemple, on prendre 3 millions d'abonnés utilisant le Smart Metering, 150000 mesures sont envoyés simultanément. A partir de ces paramètres le système va calculer le trafic que génèrent ces abonnées, et le nombre de hardware nécessaire pour le dimensionnements des nœuds vEPC.

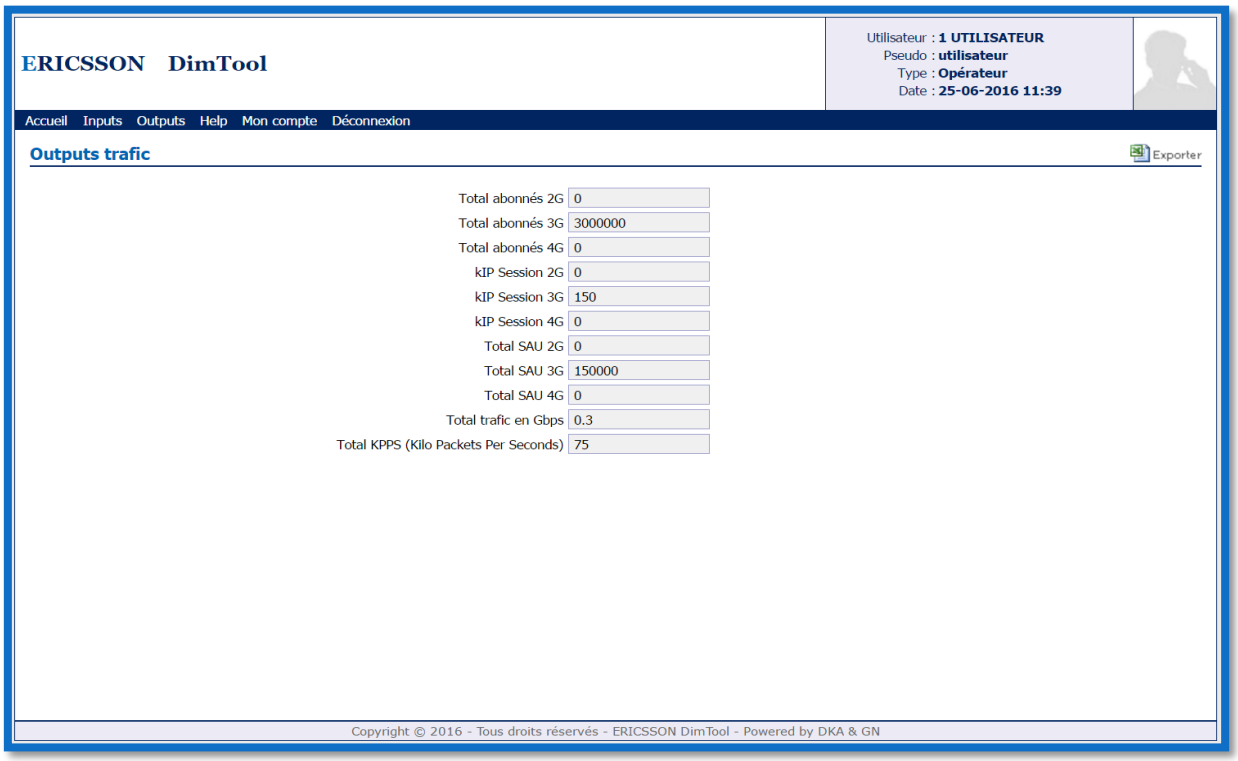

Figure 4.22 Outputs trafic

Le trafic généré est de 300 Mbps et de 75 KPPS pour le nombre d'abonnés précédent.

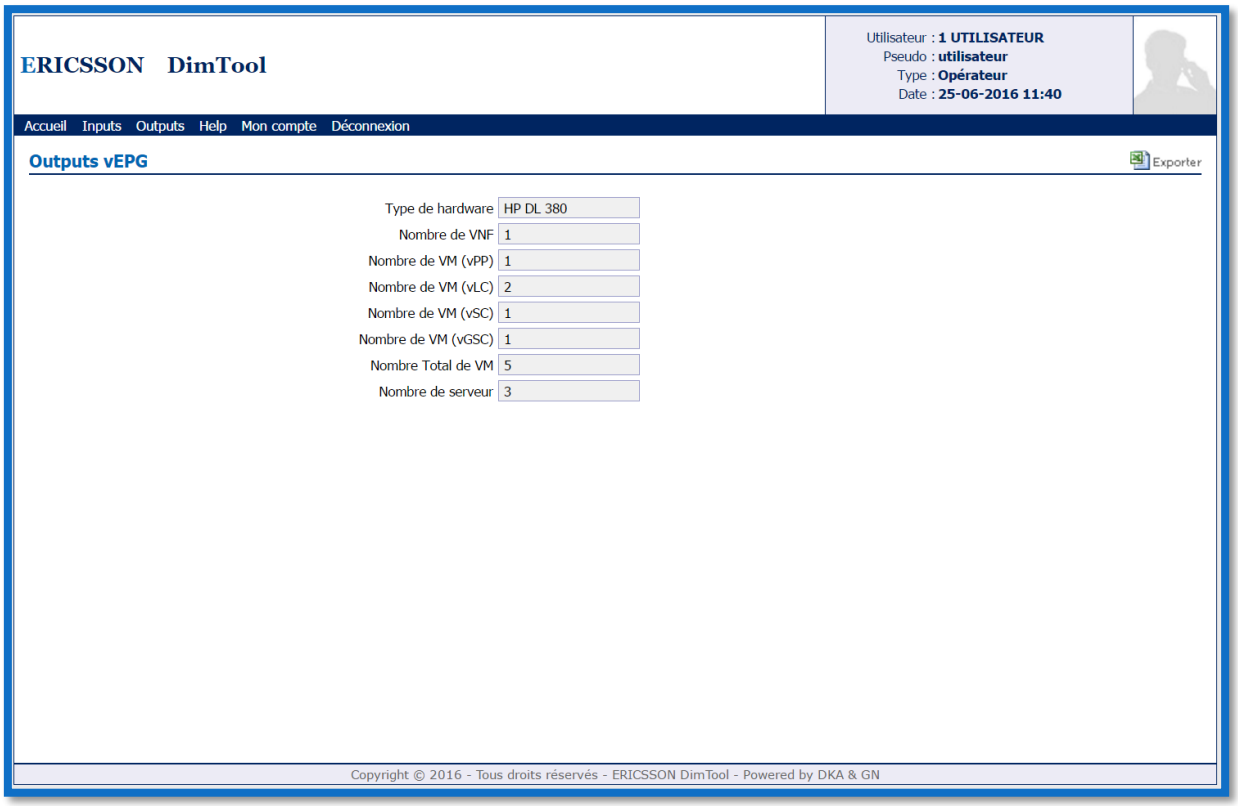

Figure 4.23 Output vEPG

La figure 4.23 représente les outputs pour le dimensionnement d'un vEPG pour le cas d'utilisation du Smart Metering.

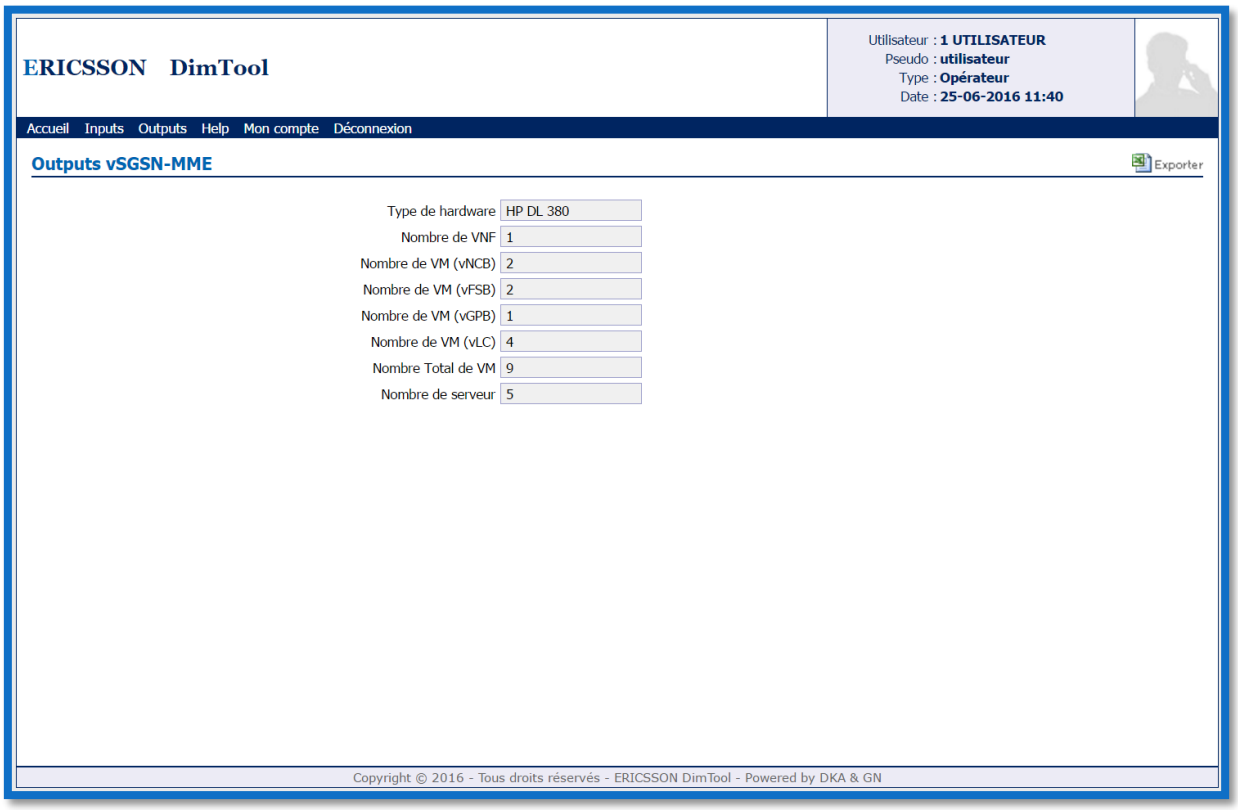

Figure 4.24 Outputs vSGSN-MME

La figure 4.24 représente les outputs pour le dimensionnement d'un vSGSN-MME pour le cas d'utilisation du Smart Metering.

4.8 Conclusion :

Dans ce dernier chapitre, nous avons présenté l'aboutissement de notre travail qui rentre dans le cadre de notre projet de fin d'études. Nous avons exposé l'application DimTool et ses fonctionnalités à travers des captures d'écran, représentant ainsi les différentes interfaces d'entrées et sorties permettant le dimensionnement d'un réseau cœur virtualisé vEPC. Nous avons pu tester l'application pour deux cas d'utilisation, le mobile Broadband et le Smart Metering.

Conclusion générale :

Notre projet de fin d'études a porté sur la conception et le développement d'un outil de dimensionnement de réseau cœur paquet virtualisé vEPC. Cette application permet de dimensionner en toute aisance les nœuds d'un réseau cœur, plus exactement les nœuds vEPG, vSGSN-MME, et vSAPC (vPCRF). Ainsi face à une certaine charge de trafic générée par les abonnés du réseau mobile, ou bien par des applications IoT (Internet of Things) qui vont enregistrer une nette recrudescence dans les années à venir, l'application est en mesure de déterminer le nombre adéquat de Hardware (serveur) pour dimensionner ces nœuds virtuels, tout en spécifiant les VM (Virtual Machine) et les VNF contenu dans ces serveurs.

Tout au long de ce projet, nous avons pu acquérir de solides bases sur le réseau cœur de quatrième génération et nous imprégner de connaissances technologiques nouvelles, telles que le SDN (Software-Defined Networking) et le NFV (Network Function Virtualisation) qui sont le fer de lance des futures générations de réseaux mobiles. Ces deux technologies ont été rendu possibles par l'introduction de la virtualisation dans les réseaux.

Le travail que nous avons effectué s'avère une solution tout à fait naturelle pour faire face à l'augmentation du nombre d'abonnée et leur engouement pour les applications de plus en plus gourmandes en termes de débit et de bande passante. L'apparition des objets connectés (IoT) et leurs flots massifs de données (Big Data) conjugué aux exigences des abonnées ont amené à repenser les architectures rigides et figés actuelles. Ce qui donne lieu à des réseaux virtuels très automatisés, notamment le réseau vEPC qui est une solution beaucoup plus flexible permettant entre autre le déploiement de nouveaux services rapidement.

L'horizon des réseaux mobiles s'entrevoit avec la virtualisation sous forme de fonctions réseau virtualisées (VNF) exécutés dans des VM se trouvant dans des datacenters qui forment le Cloud. Le SDN permet de contrôler ces réseaux logiciels, il permet selon l'application ou services souhaité d'ouvrir un réseau virtuel avec les ressources nécessaires et avec la bonne qualité de service et non pas une QoS globale. Ces technologies vont se généraliser plus concrètement avec l'arrivé de la cinquième génération fortement virtualisée. En perspective de notre travail il serait intéressant d'envisager le déploiement des systèmes IoT pour le développement des différents secteurs (banques, hôpitaux, universités, etc.).

Glossaire

2.5G : 2ème Génération de réseau de télécommunication mobile améliorée
2G+ : 2ème Génération de réseau de télécommunication mobile améliorée
3G : 3ème Génération de réseau de télécommunication mobi
3GPP : 3rd Generation Partnership Project
4G : 4ème Génération de réseau de télécommunication mobile
5G : 5ème Génération de réseau de télécommunication mobile

A

ADC : Automated Device Configuration
ADD : Automated Device Detection
API : Application Programming Interface
APN : Access Point Name
AuC : Authentification Center
AUTN : Authentification Number

B

BSC : Base Station Controller
BSS : Base Station Subsystem
BSS : Business Support System
BTS : Base Tranceiver Station

C

Cat 0 : Catégorie 0
Cat 1 : Catégorie 1
CCCH : Common Control Channel
CDMA : Code Division Multi Access
COTS : Commercial Off-The-Shelf
CPU : Central Processing Unit
C-RAN : Cloud-Radio Access Network

D

D2D : Device to Device
DPI : Deep Packet Inspection
DRB : Data Radio Bearer

E

ECGI : Evolved Cell Global Identifier
EC-GSM : Extented Coverage-Global System Mobile

ECM : EPS Connection System
EIR : Equipement Identity Register
EMM : EPS Mobility Management
EMS : Element Mangement System
eNode B : evolved Node B
EPC : Evolved Packet Core
EPG : Evolved Packet Gateway
EPS : Evolved Packet System
E-RAB : E-UTRAN Radio Access Bearer

F

FDMA : Frequency Division Multi Access

G

GGSN : Gateway GPRS Support Node
GPRS : General Packet Radio Service
GSM : Global System for Mobile communication

H

HLMN : Home Land Mobile Netwok
HLR : Home Location Register
HSS : Home Subscriber Server

I

IaaS : Infrastructure as a Service
IMS : IP Myltimedia Subsystem
IMSI : International Mobile Subscriber Identity
IoT : Internet of Things
IP : Internet Protocole
IP-TV : IP télévision
IP v4 : Internet Protocole version 4
IP v6 : Internet Protocole version 6

K

KDF : Key Derivation Function
KPI : Key Performance Indicator

L

LPWA : Low Power Wide Area
LTE : Long Term Evolution
LTE-M : Long Term Evolution-Machine Type Telecommunications

M

M2M : Machine to Machine
MANO : Management and Network Orchestration
MME : Mobility Management Entity
MS : Mobile Station
MSC : Mobile service Switching Center
MTC : Machine Type Telecommunication
MVNO : Mobile Virtual Network Operator

N

NAS : Non Access Stratum
NB-IoT : NarrowBande IoT
NFV : Network Function Virtualisation
NFVI : Network Function Virtualisation Infrastructure
NMT : Nordic Mobile Telephone
NOS : Network Operating System
NSS : Network Subsystem

O

OMC : Operation and Maintenance Center
ONF : Open Network Foundation
OSS : Operations Support System

P

PaaS : Plateform as a Service
PCEF : Policy Control Enforcement Function
PCRF : Policy Control Charging Rules Function
PCU : Packet Controler Unit
PDN : Packet Data Network
P-GW : PDN-GW, Packet Data Network Gateway
PLMN : Public Land Mobile Network

Q

QCI : QoS Class Identifier
QoS : Quality of Service

R

RAM : Random Access Memory
RAP : Radio Access Point
RES : authentication RESult
RFID : Radio Frequency Identification

RNC : Radio Network Controller
RRC : Radio Ressource Control

S

SaaS : Software as a Service
SAU : Simultaneous Attached Users
SDN : Software-Defined Networking
SGSN : Serving GPRS Support Node
S-GW : Serving Gateway
SQN : Sequences Number
SRB : Signal Radio Bearer

T

TAI : Tracking Area Identifier
TDMA : Time Division Multi Access

U

UE : User Equipment
UMTS : Universal Mobile Telecommunications System
UTRAN : Universal Terrestrial Radio Access Network
UWB : Ultra Wide Band

V

vEPC : virtual Evolved Packet Core
vEPG : virtual EPG
vSGSN-MME : virtual SGSN-MME
vSAPC : virtual SAPC
VIM : Virtualized Infrastructure Manager
VLR : Visited Location Register
VM : Virtual Machine
VNFM : Virtual Network Function Manager
VNFO : Virtual Network Function Orechtrator
VoIP : Voice over IP
VPN : Virtual Private Network

W

WCDMA : Wideband Code Division Multi Access
WiFi : Wireless Fidelity

X

XRES : Expected authentication Result

Références bibliographiques:

[1] : Claude Servin. « Réseaux et Télécommunications ». Edition Dunod, Paris, 2003.

[2] : Guy Pujolles. « Les Réseaux édition 2014 ». Edition Eyrolles, Paris, 2014.

[3] : Guy Pujolles. « Réseaux Logiciels ». Edition ISTE, Paris, 2015.

[4] : Yannick Bouguen, Eric Hardouin, François-Xavier Wolff. « LTE et les réseaux 4G ». Edition Eyrolles, Paris, 2010.

Références Webographiques

[5] : http://fr.slideshare.net/mustahidali90/umts-31480722

[6] :https://www.google.dz/search?q=architecture+4G&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjn1660_6TNAhUB1x4KHfZiD9kQ_AUICCgB#imgrc=eLoDlwZy7CaQeM%3A

[7] : http://sparc.nfu.edu.tw/~sylien/Publications/Conference/120-Efficient_Network_Structure_of_5G_Mobile_Communications.pdf

[8] : https://www.ericsson.com/news/160106_ericsson_delivers_massive_iot_244039856_c

[9] : http://www.netmanias.com/en/post/techdocs/6102/attach-emm-lte/emm-procedure-1-initial-attach-part-2-call-flow-of-initial-attach

[10] : https://s.nsit.com/fr01/fr/content/shop/netgear/la_virtualisation_de_serveurs.pdf

[11] : http://www.business-review.eu/featured/cloud-cover-increasing-42420/attachment/cloud-computing-virtual-machine-motion

[12] :http://www.medinsoft.com/website/custom/module/cms/content/file/Ce_qu_il_faut_savoir_sur_le_Cloud....pdf

[13] : http://searchsdn.techtarget.com/answer/NFV-vs-VNF-Whats-the-difference

[14] : http://www.intel.fr/content/dam/www/public/emea/fr/fr/documents/white-papers/end-to-end-optimized-nfv-paper.pdf

[15] : http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2014/10350-journey-packet-core-virtualization.pdf

[16] : https://www.ericsson.com/research-blog/

[17] : http://www.orange-business.com/fr/blogs

[18] : https://www.sdxcentral.com/

[19] : http://www.reseaux-telecoms.net/actualites/lire-quelles-differences-entre-nv-nfv-et-sdn-26704.html

[20] : http://www.lemagit.fr/actualites/2240228195/Les-bases-du-SDN-comprendre-les-atouts-de-la-programmabilite-et-du-controle-centralise

[21] : https://search.cisco.com/search?query=nfv&locale=enUS&tab=Cisco

[22] : http://www.phpdebutant.org/article118.php

[23] : https://openclassrooms.com/courses/concevez-votre-site-web-avec-php-et-mysql

[24] : http://www.etsi.org/news-events/news/864-2015-01-press-etsi-network-functions-virtualisation-completes-first-phase-of-work

[25] : http://www.ericsson.com/res/ourportfolio/pdf/ericsson-academy/education-centers/packet-core-network.pdf