Nom, prénom : **Lacroix Bastien** Responsable pédagogique UTT : **Mr Patrick Lallemand** Stage: ☐ TN09 ☐ TN10 ☑ **TN30**	Branche : **SRT – TMSE / M2 - SSI** Année : **2016** Semestre : **Automne**

Université de technologie de Troyes

Intégrateur système 4G/LTE

Résumé

Dans le cadre de ma formation d'ingénieur à l'Université de technologie de Troyes, j'ai effectué mon stage de fin d'études au sein du service PMR de Thales Communication & Security. Les offres PMR s'inscrivent dans un contexte de renouvellement, afin de proposer des solutions très haut débit, reposant notamment sur la technologie 4G/LTE. L'objectif de ce stage était de travailler sur des systèmes de communication 4G/LTE à travers la réalisation et l'intégration d'applications innovantes.

Ainsi, j'ai pu travailler dans le cadre d'un projet, sur la mise en place d'une architecture réseau dédié 4G/LTE et intégrer les différents services PMR. Ces intégrations ont servi à plusieurs démonstrations pour des clients et partenaires.

J'ai aussi pu mettre en place une interconnexion avec un autre réseau 4G/LTE, cette fois-ci publique, via une connexion sécurisée.

Ce stage a été très enrichissant à différents niveaux, et m'a notamment permis d'affiner mon projet professionnel.

Entreprise : **Thales Communication & Security**

Lieu : **Vélizy-Villacoublay**

Responsable : **Mr Eric Robert**

Mots clés (CF Thésaurus)

Logiciel - Recherche
Réseau mobile
Sécurité des systèmes
Informatique

utt université de technologie Troyes

Remerciements

Au cours de ce stage, j'ai eu l'occasion de travailler avec de nombreuses personnes qui ont pu m'aider dans les différentes intégrations, qui ont su m'aiguiller correctement au cours de mes recherches et qui ont pris le temps de me transmettre leur savoir-faire. Je tiens d'abord à remercier l'ensemble du service Wireless Network (WNW) de l'entité Thales Communications & Security de Vélizy.

Je souhaite remercier en particulier mon responsable de stage Eric pour m'avoir permis de réaliser ce stage dans le domaine de la 4G et de m'avoir fourni les outils nécessaires à la réalisation des missions. Eric m'a aussi offert une grande liberté d'actions pour mes recherches.

Je remercie Alicia, une stagiaire qui m'a précédé, pour l'ensemble des connaissances qu'elle m'a apporté et pour les projets réalisés ensemble.

Je remercie Christophe ainsi que Sandrine et Claire qui ont toujours su trouver des disponibilités pour m'aider lorsque je rencontrais des difficultés sur mes missions au niveau de l'intégration système.

Je remercie également Eric, Laurent et Stéphane pour m'avoir aidé dans certaines mises en place d'architecture et équipements réseaux.

Je remercie Emmanuelle et Marc pour m'avoir permis d'assister à la démonstration devant le ministère de l'intérieur.

J'adresse mes remerciements à Corinne pour son aide dans la gestion administrative de mon profil au sein du groupe Thales.

Enfin, je souhaite remercier les apprentis et les autres stagiaires pour m'avoir permis de m'intégrer au sein de l'équipe et avoir pu travailler dans une atmosphère conviviale.

Sommaire

Table des figures

Glossaire

Android	Système d'exploitation mobile basé sur un noyau Linux
Asa 5505	Equipement Cisco. Permet de créer un lien VPN et de mettre en œuvre des politiques de sécurité
Bash	Interpréteur en ligne de commande de type script.
BSC	Base Station Controller, gère et contrôle les antennes dans une architecture 2G.
DSI	Direction des Systèmes d'Information
eNobeB	Evolved Node B, c'est la station de base, l'antenne dans les architectures des réseaux 4G
EPC	Evolved Packet Core, désigne le cœur de réseau 4G
E-UTRAN	Evolved Universal Terrestrial Radio Access Network, désigne la partie radio ou réseaux d'accès, des réseaux 4G.
HSS	Home Subscriber Server, base de données des utilisateurs
IMSI	International Mobile Subscriber Identity, numéro unique permettant à un usager de s'identifier sur un réseau mobile (2G, 3G ou 4G).
IP	Internet Protocol
IPSEC	Internet Protocol Security, c'est un protocole agissant à la couche 3 qui permet d'authentifier et chiffrer des données, et qui est souvent utilisé dans les VPN.
IVVQ	Intégration Vérification Validation Qualification
LTE	Long Term Evolution, désigne la 4ème génération des réseaux mobiles.
MME	Mobility Management Entity
NAT	Network Address Translation, correspondance ente des adresses IP internes (souvent non routables) et des adresses IP externes et routables.
PCRF	Policy and Charging Rules Function
PGW	Packet Gateway
PLMN	Public Land Mobile Network, c'est un réseau de télécommunications permettant l'accès à différents services, pour les utilisateurs autorisés.
PMR	Professional Mobile Radio
PoC	Proof of Concept, une démonstration de faisabilité.
Python	Langage de programmation objet multiplateforme.
RNC	Radio Network Controller, contrôle les transmissions radio des antennes (Node B) en 3G. C'est l'équivalent des BSC en 2G.
SGW	Serving Gateway

SIM	Subscriber Identity Module, puce permettant de stocker les informations spécifiques à un abonné d'un réseau mobile.
SIP	Session Initation Protocol, protocole de gestion de session utilisé pour divers média (son, image, etc.). Il est largement utilisé pour la VoIP.
SSL	Secure Sockets Layer, c'est un protocole qui permet d'assurer des fonctions de sécurité, telles que l'authentification, la confidentialité et l'intégrité de données.
TCP	Protocole de transport de données synchrone, garantissant l'intégrité et la réception des données.
Tetra	TErrestrial Trunked RAdio, système de radio numérique mobile professionnel, à destination notamment l'armée, des services de secours et des services de transport public.
UDP	Protocole de transport de données asynchrone, ne garantissant ni l'intégrité ni la réception des données.
UE	User Equipment, désigne l'appareil utilisé pour se connecter à un réseau 3G ou 4G, comme un Smartphone, une tablette ou encore un ordinateur muni d'une clé 4G (ou 3G).
VLAN	Virtual Local Area Network, réseau local virtuel regroupant des machines de façon logique.
VMs	Virtual Machines, ordinateur sans matériel physique, « émulé » sur un hôte physique
VoIP	Voice over IP, technologie permettant de faire du transport de voix sur réseaux IP.
VPN	Virtual Private Network, système permettant de mettre en place une liaison sécurisée entre 2 ordinateurs, en passant par un réseau public comme Internet.
Cisco	Entreprise informatique américaine spécialisée, à l'origine, dans le matériel réseau.
XML	« eXtensible Markup Language ». Langage à balises qui définit du contenu dans une arborescence structurée.
WireShark	Logiciel écoutant le trafic des trames sur le réseau.

I. Le contexte de travail

A. Identité de l'entreprise

1. Le groupe Thales

Thales est le résultat d'une longue histoire, comprenant entre autres la fusion et la réorganisation de plusieurs grandes entreprises technologiques, telles que Dassault Electronique, Alcatel et Thomson-CSF. On peut ainsi résumer l'évolution du groupe en quelques dates clefs (figure 1)

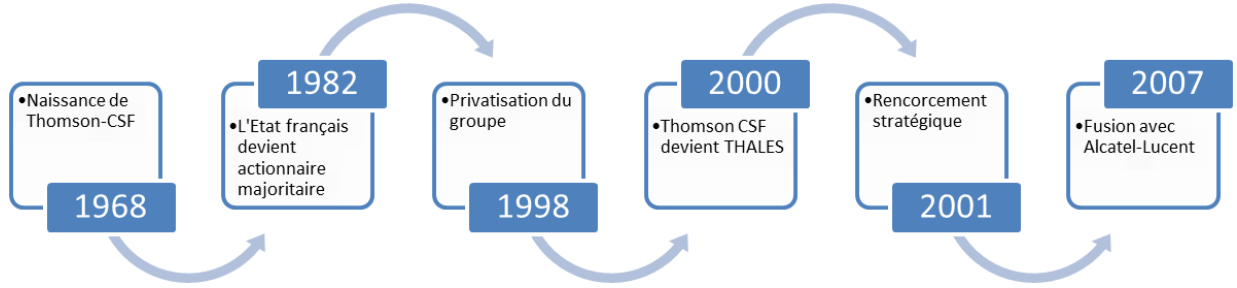


Figure 1 - Dates clefs de l'évolution du groupe

1968 : Fusion de la Compagnie Générale de Télégraphie et des activités électroniques de Thomson-Brandt pour devenir Thomson-CSF.

1982 : Nationalisation de Thomson qui est au bord de la faillite

1998 : Alcatel et Dassault Industries entrent majoritairement dans le capital. L'entreprise se recentre sur les domaines de la défense et de l'électronique industrielle.

2000 : Thomson-CSF devient THALES, et annonce un partenariat avec l'Américain Raytheon dans le domaine de la défense (aujourd'hui Thales Raytheon).

2001 : Thales renforce ses compétences et son engagement dans les segments les plus technologiques de l'industrie de la défense, suite aux attentats du 11 Septembre 2001.

2007 : Alcatel transfère ses activités transport, sécurité et aéronautique vers Thales.

2009 : Dassault Aviation achète les parts d'Alcatel-Lucent et entre dans le capital de Thales.

2011 : Thales fusionne deux filiales pour créer la nouvelle société Thales Communications & Security.

2014 : Thales reprend les activités de services de cyber-sécurité d'Alcatel-Lucent

2015 : Acquisition de l'entreprise américaine Vormetric, spécialisée dans la protection des données des entreprises et leur chiffrement.

2. Les activités de Thales

Aujourd'hui, Thales est un groupe d'électronique spécialisé dans l'aérospatial, la défense et les technologies de l'information. Thales est présent dans les domaines militaire et civil, et divisé en 5 grands domaines d'activité :

- **Défense**
  Thales conçoit des systèmes qui servent aussi bien les milieux traditionnels (air, terre, mer espace) que les nouveaux environnements (combat urbain, cyberguerre). De la conception des systèmes jusqu'au maintien en condition opérationnelle et à la formation du personnel, Thales assure un service complet de la conception du produit jusqu'à sa mise en place opérationnelle

- **Sécurité**
  Thales propose des solutions intégrées et résilientes qui permettent à ses clients de mieux protéger les citoyens, les données sensibles et les infrastructures. Il se distingue par sa capacité d'intégrateur de systèmes complexes et son aptitude à tirer parti des solutions déjà existantes chez ses clients.

- **Aéronautique**
  Thales fournit des équipements, des systèmes et des services, à bord des aéronefs au sol, et aide ainsi ses clients à relever les défis qui se posent à eux : croissance, sureté, efficacité économique et environnementale, sécurité. Ses positions dans le domaine de l'avionique, de la gestion du trafic aérien et du spatial font de Thales le groupe mondial capable de répondre aux défis du transport aérien.

- **Espace**
  Thales offre une combinaison exceptionnelle d'expertises couvrant l'ensemble de la chaîne de valeur : équipements charges utiles, satellites, systèmes et services. Cette activité permet au groupe d'apporter des réponses globales aux besoins de ses clients et d'être un acteur majeur des plus grands programmes civils et militaires.

- **Transport terrestre**
  Thales élabore des systèmes et services permettant d'accroître la capacité des infrastructures de transport et d'acheminer les voyageurs et les marchandises plus rapidement à un coût moindre et dans des conditions de sécurité optimales. Il développe des solutions innovantes, fondées sur des technologies de pointe : systèmes CBTC (Communication-Based Train Contol), ETCS (European Train Control System), carte sans contact, etc...

3. Le système de management du groupe

Le système de management du groupe, Chorus 2.0, est structuré en processus. Pour chacun d'eux, il définit les rôles activités, revues et documents ainsi que les règles et modalités d'ajustement. Il inclut également le système de vérification de l'application des processus ainsi que les éléments de formation associés.

Ce système unique est commun à toutes les entités, adaptable au contexte opérationnel local et conçu pour donner à chaque collaborateur du groupe un accès simple aux éléments dont il a besoin pour la réalisation de sa mission.

Il permet le renforcement du rôle de la qualité pour l'ensemble des étapes clés des processus, respecte les niveaux d'exigences requis par les normes et standards applicable, et favorise un partage des meilleurs pratiques et le travail collaboratif.

Il contribue à renforcer l'efficacité individuelle et collective en favorisant le déploiement de processus optimisés dans l'ensemble du Groupe.

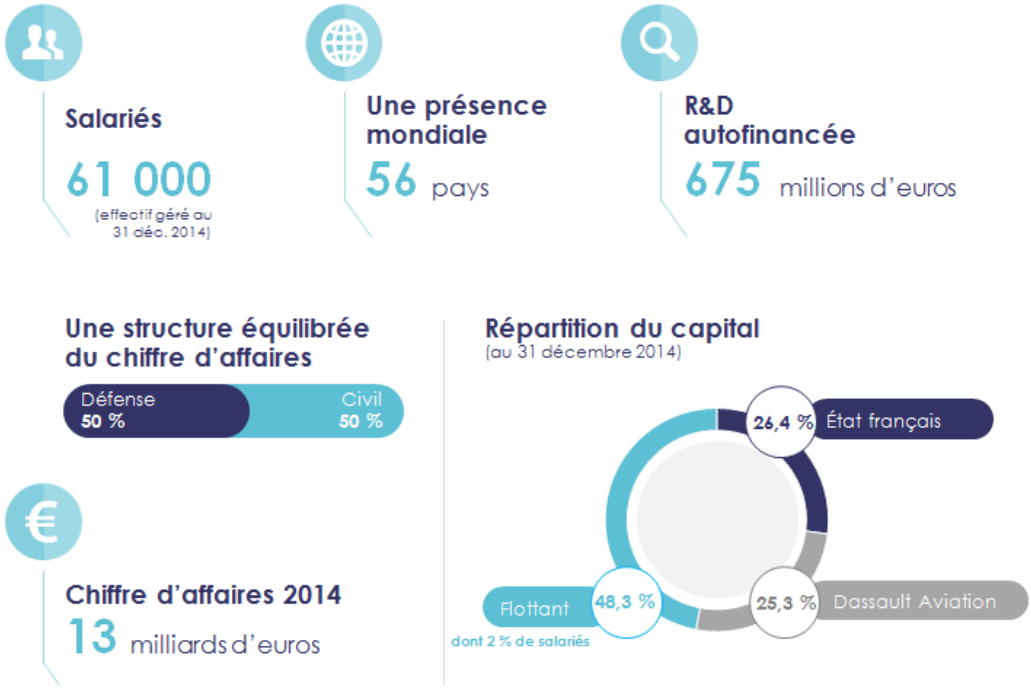


Figure 2 : Chiffre clef et répartition du capital de Thales

4. L'entité Thales Communication & Security

Thales Communications & Security est une société créée par le groupe Thales le 1er Juillet 2011. Elle est le fruit de la fusion de deux sociétés du Groupe :

- Thales Communications, spécialisée dans les produits et systèmes d'information et de communication sécurisés pour les forces armées et de sécurité.

- Thales Security Solutions & Services, société dédiée aux systèmes de sécurité urbains, de protection des infrastructures critiques et des voyageurs.

Avec cette nouvelle société, Thales souhaite conforter sa position de leadereuropéen des systèmes d'information et de communication sécurisés pour les marchés mondiaux de la défense, de la sécurité et du transport terrestre.

Par rapport à l'organigramme de la figure 3, le service Wireless Network, dans lequel j'ai travaillé, appartient à la direction des Réseaux Mobiles du domaine Réseaux & Système d'Infrastructure.

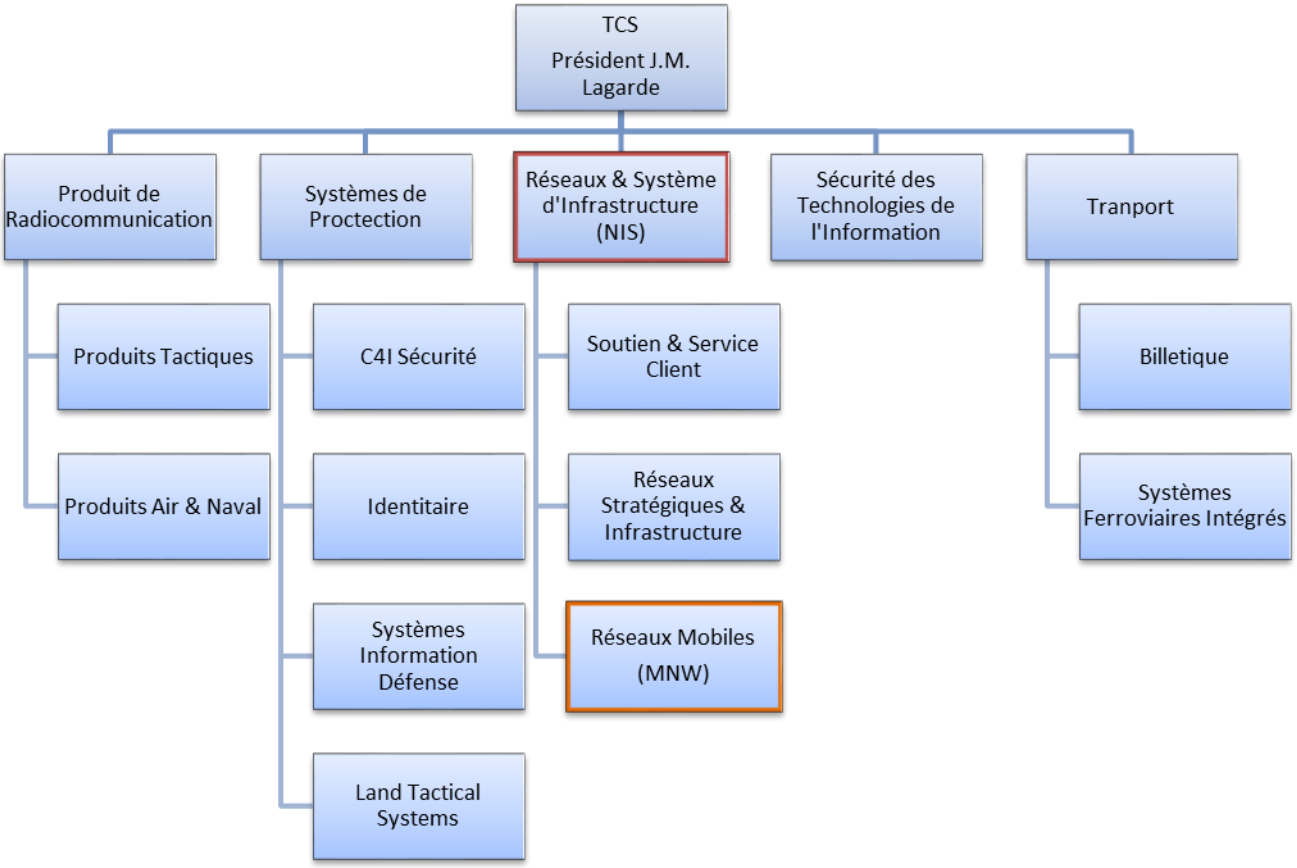


Figure 3 - Organigramme de Thales Communications & Security

B. Problématiques et objectifs

1. Ma position dans la structure

Le domaine Réseaux Mobiles (MNW) est composé de trois services :

- **Satcom & Réseaux de Théâtre (SRT)**, spécialisé dans les systèmes de transmissions satellites.
- **Satcom & Deployable Network (SDN),** spécialisé dans les réseaux tactiques.
- **Wireless NetWork (WNW),** spécialisé dans les systèmes de radio professionnels.

Le secteur WNW (Wireless Networks) dans lequel j'ai effectué ma mission est plus connu sous son ancien nom « Professional Mobile Radio » ou « Private Mobile Radio » (PMR). On parle de réseau de communication « professionnel », car les infrastructures déployées sont à destination de forces de sécurité publique, d'opérateurs d'infrastructures vitales ou d'entreprises privées. On emploie le terme « privé », car les utilisateurs de ces réseaux en sont généralement propriétaires. La PMR désigne ainsi un système de communication radio mobile, utilisé sur courtes ou moyennes distances, et dont le talkie-walkie, inventé en 1943 par Motorola, est le précurseur. Avec le temps, ce type de système de communication est devenu une référence pour les forces de sécurités. Par la suite, de nouveaux systèmes de radio mobiles professionnelle sont apparus, tel que le TETRA (TErrestrial Trunked RAdio) et beaucoup plus récemment des solutions très haut débit multimédia

exploitant la technologie 4G/LTE.

La capacité d'échanger des informations clés avec précision et en temps réel est essentielle au succès d'une opération et à la sécurité des équipes sur le terrain. L'échange d'informations multimédias est maintenant une exigence essentielle, à la fois pour améliorer la connaissance de la situation et pour fournir aux forces sur le terrain l'accès en temps réel aux données critiques et services vidéo. Ces nouveaux systèmes, tel que celui développé au sein du service, intègrent des fonctionnalités vocales comme le Push-To-Talk ainsi que des applications de données à large bande stratégiques dans un format robuste, avec une connectivité et une sécurité totale (garantie de service en cas de crise). Parmi les principaux utilisateurs de ces réseaux, on retrouve entre autres : la police nationale, la gendarmerie, les pompiers, les ports, la SNCF, les réseaux autoroutiers, des municipalités, des régies de transport urbains etc…

2. Contexte de travail

Mon travail s'est inscrit dans un contexte de renouvellement des offres en PMR de Thales, qui met en place de nouveaux systèmes basés sur la technologie 4G/LTE.

Le secteur WNW repose sur 5 services : Stratégies & Marketing, Produits et Système, Offres, Projets, et Design Authority. C'est au sein de ce dernier que j'ai eu l'occasion de travailler sur des projets mettant en œuvre des systèmes PMR exploitant la technologie 4G/LTE. J'ai eu également l'opportunité de participer à des démonstrations des services dans un contexte réel. Ainsi qu'être responsable d'un des partenaires d'un projet lors d'une conférence. Enfin, j'ai pu évoluer sur des missions visant à développer des idées innovantes, permettant de mettre en avant les possibilités offertes par le LTE.

C. Objectifs du stagiaire

1. Le stage

L'intitulé de mon stage est « Intégration et évaluation de performances d'un système de communication PMR 4G/LTE ».

C'est un sujet assez large, au sein duquel j'avais deux objectifs principaux :

- Réaliser des tests fonctionnels sur un système 4G/LTE donné
- Intégrer des applications innovantes sur le système, en particulier des services multimédia mobiles

En parallèle de ces deux objectifs, j'ai pu participer à des présentations et des démonstrations sur les différents outils que proposaient le service PMR et les entreprises partenaires du projet.

De façon générale, mon stage avait un périmètre assez large. De ce fait, avant de débuter, je n'avais pas de connaissances détaillées des tâches que j'allais réaliser. Ce périmètre s'est défini plus précisément à mon arrivée, en permettant de s'adapter aux différents besoins de mon tuteur et particulièrement à ceux du projet dans lequel mes missions se sont définies.

2. La temporalité des missions

Je vais détailler ici les deux principaux axes qui ont représenté dans l'ensemble la majeure partie de mon stage et qui, d'après moi, s'intègrent au mieux dans la continuité de ma formation ingénieur.

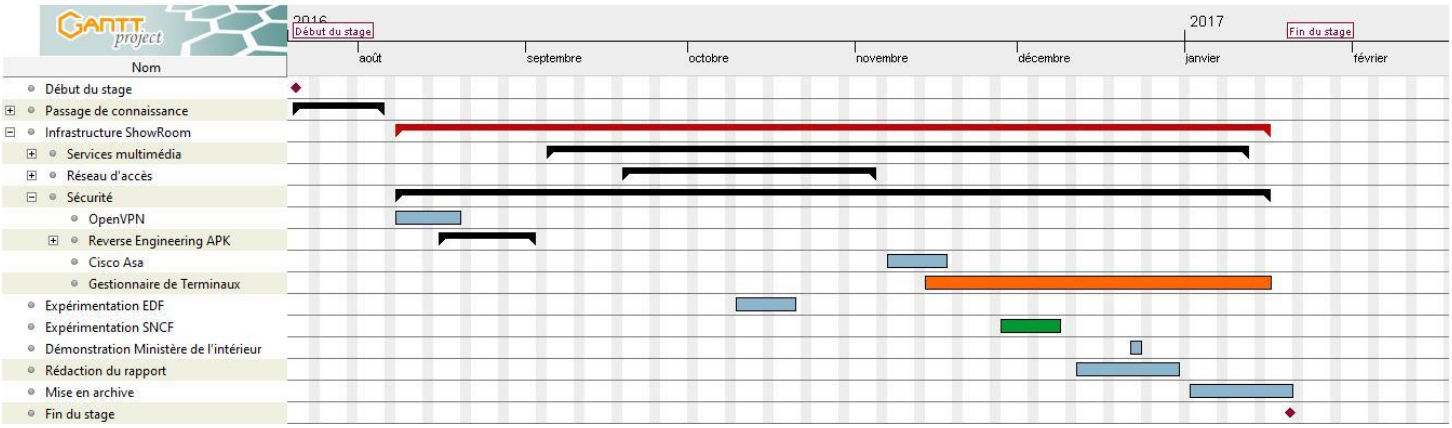


Figure 4 : Diagramme de Gantt réduit de la répartition des missions du stage

Tout au long de ce stage j'ai été amené à travailler sur différentes missions et sujets. Néanmoins, chacun de mes travaux ont été réalisé pour un seul et même objectif : l'évolution de la plateforme de démonstration du ShowRoom. Chacune des missions seront détaillées dans ce rapport. Je n'avais pas d'objectifs temporels fixés, c'est pour cela que le diagramme de Gantt ci-dessus n'est pas un diagramme prévisionnel, mais celui représentant la répartition réelle de mon travail dans le temps. Ce diagramme n'est qu'une représentation réduite de toutes les taches effectuées afin de montrer les principaux axes. Une version complète se trouve en Annexe 1.

La mission sur l'intégration du gestionnaire de terminaux, qui sera vue dans la dernière partie de ce rapport, a pris place au sein d'une mission plus large, à savoir un travail en collaboration avec l'entreprise Ibelem du projet Fed4pmr. Cette collaboration consistait d'une part à étudier et améliorer le fonctionnement du gestionnaire de terminaux dans le cadre des projets PMR du service et d'autre part je jouais un rôle central lors des différentes discussions et présentations de leur produit au sein du service.

J'ai tenu aussi à mettre en valeur l'expérimentation à la SNCF pour le projet Fed4pmr. C'était personnellement l'occasion d'avoir un contact avec les clients et d'avoir une vue d'ensemble sur le système sur lequel le service travail. Par ailleurs, Ibelem étant partenaire du projet, devait avoir la possibilité de montrer leur produit durant la journée de démonstration. J'étais donc responsable de leur stand et je devais leur fournir un accès au gestionnaire de terminaux intégré sur la plateforme du ShowRoom.

Enfin, le premier mois, j'ai accompagné la précédente stagiaire sur une plateforme dédié pour un projet EDF. Je n'ai pas pris en compte cette mission dans le diagramme car j'étais plus spectateur qu'acteur. Par ailleurs, je n'ai pas continué dessus après son départ. La plateforme du ShowRoom a été pendant le reste du stage ma plateforme de recherche, de développement et m'a permis d'apprendre beaucoup techniquement.

II. Présentation du domaine de la 4G

A. Un peu d'histoire

En l'espace d'une vingtaine d'année, l'usage des services de communications mobile a connu un essor remarquable. On compte depuis la fin de 2011, près de 6 milliards d'abonnés à travers le monde. C'est un nouveau secteur de l'industrie mondiale qui s'est créé, regroupant notamment des constructeurs de terminaux mobiles, constructeurs d'infrastructures de réseaux, de développeurs d'application et des services et opérateurs de réseaux mobiles.

1. Les premières générations

Plusieurs générations de réseaux mobiles se sont succédées depuis leur début dans les années 1970. La première génération de réseaux mobiles est caractérisée par une multitude de technologie introduites simultanément à travers le monde comme par exemple AMPS (Advanced Mobile Phone System) aux Etats-Unis ou bien encore Radiocom2000 en France. Cette génération ne parvint pas à imposer une norme internationale. L'itinérance était impossible et la capacité des systèmes était très limitée (de l'ordre de quelques appels voix simultanés par cellule).

La deuxième génération de réseaux mobiles (2G) a suivi son prédécesseur dans le nombre de systèmes ayant été définis et déployés à travers le monde. On retrouve le GSM (Global System for Mobile communication) en Europe ou bien le PDC (Personal Digital Communications) au Japon. Les deux nouveautés qu'offraient ces réseaux mobiles étaient la possibilité d'envoyer des messages textes courts, plus connus sous le nom de SMS (Short Message Service) ainsi que l'utilisation du transfert de données à faible débit. Mais c'est en 1990 que le système GSM s'est imposé dans un grand nombre de pays. Actuellement, les réseaux GSM couvrent 90% de la population mondiale.

La troisième génération (3G) regroupe deux familles de technologies ayant connus un succès commercial : l'UMTS (Universal Mobile Telecommunication System), issu du GSM et le CDMA2000 déployé principalement en Asie et Amérique du nord. Nous allons seulement nous intéresser à l'UMTS car c'est la famille de technologie qui va donner naissance au LTE. Cette génération a notamment connu deux évolutions majeures, que nous présenterons brièvement, au cours de son succès. La 3G est caractérisée par une volonté de définir une norme au niveau mondial afin d'offrir aux utilisateurs un service à moindre coût.. Les organismes issus du monde GSM se sont donc regroupés en un consortium appelé 3GPP (3rd Genration Partnership Project). Les innovations associées au système UMTS ont principalement été accès sur le réseau d'accès. Les objectifs étant d'accroitre la capacité du système pour le service voix mais surtout d'améliorer le service de données.

La première évolution est appelée HSPA (High speed packet access) afin d'accroitre les débits possibles et de réduire la latence du système (la latence désigne le temps de réponse du système à une requête de l'utilisateur). L'innovation principale du HSPA concerne le passage d'une commutation circuit sur l'interface radio, où des ressources radio sont réservées à chaque « utilisateur » (UE) pendant la durée de l'appel, à une commutation par paquets, où la station de base décide dynamiquement du partage des ressources entre les UE actifs. Cependant, cette évolution a commencé à montrer leurs limites en termes de capacité avec la mise sur le marché des terminaux tels que les Smartphones et des applications nécessitant un accès quasi continue

au réseau.

Ces limites ont entrainé l'arrivé de la norme HSPA+. C'est un terme qui regroupe plusieurs évolutions techniques visant principalement à améliorer les débits fournis aux utilisateurs, la capacité du système ainsi que la gestion des utilisateurs *always-on.* L'augmentation de la capacité a été rendu possible par l'introduction de nouvelles technologies. De plus, la largeur de bande plus élevé permet au système une gestion plus efficace des ressources spectrale. La fonctionnalité MIMO (Multiple Input Multiple Output) est également introduite pour améliorer les débits en voie descendante.

Le tableau suivant fait l'état des lieux en comparant sur quelques paramètres non exhaustifs entre les différentes technologies vu précédemment.

	GSM/GPRS/EDGE	UMTS	HSPA	HSPA+
Débit Maximal UL	118 Kbits/s	384 Kbits/s	5,8 Mbit/s	11,5 Mbit/s
Débit Maximal DL	236 Kbit/s	384 Kbit/s	14,4 Mbit/s	42 Mbit/s
Latence	300 ms	250 ms	70 ms	30 ms
Largeur de canal	200 kHz	5 MHz	5 MHz	5 MHz avec possibilité de deux canaux simultanés
Technique d'accès multiple	FDMA/TDMA	CDMA	CMDA/TDMA	CDMA / TDMA
Modulation DL	GMSK	QPSK	QPSK, 16QAM	QPSK, 16QAM, 64 QAM
Modulation UL	8PSK	BPSK	BPSK, QPSK	BPSK, QPSK, 16QAM
Bande de fréquences usuelles (MHz)	900/1800	900/2100	900/2100	900/2100

Figure 5 : Comparaison des technologies [tiré de l'UMTS forum, 2010]

2. Introduction au LTE

Le LTE a été envisagé dès novembre 2004 comme l'évolution à long terme de l'UMTS, d'où son nom de Long Term Evolution. Cette nouvelle norme est plus connue sous le nom de quatrième génération, c'est-à-dire 4G. Le LTE n'est en fait pas qu'une simple évolution de la génération précédente HSPA+ mais bien réellement une révolution du fait de son saut technologique utilisé. A l'instar de chaque nouvelle génération de réseau d'accès, le LTE a pour objectif de proposer une capacité accrue et fait appel à une nouvelle technique d'accès à la ressource fréquentielle.

L'émergence du LTE est liée à un croisement de facteurs techniques et industriels qui ont constitué une réelle motivation pour son développement. La première étape des travaux de normalisation du LTE consista à définir les exigences que ce dernier devait satisfaire. L'objectif majeur du LTE est d'améliorer le support des services de données via une capacité accrue, une augmentation des débits et une réduction de la latence. Nous rappelons que la capacité correspond pour une cellule au trafic total maximal qu'elle peut écouler en situation de forte charge au cours d'une période donnée. La latence représente le temps nécessaire pour établir une connexion et accéder au service.

Avec l'explosion des services nécessitant une connexion « *always-on* », la contrainte appliquée sur la capacité en nombre d'utilisateurs simultanés devient forte. Le LTE promet une connexion de plusieurs centaines d'utilisateurs en simultané par cellule. De plus, la technologie LTE doit assurer un débit correct pour chacun d'eux. Les objectifs initiaux de débit maximal définis sont les suivantes. Ces chiffres supposent que l'utilisateur est en présence de deux

antennes en réception et une antenne en émission.

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

De nos jours, ces exigences ont été largement dépassées.

Concernant la latence, elle se décline en deux plans différents : plan de contrôle et plan usager.
L'objectif fixé pour le LTE est d'améliorer la latence du plan de contrôle par rapport à l'UMTS, via un temps de transition inférieure à 100 ms entre un état de veille de l'utilisateur et l'état actif autorisant l'établissement du plan usager.
La latence du plan usager correspond au délai de transmission d'un paquet IP au sein du réseau d'accès. Le LTE vise une latence du plan usager inférieure à 5 ms.

D'autres exigences et objectifs ont été fixés pour la technologie LTE tel que la mobilité, qui une fonction clé pour un réseau mobile. Le LTE vise à rester fonctionnel pour des UE se déplaçant à des vitesses très élevées. De plus, le LTE doit coexister avec les autres technologies.

Allocation spectrale en France

Le spectre est une ressource rare. Son organisation aussi bien France, qu'au niveau mondial est nécessaire à plusieurs tiers notamment nos fournisseurs d'accès internet (FAI). Cette organisation garantit notamment la compatibilité des systèmes entre pays, autorisant l'itinérance des utilisateurs à travers le monde.

Pour permettre le déploiement du très haut débit mobile de manière satisfaisante, l'Europe a choisi d'harmoniser les bandes attribuées au LTE entre les différents pays de l'Unions. Ce sont les bandes 800 MHz et 2.6GHz qui ont été identifiées. Cette approche a pour principal objectif la création d'un marché européen pour les équipements de réseau et les terminaux ainsi qu'une meilleure coordination aux frontières pour les opérateurs européens.

En France, l'ARCEP (Autorité de régulation des communications électroniques et des postes) est l'organisme en charge d'accompagner l'ouverture à la concurrence du secteur des télécommunications et de réguler les marchés correspondants. Il veille principalement à l'exercice d'une concurrence effective et loyale au bénéfice des consommateurs.

La bande 800 MHz, ou bande 20, est fortement prisée par les opérateurs mobiles car elle possède de bonnes propriétés de propagation. En d'autres termes, les ondes radio se propagent plus loin avec des fréquences basses et pénètrent mieux les bâtiments et la végétation qu'avec des fréquences hautes telles que la bande 2.6 GHz. Cependant, bien que cette bande permette aux opérateurs d'offrir une meilleure couverture (notamment à l'intérieur des bâtiments), cette bande présente des inconvénients : la largeur de bande, par exemple, très étroite limite les débits et la capacité des réseaux 4G.

La bande 2.6 GHz, ou bande 7, a été moins prisée car comme nous l'avons dit précédemment, elle possède de moins bonnes propriétés de propagation. Toutefois, la largeur de bande allouée dans cette bande est nettement plus importante que pour la bande 20, ce qui autorise des débits et des capacités plus élevés pour les réseaux. Elle est donc plus appropriée pour le déploiement en zone dense d'utilisateurs.

Architecture LTE

La technologie LTE présente une architecture générale simplifiée, notamment sur le réseau d'accès, où on s'affranchit des BSC et RNC des systèmes 2G et 3G.

La figure 5 permet de visualiser 3 domaines :

- Utilisateur, également désigné par UE (User Equipment)
- Réseau d'accès, aussi appelé E-UTRAN
- Réseau cœur, nommé EPC (Evolved Packet Core)

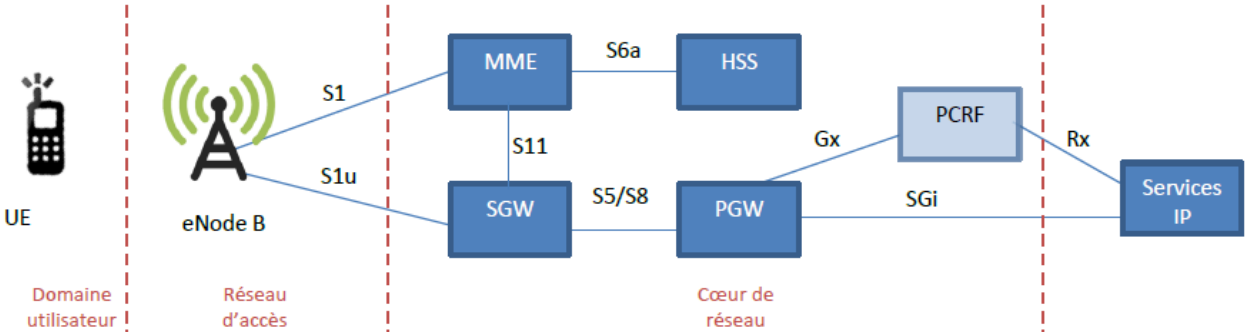


Figure 6 : Infrastructure type d'un réseau 4G

Le fonctionnement du LTE repose sur les différents éléments présents sur le schéma précédent.

SGW (Serving Gateway) : elle est traversée par tous les paquets IP à destination UE. Elle sert de point d'ancrage pour l'interfonctionnement avec les réseaux 2G ou 3G par exemple.

PGW (Packet Gateway) : Elle sert d'abord à allouer une adresse IP aux UE. C'est également une porte d'entrée unique entre le réseau IP de l'opérateur et Internet. Enfin, elle permet l'interconnexion avec des réseaux de type WiMAX.

MME (Mobility Management Entity) : c'est le nœud de contrôle qui gère la signalisation entre l'utilisateur et le cœur de réseau. Il a en charge la gestion de la connexion de signalisation et de la sécurité entre le réseau et l'UE.

HSS (Home Subscriber Server) : il contient les informations de souscription de l'utilisateur (QoS, restrictions d'accès), ainsi que les informations à propos des réseaux de données auxquels les utilisateurs peuvent se connecter. Il peut intégrer un élément qui permet l'authentification des abonnés, en dialoguant avec le MME.

PCRF (Policy and Charging Rule Function) : c'est un nœud optionnel de l'architecture d'un EPC, avec lequel je n'ai pas travaillé. Il permet d'appliquer des règles de gestion sur le trafic et la facturation d'un utilisateur en fonction de son offre.

B. Mon architecture

1. Description

A mon arrivée dans le service, j'ai assisté Alicia, une autre stagiaire dans son dernier mois de stage. Je l'ai accompagné sur la fin de ses missions et je me suis approprié l'ensemble des systèmes sur lesquels j'allais travailler durant mon stage car j'allais devoir poursuivre ses travaux. Avec l'aide d'Alicia, j'ai pu très rapidement prendre en main les principaux outils des différents systèmes.

La mission principale qui m'a été assigné après le départ d'Alicia était la continuation de l'architecture réseau 4G dédié destiné à des démonstrations ainsi que des preuves de concept « PoC » pour les différents projets du service. En d'autres termes, sur cette plateforme je devais intégrer des éléments, des services afin de montrer aux clients leurs fonctionnement sur du réseau 4G. Nous verrons par la suite ces différents éléments plus en détails. Par analogie, nous pourrions prendre des blocs de Lego et les assembler ensemble afin de construire une structure stable.

La plateforme, communément appelé « ShowRoom » dans le service, était déjà opérationnel au niveau de la 4G, c'est-à-dire que l'ensemble des équipements tel que le MME, le HSS vue précédemment étaient fonctionnels. Un autre réseau d'accès tel que la WiFi, via un access point était aussi mis en place ainsi que des services multimédias mobile comme un service de VoIP, le service Nexium Wireless TT développé par le service et une application pour la diffusion de vidéo en temps réel. Les différents éléments réseaux tel que le switch et routeur étaient aussi configurés pour le fonctionnement des services cités précédemment.

Ma mission consistait donc à améliorer ce système existant aussi bien dans l'ajout des services et type de réseau d'accès que sur la configuration et la mise en place des équipements réseau. Mon responsable avait déjà en tête l'intégration de plusieurs éléments comme la mise en place d'un VPN sur un serveur Linux et d'une application de contrôle, le Dispatcher, développé par une entreprise partenaire du projet. On pourrait donc voir la plateforme réseau du ShowRoom comme une architecture multi services et multi bandes comme représenté sur la figure ci-dessous :

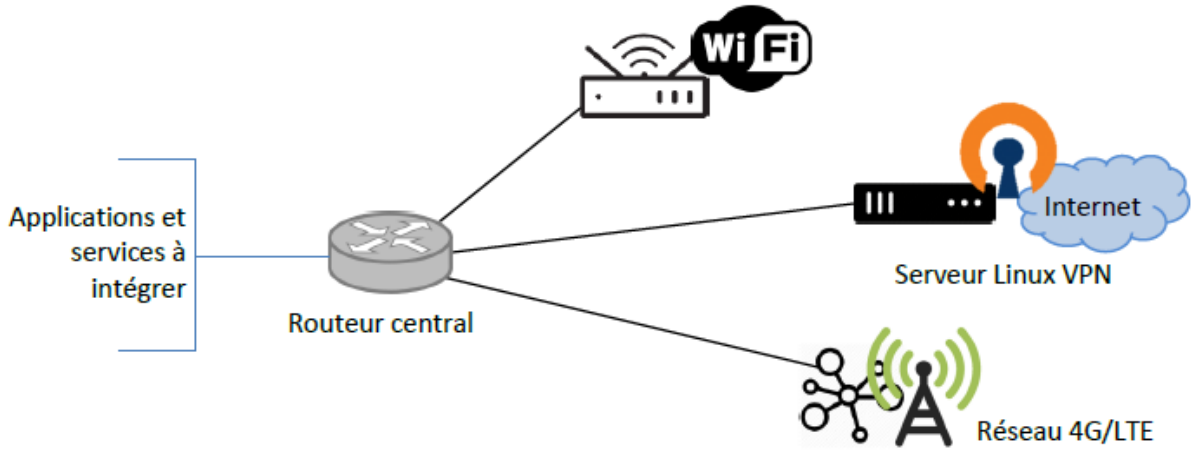


Figure 7 : Multi band architecture

2. Nexium Wireless & Dispatcher

L'application mobile Nexium Wireless et l'application Web Dispatcher représentent le futur des applications de la PMR utilisé au quotidien par le ministère de l'intérieur, la gendarmerie nationale, les pompiers etc…

Les utilisateurs professionnels de la radio mobile ont maintenant besoin de capacités multimédias plus performantes et à bande passante élevé pour partager des informations sur le terrain comme par exemple la recherche en bases de données, la vidéo en temps réel, la prise de conscience de la situation, le transfert d'images ainsi que la géolocalisation pour suivre l'évolution du déploiement des troupes. L'ensemble de ces besoins sont regroupés dans ces deux applications.

Sur la plateforme du Showroom, les services nécessaires pour le fonctionnement de l'application Nexium Wireless étaient déjà présents et configurés dans un serveur. Mon objectif était donc d'ajouter les services du Dispatcher à ceux déjà présent sur le serveur. Cependant, bien que déjà grandement utilisé par une autre entité du service sur le projet du ministère de l'intérieur, les versions d'applications sur mon serveur étaient différentes des leurs. En effet, deux versions étaient présentes dans le service : une version 3.0, que j'utilisais, qui avait en plus de la voix les fonctionnalités de diffusion vidéo et le transfert d'image. Et une version 2.0 qui possédait seulement la fonctionnalité de voix nettement amélioré par rapport à la 3.0 avec une meilleure gestion des paquets, du Push-to-Talk etc…
Ces écarts de version m'ont créé de nombreux problèmes d'incompatibilités. Par conséquent, j'ai dû travailler en collaboration avec un développeur de l'entreprise partenaire afin de pouvoir intégrer au mieux la version 3.0 du Dispatcher sur mon architecture. Etant le premier à intégrer la version 3.0 du Dispatcher, j'ai créé un document d'installation pour laisser une trace des différents problèmes rencontrés pour des futures installations.

Une fois l'ensemble des problèmes corrigés et le Dispatcher fonctionnel sur mon infrastructure, j'ai commencé par m'approprier les différentes fonctionnalités afin de pouvoir les présenter en démonstration par la suite. Cependant, suite à de nombreuses discussions entre les responsables de projet et un changement interne, il a été décidé d'arrêter le développement de la version 3.0 et de remettre l'ensemble des fonctionnalités de vidéo, d'images sur la version 2.0. J'ai donc dû enlever l'ensemble des services de l'outil Dispatcher et de l'application Nexium Wireless de mon serveur afin de mettre ceux de la version 2.0. J'ai dû ensuite faire toutes les configurations nécessaires réseaux. Cette étape ne m'a finalement pas posé de problème car j'avais déjà eu l'occasion de regarder en détail les fichiers de configurations, leurs structures et les protocoles de communications de la version 3.0. A noter, que dans cette nouvelle version, l'ensemble des services utilisé pour l'application Nexium Wireless et ceux du Dispatcher sont sur une seule machine virtuelle dans le serveur. Nous parlerons de la virtualisation dans une prochaine partie.

3. Cellule Pico NSN

Lorsque j'ai commencé à travailler sur la plateforme, l'eNodeB connecté était une cellule Macro. Il existe plusieurs sortes de cellule : les cellules macro, micro, pico et femto. Les eNodeB Macro sont des cellules larges dont le rayon est compris entre quelques centaines de mètres et plusieurs kilomètres. La puissance émise par la cellule est environ de 40W. De nombreux atténuateurs étaient mis en série au niveau des antennes afin de nous protéger du rayonnement. Cependant, au vu des distances d'émission, et au vu de l'utilisation que nous faisons dans le ShowRoom, la taille de la cellule n'était pas adaptée. De plus, même si des

atténuateurs ont été installés, la puissance d'émission restait toutefois très élevée pour des distances inférieures à 5 mètres.

Après avoir discuté de mon problème avec Christophe, un ingénieur IVVQ, j'ai appris qu'il restait une cellule Pico en stock. Les cellules pico poursuivent les mêmes buts que les cellules macro, mais sont associées à des puissances bien plus faibles, de l'ordre de 0.25 W à 5 W. Elles sont destinées à couvrir des grandes zones intérieures (indoor). Je suis allé voir le responsable de l'équipement en question pour lui proposer d'échanger ma cellule Macro contre la Pico. Il s'est avéré qu'il recherchait justement une cellule Macro. J'ai donc pu installer la cellule Pico sur ma plateforme.

Les avantages de la cellule Pico pour ma plateforme ne se restreignent pas seulement à sa faible puissance d'émission. En effet, les cellules Pico, de par leur nom, sont nettement plus petites que les eNodeB Macro. Elles sont facilement transportables à la main. J'ai donc gagné en place et en volume dans mon infrastructure. La question sur la mobilité et sur le volume peut se révéler d'être de bons arguments pour les démonstrations auprès des clients. De plus, de par leur faible puissance d'émission, elles chauffent moins et par conséquent ne demandent que très peu de moyen de refroidissement. Sa structure striée permet à elle seule d'évacuer la chaleur. Le dernier avantage est sa simplicité avec un seul port Ethernet Gigabit pour l'accès au réseau et sa configuration.

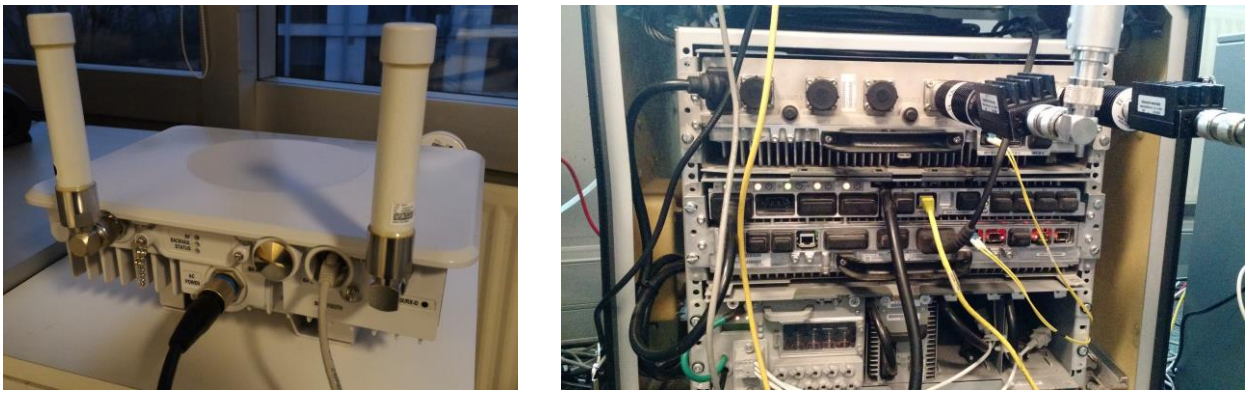


Figure 8 : Photo d'une cellule Pico et d'une cellule Macro

La configuration des eNodeB que le service possède se réalise par l'intermédiaire d'un logiciel : BTS Manager. Les eNodeB, et notamment la cellule Pico de ma plateforme, ont une adresse IP par défaut pour accéder à l'interface de configuration. Une fois connectée avec le logiciel, on peut observer de nombreux paramètres tels que l'état des différents composants de la cellule ou les différentes erreurs qui vont à l'encontre du bon fonctionnement de l'eNodeB par exemple. C'est justement les logs des erreurs rencontrées comme la *non synchronisation GPS* ou la *liaison S1 qui n'arrive pas à se faire* qui vont nous indiquer la localisation du problème. Plusieurs états d'erreur existent mais seulement l'état « Major » et « Critical » sont bloquants dans le fonctionnement de la cellule. Pour le détail de la configuration de la cellule, nous pouvons modifier vraiment tout, ce qui m'a demandé quelques jours d'étude des paramètres afin de pouvoir la configurer correctement selon nos besoins. Par exemple, le PLMN (Public Land Mobile Network) est un paramètre qui joue un rôle important. Le PLMN est un numéro unique pour chaque réseau mobile, dans mon cas, il s'agit du 310-14. Il est renseigné à plusieurs endroits (EPC, HSS, eNodeB), et il a donc fallu que je m'assure que c'était bien le même partout. C'est grâce à ce paramètre que les utilisateurs autorisés peuvent accéder à différents services. D'autres paramètres comme la puissance d'émission, la fréquence, la bande passante peuvent être modifiées.

4. Interconnexion

L'interconnexion entre plusieurs réseaux 4G est un enjeu crucial pour le fonctionnement de nos différents services et projets. En effet, il faut qu'un utilisateur puisse passer d'un réseau opérateur à un réseau privé sans aucune coupure et sans action de sa part.

Etant donné que je travaille sur des preuves de concept, mon responsable de stage m'a demandé de regarder un peu plus en détail la mise en place de l'interconnexion avec notre réseau privé et le réseau 4G de SFR. En effet, SFR, une des entreprises partenaires du projet sur lequel je travaille, nous a mis à disposition un réseau dédié sur leur infrastructure à l'aide de carte SIM et d'un APN spécifique. Dans un premier temps, ma mission était de mettre en place un serveur avec les mêmes services qu'au ShowRoom sur l'infrastructure dédiée de SFR. J'ai donc dû analyser les équipements réseaux avec leurs configurations pour pouvoir faire au mieux les modifications réseaux sur les services Nexium Wireless et Dispatcher.

Une fois les services mis en place, l'objectif était de réaliser une liste exhaustive de tests comme par exemple des tests de robustesse en utilisant l'application AutoMagic, des tests sur la perte et la récupération du réseau et observer le comportement de l'application Nexium Wireless. AutoMagic est une application permettant l'automatisation de commande à exécuter (appui sur le bouton d'appel, envoie d'une image, raccrocher dans le cas de notre application Nexium Wireless etc…). J'ai aussi profité de ces tests pour imaginer la veste du « policier du futur » en ajoutant un micro/haut-parleur Push-To-Talk Bluetooth relié au Smartphone et à l'application Nexium Wireless, ainsi qu'une caméra HD positionné au niveau du torse relié au Smartphone pour diffuser le flux vidéo sur le réseau 4G. Pour pousser toujours plus loin la question sur la mobilité, j'ai proposé l'idée de rendre mobile le poste de commandement en utilisant l'application Dispatcher sur une tablette connecté sur le réseau 4G via un dongle LTE.

Après que l'ensemble des tests soient terminés et vérifiés par un ingénieur IVVQ, j'ai appris que le serveur sur la plateforme SFR allait être utilisé pour une démonstration. Je ne devais donc plus faire d'essais et de modifications dessus. Je pouvais néanmoins garder deux cartes SIM du réseau dédié de SFR pour continuer à faire des tests. Mais n'ayant plus de serveur à disposition je devais trouver une solution pour relier le réseau SFR sur le réseau du ShowRoom. C'est à ce moment-là que la problématique de l'interconnexion s'est posée. En posant à plat le problème, en définissant les différents éléments sur un tableau et en essayant de comprendre les différentes règles de routage et configurations réseaux qu'il fallait mettre en place. Ne pouvant pas toucher à l'infrastructure mis en place par SFR, je devais adapter l'adresse IP des services du ShowRoom pour pouvoir atteindre le serveur avec les terminaux SFR. Finalement, j'ai réussi à interconnecter le réseau dédié de SFR et celui du ShowRoom. Je pouvais donc à ce moment communiquer, via l'application Nexium Wireless, entre les deux réseaux. En utilisant un terminal double Sim, je pouvais tester le changement de réseau en passant de l'un à l'autre et observer le comportement de l'application. La figure ci-contre montre l'accès aux services par les deux réseaux :

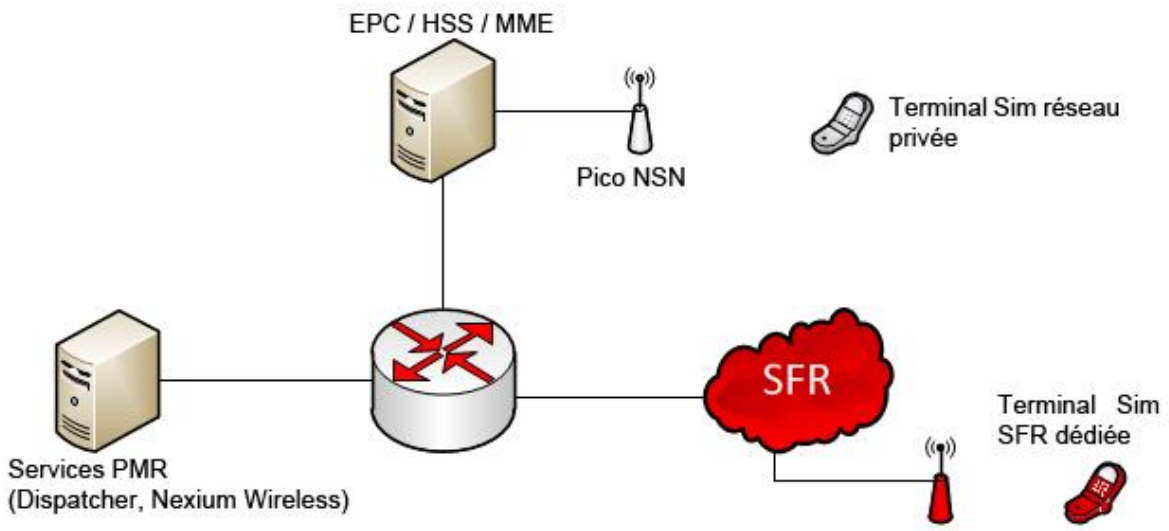


Figure 9 : Schéma de l'interconnexion entre le réseau SFR et celui du Showroom

5. ThalesEye

Mon tuteur a mis en place une collaboration avec une autre entité du groupe (Thales Service), afin que je puisse travailler sur l'intégration d'une application du nom de : ThalesEye, pour une preuve de concept (PoC) lors d'une démonstration des services dans une centrale nucléaire. Nous parlerons de cette expérimentation dans une prochaine partie.

ThalesEye est un démonstrateur d'une solution de téléassistance collaborative dans le domaine de la maintenance industrielle. L'application permet à un expert distant de guider un opérateur sur site grâce à des outils de réalité augmentée.

Le système de collaboration mis en place permet à un utilisateur actif muni d'un appareil mobile (équipé d'une caméra) tel que des lunettes de réalité augmenté ou bien même un simple Smartphone, d'interagir avec un autre utilisateur à distance. L'utilisateur actif transmet à l'utilisateur à distance des informations sur son environnement. Le système permet alors à l'utilisateur à distance de guider l'utilisateur actif en incluant un ou plusieurs outils de collaboration localisés dans l'espace. L'utilisateur actif peut alors visualiser les indications de son collaborateur sur son appareil mobile en superposition de l'espace observé.

Dans le cadre de cette intégration, j'ai eu pour premier objectif d'analyser, de comprendre et de faire fonctionner le système dans un environnement local, c'est-à-dire via un point d'accès WiFi. Le serveur hébergeant l'application ainsi que les deux terminaux étaient donc dans le même réseau local. Il n'y avait donc à ce stade pas vraiment de difficulté pour la configuration réseau afin que la communication entre le terminal et son serveur soit possible. Ne pouvant pas aller réaliser personnellement la preuve de concept à la centrale, j'ai dû faire un passage de connaissance rapide à une collègue afin qu'il soit capable de réaliser le montage.

Le deuxième objectif, et finalement, le réel challenge que m'a proposé mon responsable, était de faire fonctionner l'application sur notre architecture 4G\LTE, comme illustré sur la figure suivante :

Figure 10 : Architecture ThalesEye intégrée à l'architecture 4G/LTE de la plateforme multi-accès

Dans un premier temps, il a fallu que je déploie la machine virtuelle du serveur de l'application sur un hôte physique, et que je fasse les configurations réseaux sur l'hôte et la machine virtuelle. J'ai dû ensuite m'adapter sur mon architecture par rapport à l'adresse IP imposée par l'application mobile Thales Eye. En effet, cette dernière introduit en dur dans le code source l'adresse IP du serveur sur lequel elle doit se connecter. N'ayant pas les droits et surtout la clef de signature, je ne pouvais pas utiliser l'outil de décompilation et recompilation d'application afin de modifier cette adresse IP. Cet outil sera détaillé dans la partie sécurité du rapport.

Une fois fait, j'ai commencé par analyser le comportement de la transmission du flux vidéo qui n'a montré aucun problème ni en termes de latence, ni en termes de qualité de service. Ainsi que le comportement des objets de réalité augmenté.

6. QualIT

Le passage de la voix de l'application Nexium Wireless se fait au travers du protocole UDP. Il était intéressant de tester la qualité du lien 4G à vide pour simuler une charge faible sur le réseau, en d'autres termes avec seulement une communication voix, et de tester ce lien en charge élevé, c'est-à-dire lorsque tous les services multimédias tel que la diffusion de flux vidéo ainsi que l'application Thales Eye sont en fonctionnement.

La qualité de service (QoS : Quality of Service) est un point clé dans le développement de la téléphonie et des services temps réel sur Internet. La QoS est étroitement liée à la gestion de trafic réseau et désigne un ensemble de paramètres permettant d'assurer la qualité d'un service réseau.

Les principaux indicateurs de niveau de performance du réseau VoIP pour en déterminer l'intégrité sont décrits ci-dessous :

Latence/Delai : L'un des paramètres essentiel utilisé pour mesurer la qualité vocale et vidéo d'un réseau IP est le délai ou la latence. Le délai mesuré est le temps requis pour que la voix d'un interlocuteur du site source atteigne l'autre interlocuteur au site de destination. Le temps de réponse du réseau contribue à retarder la transmission de la voix, ce qui se traduit par des saccades et des interruptions au cours de la conversation.

Instabilité/Jitter(Gigue) : Il s'agit d'un paramètre clé permettant de mesurer la qualité vocale et vidéo sur un réseau IP. L'instabilité ou gigue indique une variation du délai entre les paquets reçus (écart de délai entre paquets). Les utilisateurs observent régulièrement des saccades dans le discours de leur interlocuteur, et même parfois des sons désagréables pendant la conversation, avec perte de synchronisation par exemple. Pour une bonne qualité de la communication, la gigue doit être constante et rester inférieure à 100 ms.

Perte de paquet : La perte de paquet est une mesure des données perdues pendant la transmission d'une ressource vers un autre réseau. Des paquets sont régulièrement rejetés en raison du temps de réponse du réseau (TTL). Il est donc important de surveiller la perte de paquets et d'entreprendre des actions correctives en fonction des informations des indicateurs de QoS.

L'objectif est donc de satisfaire le client au mieux avec les ressources réseau dont on dispose. Il faut alors privilégier certains services ou certaines actions au détriment d'autres selon une politique bien réfléchie à l'avance. On peut améliorer la qualité de service en mettant en place une classe de service qui a pour objectif de différencier les différents types de paquets (voix, vidéo, mail, web) et de créer une priorité de traitement pour les paquets ayant un niveau de qualité élevé et une réservation de la bande passante en conséquence.

Figure 11 : Schéma type du fonctionnement de QualIT sur le réseau

Pour effectuer ces tests, j'ai utilisé le logiciel QualIT. Ce produit, développé par la société J3TEL, permet également de mesurer divers paramètres réseaux et présente l'avantage d'offrir une interface graphique, permettant de visualiser des courbes de débits ou latences par exemple. L'objectif était donc de découvrir et prendre en main Qual'IT, afin de mener les tests que nous voulions.

Qual'IT fonctionne avec un serveur maître, pilotant des sondes (Agents Qual'IT) placées aux extrémités du lien à tester, comme on peut le voir dans la figure précédente. Des résultats de test de qualité de service entre une Box QualIT et un Smartphone sur le réseau dédié ainsi que sur le réseau SFR se trouvent en annexe 2.

7. Vlans & protocole OSPF

L'infrastructure du ShowRoom commençait à être bien remplie avec tous les services ajoutés comme Thales Eye, l'interconnexion avec la plateforme SFR, le serveur QualIT et sa box ainsi que d'autres services que nous verrons dans les prochaines parties tel que le serveur VPN et le serveur du gestionnaire de terminaux. A chaque nouvel ajout, c'était un câble Ethernet en plus sur le routeur ou sur le switch mais aucune stratégie d'ordonnancement particulier n'avait été établi au départ de la construction de l'infrastructure. Cela devenait donc compliqué de s'y retrouver. Lors d'une coupure de courant du bâtiment, j'ai décidé de reprendre à zéro l'agencement des équipements. Vous pouvez voir en annexe 3 le nouvel agencement de mon architecture.

Pour la configuration de tous les équipements, une Workstation est déployée. Par souci de simplicité, la stagiaire qui m'a précédé avait ajouté pour chaque sous réseau de l'infrastructure une adresse IP à la Workstation. Nous avions donc une dizaine d'adresse IP sur

la même machine. Ceci n'était pas propre et un nombre égal de routes statiques avait été créé sur le routeur afin de pouvoir atteindre les équipements. J'ai donc décidé de séparer en deux parties l'infrastructure : une partie pour les données et une autre réservée au management des équipements. Par analogie, j'ai donc créé sur le switch et le routeur deux Vlans distinct. Pour le Vlan Management, j'ai privilégié l'adressage IP du sous réseau 192.168.1.0. Pour les serveurs, j'ai utilisé une sortie physique dédié au management relié au switch. Pour les équipements n'ayant qu'une seule sortie physique comme l'eNodeB Pico, j'ai mis en place le tag de paquet pour différencier les Vlans de chaque paquet envoyé.

Le routage statique est adapté pour de petites infrastructures mais peut s'avérer être compliqué à maintenir lors d'une mise à l'échelle. J'ai justement rencontré le problème de ne plus savoir à quoi correspondaient certaines routes mises en place. Des équipements avait été enlevé, changé de place, changé de sous réseau mais les routes n'avaient pas été modifiées. Je me suis rapidement rendu compte que le routage statique était très pratique pour mettre en place des équipements rapidement et connaitre à 100% la topologie du réseau et le chemin de chaque paquet. Par contre, sans archivage régulier le routage statique peut devenir un problème. C'est de par ces difficultés que j'ai décidé de passer en routage dynamique en utilisant le protocole OSPF.

Le protocole OSPF est basé sur l'algorithme de routage à état de lien qui a été conçu en 1987. Pour permettre à chaque routeur de connaitre son voisinage et de le disséminer à tous les autres routeurs, OSPF se charge de maintenir une base donnée propre à chaque routeur. Cette base de données nommé LSDB (Link State DataBase) contient la cartographie du réseau, c'est-à-dire l'ensemble des routeurs composant le réseau et des liens entre ces routeurs. Cette base se construit à la réception des paquets de contrôle et est utilisée une fois constitué pour calculer localement les routes à l'aide de l'algorithme de Dijkstra. Pour cela, OSPF envoie régulièrement des paquets Hello à tous ces voisins. Le paquet Hello est envoyé en multicast sur une adresse IP spécifique connue par tous les routeurs utilisant le protocole OSPF. Il contient notamment les paramètres de configuration ainsi que la liste de ces autres voisins. La raison d'envoyer la liste de ces voisins, permet à un routeur de confirmer ses messages Hello antérieurs, cela augmente donc la fiabilité du processus d'identification des voisins. Ce paquet Hello contient aussi le type de réseau qui sépare les deux routeurs. Ce type de réseau permet au routeur d'associer une métrique à chaque relation de voisinage. Plus le réseau reliant deux routeurs est rapide, plus la valeur de la métrique sera petite, donc plus ce lien sera favorisé dans le processus de sélection des routes.

Pour le passage à l'échelle, et s'assurer que le protocole soit efficace aussi bien dans les petits réseaux que dans les grands, OSPF permet de diviser le réseau en d'autres plus petits réseaux appelés aire. Il peut avoir une correspondance entre les aires et les sous réseaux IP mais ce n'est pas forcément nécessaire. Finalement, ce protocole est distribué, dynamique et permet de s'adapter facilement au changement de topologie.

Pour faire l'analogie avec mon réseau, la figure ci-dessous décrit la division de mon architecture en aire. On retrouve donc sur le schéma le routeur central de mon infrastructure ainsi que le routeur utilisé pour l'accès aux services depuis le réseau SFR. Pour les relier entre eux avec une zone, il faut que les deux routeurs possèdent une interface physique dans le même sous réseau. Au final, ma topologie étant assez réduite, il est pertinent de se demander si l'utilisation du protocole OSPF est vraiment nécessaire. Dans la mesure où l'infrastructure actuellement déployée est amenée à grossir et changer dans un futur proche ou lointain avec l'ajout de nouveaux services multimédias ou d'un nouveau routeur pour accueillir une nouvelle station de base, j'ai pris le pari dès maintenant de déployer un protocole dynamique pour faciliter ce changement de topologie.

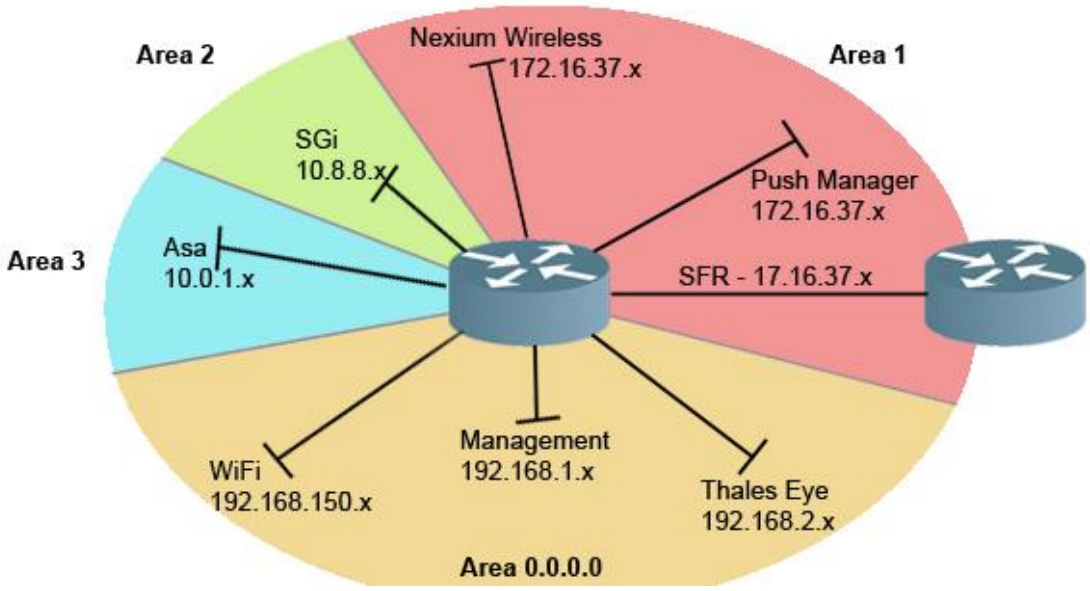


Figure 12 : Définition des zones pour le protocole OSPF

8. Autres

Au cours de mon stage, mon responsable m'a donné l'occasion de travailler sur un drone. Le drone en question était un Dji Phantom 3 avec une camera 4K. L'objectif était de mettre à la place de la caméra initiale, une autre caméra reliée à un terminal par lequel nous diffuserions la vidéo sur le réseau 4G. Nous pourrions ainsi récupérer par le drone des informations crucial pour un contexte par exemple de force de police sur une situation à risque. C'était aussi pour le service l'occasion de pouvoir montrer pendant une preuve de concept chez un client les différentes possibilités que nous permet la technologie 4G. J'ai donc pour cela, démonté le support de camera 4K, et accroché de la façon la plus propre possible l'autre caméra et le terminal sur le drone. Des supports et stabilisateurs sans caméra sont disponibles pour le modèle du drone. Malheureusement, n'ayant eu que très peu de temps avant la démonstration, je n'ai pas pu tester ces supports. Néanmoins, lors de la preuve de concept, le drone a fait parler de lui.

Dans le même contexte, mon responsable m'a fourni une application utilisant l'oculus rift. Le but de l'application est de pouvoir contrôler une caméra 360° à distance avec l'oculus rift. Les mouvements de la tête font bouger la caméra. Cela permet de réaliser une surveillance à distance, ou dans des endroits à fort risque comme dans certains endroits d'une centrale nucléaire. L'objectif était de déporter le fonctionnement local en WiFi de l'application sur un réseau 4G. Je n'ai pas pu implémenter au final l'application à cause de la puissance requise nécessaires sur un PC pour faire tourner de la réalité virtuel. Malheureusement, je n'ai reçu que trop tard une carte graphique de nouvelle génération, c'est-à-dire « *VR Ready* », pour implémenter l'application sur notre réseau 4G.

III. Sécurité

A. Reverse Engineering Apk android

Avant d'aller plus loin, introduisons brièvement le terme de Reverse Engineering, ou de rétro conception.

Le reverse engineering est un processus où tout type d'équipement, d'objet ou de système comme une voiture, un logiciel par exemple sont déstructurés dans un but de retrouver les détails originaux, comme le design, l'architecture ou bien dans notre cas le code source.

Dans le domaine informatique, le reverse engineering est majoritairement utilisé pour :

- Trouver des vulnérabilités
- Découvrir des informations secrètes
- Analyser le fonctionnement des protocoles
- Des recherches académiques
- La création de patchs et mises à jour

L'application Nexium Wireless offre la possibilité de changer différents paramètres tel que l'adresse IP du serveur du TCU, l'URI de l'utilisateur ou bien même la gigue. Ces paramètres ont une valeur par défaut lors de l'installation de l'application sur notre terminal et certains doivent être changés par l'utilisateur pour que l'application puisse se connecter au serveur. Nous parlons bien entendu des deux premiers paramètres que nous avons cités plus haut : l'adresse IP du serveur et l'URI. Dans le cadre de la recherche et de l'intégration dans notre infrastructure, le changement de ces paramètres ne pose pas de problème. Cependant, ces services sont à destination de professionnel tel que des gendarmes, des pompiers etc… Ce n'est donc pas à eux directement de les changer. Il est donc pertinent de poser la problématique suivante : comment modifier les paramètres de l'application par défaut selon les identifiants de chaque utilisateur ?

Pour répondre à cette problématique, nous devons dans un premier temps nous demander par quel moyen nous allons réussir à décompiler l'application Nexium Wireless afin de modifier directement les paramètres de l'utilisateur. C'est ainsi que nous allons utiliser le principe de reverse engineering grâce à un outil spécialisé dans la décompilation d'application Android : Apktool. C'est avec ce programme que nous allons restituer l'application dans sa forme originale de dossier avec l'ensemble de ses composants lisible.

L'outil permet également de résoudre l'opération inverse, c'est-à-dire la recompilation du code depuis les composants qui constituent l'application. Apktool est principalement utilisé pour modifier les applications existantes sans avoir le code source : on désassemble l'application, on modifie et on réassemble ces derniers. Nous obtenons donc une application au format .apk modifiée selon nos envies.

La mission consistait donc à écrire un script prenant en paramètre le fichier .apk de l'application Nexium Wireless et de faire toutes les modifications nécessaires dans les paramètres de préférences avant de recompiler le tout. J'ai commencé dans un premier temps par réaliser le script en Bash. Ayant déjà une bonne expérience avec ce langage et un accès à un pc sous Linux, je n'ai pas rencontré de difficulté pour le développement du script. Néanmoins, l'utilisation de l'outil Apktool m'a demandé de faire quelques recherches supplémentaires afin de bien comprendre son fonctionnement. Cependant, lors d'une journée réunissant les

partenaires du projet sur lequel je travaillais, j'ai eu l'occasion de discuter avec un responsable d'Ibelem. Cette entreprise est un intégrateur de solution MDM (Mobile Device Management), c'est-à-dire un gestionnaire de terminaux, en proposant donc à différentes sociétés des produits en cohésion avec leurs besoins. Ibelem développe aussi son propre MDM, appelé le Push Manager. Mon responsable de stage avait donc l'intention d'intégrer ce logiciel dans notre environnement 4G. Nous verrons plus en détails ce dernier dans la dernière partie de ce rapport.

Lors de cette discussion, le responsable d'Ibelem m'a donné une première version du Push Manager en machine virtuelle. De plus, il s'est avéré que ce gestionnaire de flotte ne pouvait pousser sur les terminaux seulement des applications et non des fichiers de configurations. En effet, par analogie avec notre infrastructure, nous voulions pousser l'application Nexium Wireless sur un terminal avec les paramètres de préférences associé à cet utilisateur. Je lui ai donc parlé de mes travaux sur la décompilation d'application via l'outil Apktool. Ils ont été très intéressés. Le seul problème c'est que le logiciel fonctionne sur un Windows server. Par conséquent, le script en Bash ne pouvait pas s'exécuter dessus. Je devais donc leur fournir une nouvelle version du script dans un langage multiOS. Le langage choisi est le Python. De ce retour et ne connaissant pas ce langage, j'ai pris quelques jours pour en apprendre les bases. J'ai ensuite refais le script en Python, que vous pouvez trouver en annexe 4, et donné cette nouvelle version à Ibelem afin qu'il puisse l'intégrer sur l'environnement du PushManager.

B. Mise en place d'un VPN

Le VPN est une solution, de plus en plus répandue, de connexion réseau sécurisée avec un site distant. D'abord utilisé de manière professionnelle, son utilisation a aussi conquis le grand public.

Le VPN est donc une connexion réseau entre un client à une extrémité et le serveur VPN à l'autre extrémité. Cette connexion réseau est virtuelle et s'appuie sur une liaison physique sécurisée, c'est-à-dire chiffré et avec authentification. En d'autres termes, le VPN est l'équivalent d'un câble réseau connecté d'un bout au client, et de l'autre bout au serveur. Cela correspond à la vision pratique de l'utilisateur, qui peut alors communiquer avec les équipements réseaux, ou bien accéder aux services multimédias comme si il était physiquement relié au réseau distant. L'architecture réseau qui sépare le client du serveur est totalement transparente. Le VPN se matérialise alors par une connexion réseau supplémentaire qui apparait dans la liste des connexions réseaux, au même titre que les connexions physiques. Du coté serveur, une connexion identique est aussi visible. Cela correspond aux deux bouts de la connexion virtuelle.

Cette connexion doit répondre à des exigences de sécurité et d'intégrité des données. Pour cela, il faut définir un chiffrement et une authentification qui garantissent un niveau de sécurité suffisant, tout en évitant de trop ralentir la connexion. Les protocoles de sécurité utilisés sont les suivant :

- PPTP (Point-to-point Tunnelling Protocol)
- L2TP (Layer 2 Tunnelling Protocol)
- IPSec (IP Security)
- SSL/TLS (Secure Sockets Layer/Transport Layer Security)

Certains protocoles sont plus populaires que d'autres, et la liste comprend les

principales technologies qui sont en cours d'utilisation. De nos jours, les protocoles IPSec et SSL sont majoritairement utilisés. Nous allons voir notamment plus en détails ces deux derniers car ce sont deux protocoles utilisés dans les solutions VPN que j'ai mises en place dans mon architecture : OpenVPN et Cisco Asa.

1. IPSec

Même si IPSec est souvent utilisé en pair avec L2TP en mode Transport, c'est-à-dire qu'il transporte seulement les données de manière sécurisé, il peut être utilisé comme un protocole de tunneling indépendant, c'est-à-dire d'encapsulation d'IP qui lui permet entre autres de créer des réseaux privés virtuels. IPSec est un protocole de la couche 3 du modèle OSI et réalise un transfert de données sécurisés en utilisant des clés cryptographiques au début de la session de tunneling et en chiffrant les données par la suite avec ces clés.

Comparer à SSL, il a l'avantage d'être transparent pour l'utilisateur. Il garantit aussi un haut niveau de sécurité et une maintenance facile. Cependant IPSec est souvent compliqué à mettre en place par manque de compatibilité, demande une puissance élevée de traitement et utilise une multitude de sous protocoles comme AH (Authentifiation heards), ESP (Encapsulating Security Payloads) et ISAKMP (Internet Security Association and key manager).

2. SSL

A l'origine, SSL a été créé pour sécuriser les transactions commerciales sur internet via un navigateur web en remplaçant http par https, avec « s » pour *secure*. Il supporte aujourd'hui d'autres applications somme les protocoles smtp ou ldap. SSl est une technologie basée sur PKI (Public Key Infrastructure) par l'utilisation de certificats X509 serveur et client. Il supporte également le mode « tunnel ».

Le VPN SSL est une solution qui pallie aux difficultés rencontrées avec IPsec et les accès distant, notamment dues à la translation d'adresses et au filtrage d'applications dans le réseau distant. Le terme de VPN *clientless* est souvent utilisé pour désigner les VPN SSL car il n'y a pas besoin de logiciel spécifique sur le client pour atteindre le réseau de l'entreprise.

L'objectif de mettre un VPN dans mon infrastructure était de permettre l'accès aux (futures) applications, depuis un réseau opérateur public (Orange, Bouygues, etc…), tout en sécurisant cet accès. Pour pouvoir déployer un VPN, la DSI Thales a mis à notre disposition une adresse IP publique qui nous permet de déboucher sur Internet. Cet accès est bien évidemment filtré par la DSI, via un firewall et du NAT. J'ai utilisé deux technologies différentes au cours de mon stage pour réaliser l'accès VPN.

C. OpenVPN

OpenVPN désigne en fait un protocole, un serveur et un client. Il propose donc une solution complète de VPN mais nécessite l'installation d'un logiciel. OpenVPN est un logiciel OpenSource, on le retrouve donc principalement dans les clients Android et Linux. Le protocole utilisé par défaut est le protocole SSL et donc par conséquent le port utilisé est le port TCP 443. Ce port étant essentiel pour pouvoir naviguer sur le web, était déjà préalablement ouvert lors du raccordement de notre plateforme sur Internet par la DSI. Je n'ai donc pas eu de problème pour la mise en fonctionnement d'OpenVPN contrairement à l'Asa.

L'architecture mis en place est illustrée sur figure ci-dessous. Le serveur VPN est en réalité un ordinateur sous Linux (Ubuntu) possédant deux ports Ethernet, ce qui permet de le raccorder à deux réseaux différents. J'ai donc installé et configuré le logiciel OpenVPN sur un ordinateur Linux.

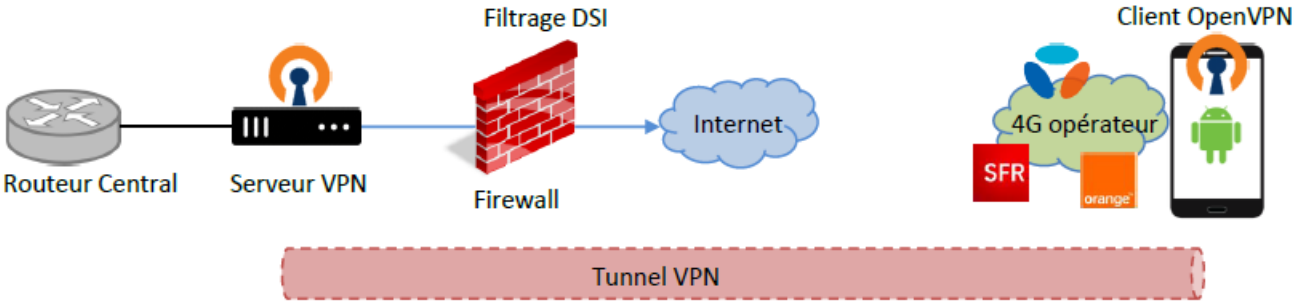


Figure 13 : Architecture VPN

La configuration se fait en trois étapes :

- La génération du certificat d'autorité, des clés, et des certificats clients et serveur
- Le paramétrage du fichier *serveur.conf*, pour indiquer le protocole, le port, le pool d'adresse IP
- Le paramétrage du fichier *client.ovpn*, miroir du *serveur.conf* mais pour les clients

J'ai ensuite installé l'application OpenVPN sur le terminal Android connecté à un réseau 4G public, et transféré le fichier *client.ovpn* sur le Smartphone afin qu'il soit utilisé par l'application pour se connecter au serveur VPN.

D. Cisco Asa 5505

Plusieurs raisons ont mené à faire le changement d'équipement pour réaliser cette liaison sécurisée VPN. La raison principal est le souhait d'harmoniser les technologies utilisées dans le service. En effet, un VPN utilisant la technologie ASA était utilisé pour la plateforme SFR afin qu'ils puissent accéder aux services PMR que nous leur mettions en place en interne. De plus, la plateforme du ShowRoom était destinée à des démonstrations et par conséquent présenté devant des clients. La solution Cisco Asa est reconnue dans le monde de l'entreprise et parlant pour les clients contrairement à la solution opensource OpenVpn. D'autre part, l'Asa met à disposition une interface graphique native permettant une configuration basique simple et rapide. Mais nous pouvons aussi utiliser le mode console via le port série. Etant donné que cet équipement est fourni par Cisco, nous retrouvons exactement les mêmes commandes que pour les équipements réseaux tel que les routeurs et les switches.

Le VPN Asa utilise les protocoles d'IPSEC et IKEV2 ou SSL. Plusieurs modes de fonctionnement sont proposés par l'Asa. Dans notre cas, nous voulons utiliser des terminaux pour pouvoir accéder aux services PMR de notre architecture. Le mode qui nous intéresse donc est le mode Site-to-Anyconnect. Pour cela, il est nécessaire d'installer l'application Anyconnect. Ce mode est asymétrique, c'est-à-dire qu'un protocole de partage de clefs est utilisé comme par exemple IKEV2 dans notre cas. Ainsi seule une authentification est nécessaire de la part de l'utilisateur. La configuration de l'Asa peut se faire comme mentionné

plus haut, par une interface graphique. Certains paramètres sont indispensable telles que la configuration du poule d'adressage IP des différents terminaux qui s'y connecteront, ou bien encore la configuration du compte pour l'authentification de l'utilisateur lors de la connexion avec l'application Anyconnect. Ainsi que la génération du certificat auto signé par l'ASA et la génération de la paire de clefs suivant le modèle RSA en 2048 bits afin que les échanges sécurisés puissent avoir lieu.

L'avantage de la solution VPN Asa Cisco en comparaison de la solution OpenVPN est sa combinaison de services de sécurité et de son architecture évolutive AIM en plus de sa fonction de VPN. En effet, il permet de mettre en place une défense proactive face aux menaces et de bloquer les attaques avant qu'elles ne se diffusent à travers le réseau, de contrôler l'activité du réseau et le trafic applicatif. L'Asa regroupe donc un firewall, des protections contre les intrusions, des listes d'accès etc...

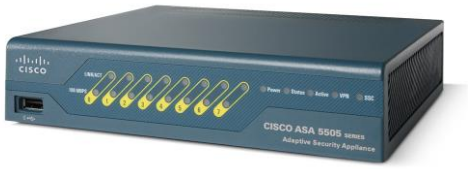


Figure 14 : Serveur de Sécurité Adaptatifs Cisco Asa 5505

E. Virtualisation

Dans le cadre de mon stage, j'ai travaillé avec des architectures de réseaux 4G/LTE. Cependant, les équipements qui constituent le cœur de ces réseaux sont d'une part coûteux, et d'autre part peuvent être encombrants. C'est notamment pour cela que j'ai travaillé avec des architectures virtualisées, qui permettent de réduire les dépenses et de gagner en place. Mais d'une manière générale, la virtualisation prend place au sein d'une tendance globale visant à placer des fonctions réseaux dans des Datacenters. Elle possède aussi des avantages en termes de sécurité. Néanmoins, la virtualisation peut s'avérer être un processus complexe, ainsi afin de bénéficier des avantages il est nécessaire que l'environnement virtuel soit bien configuré. Ces environnements permettent une réduction de matériel ce qui améliore grandement la sécurité physique. La virtualisation de serveurs peut conduire aussi à une meilleure gestion des incidents, car les serveurs peuvent revenir à un état antérieur afin d'examiner ce qui s'est produit avant et pendant une attaque. Pour donner un dernier exemple d'avantage parmi tant d'autre, la gestion des serveurs virtualisés se fait via un hyperviseur ce qui permet de réduire la surface d'attaque de l'infrastructure.

Dans mon infrastructure, concrètement, cela signifie que le MME, la SGW, la PGW et le HSS ainsi que les services PMR sont des machines virtuelles (VMs) déployées sur un serveur contenant un hyperviseur. Un deuxième serveur beaucoup plus puissant que le premier a été aussi ajouté dans la baie du ShowRoom pour accueillir des VMs tel que le PushManager qui demande quelques ressources, un serveur DNS et une autre VM Matrix, que l'on n'abordera pas en détail dans ce rapport.

Les liens qui nous intéressent donc le plus dans ce premier serveur sont :

- S1, qui va vers l'eNodeB
- SGi, qui est la passerelle vers le réseau IP (opérateur) / les autres réseaux
- Le management, qui permet de gérer l'hyperviseur

- La data, qui permet d'accéder aux services PMR

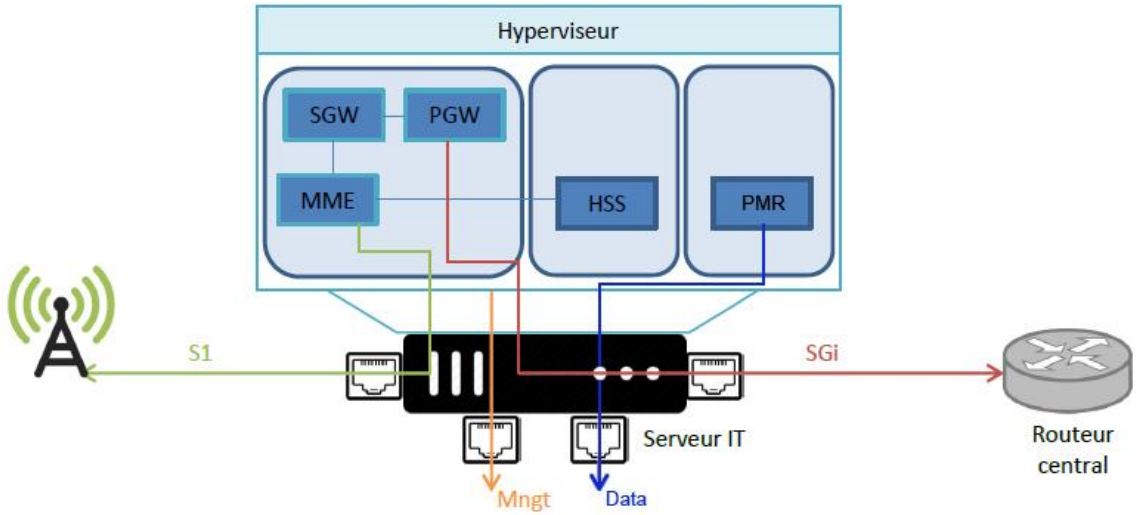


Figure 15 : Schéma d'agencement des machines virtuelles et du réseau d'un des serveurs

Dans la composition finale du serveur, on retrouve donc la dissociation de la partie management et de la partie données. Une carte réseau supplémentaire a été ajouté au serveur d'origine afin d'avoir accès à plus de port réseau. Initialement, le serveur ne comportait que deux ports Ethernet. Comme le montre la figure ci-dessus, j'ai donc pu dissocier en deux sous parties celle des données pour faire correspondre facilement le lien S1 relié à l'eNodeB et le lien SGi qui définit l'ensemble du trafic sortant de la station de base.

L'intérêt de mettre en place cette configuration, était de faciliter l'intégration de la branche LTE sur l'architecture centralisée.

Pour mettre en œuvre cette configuration en (re)partant de zéro, il a fallu que j'installe un hyperviseur sur le serveur vierge (Dell R320), que je déploie les VMs qui représentent mon cœur de réseau, que je configure le routeur central ainsi que les VMs d'un point de vue réseau, et que je raccorde l'eNodeB au bout de la chaîne. La marche à suivre pour monter cette architecture passe par des étapes clefs, il faut donc s'attacher à suivre un déroulement logique afin d'arriver au résultat souhaité.

Une fois le serveur prêt d'un point de vue physique, il fallait y installer l'hyperviseur, qui permettrait d'accueillir les machines virtuelles du cœur de réseau. J'ai donc dû récupérer le fichier ISO de la dernière version de l'hyperviseur ESXi (solution de virtualisation de VMware), depuis le site officiel de Dell, afin de s'assurer qu'il n'y aurait pas de problème de compatibilité entre le matériel hardware et le logiciel. Ensuite il a simplement suffit de rendre bootable une clef USB avec l'ISO afin de pouvoir suivre la procédure d'installation de l'ESXi.

Après l'installation de l'ESXi, il fallait y déployer les machines virtuelles. Pour ce faire, il faut pouvoir gérer l'ESXi via une interface graphique, depuis un ordinateur. J'ai donc dû installer, sur le poste de travail de la plateforme, la bonne version du « client VSphere », le logiciel permettant de manager l'ESXi. Lorsque le client est installé, il permet de se connecter à l'ESXi du serveur en renseignant, son adresse IP et son couple login/mot de passe. On a alors accès à tous les paramètres de l'hôte (CPU, RAM, mémoire ...), et c'est de là qu'on peut gérer les machines virtuelles qu'il contient.

Une fois la « structure d'accueil » prête, il ne me restait plus qu'à y mettre les VMs souhaitées.

Dans mon cas, j'avais 2 VMs à déployer/importer. Cela signifie qu'elles ont déjà été créées et qu'elles sont opérationnelles, et qu'on a un fichier (.ova) qui permet de les importer sur notre hôte, en l'état. C'est comme si ce fichier était une image à un instant donné d'un ordinateur, avec tous ses fichiers et ses caractéristiques physiques. Ensuite une fois cette partie faite, j'ai dû m'occuper de répartir les interfaces virtuelles sur différentes interfaces physiques. Cette opération se fait depuis le client VSphere, en plusieurs étapes. Dans un premier temps, il a fallu que je vérifie que les interfaces que j'avais rajoutées étaient bien détectées. Et une fois fait, j'ai dû identifier à quelle interface physique correspondaient chaque noms de la liste des interfaces. Il s'agit simplement de brancher un équipement sur un port, et de vérifier dans la liste lequel passe du statut « down » à « up ».

Après avoir décidé sur quel port physique je souhaitais brancher le routeur central, l'eNodeB et la Workstation, il m'a fallu faire des configurations depuis le client VSphere afin de faire correspondre les interfaces virtuelles aux ports physiques voulus. J'ai donc dû créer des entités appelées « VMNetwork » dans VSphere. Les VMNetworks peuvent être assignés aux ports physiques par l'intermédiaire d'un switch virtuel (cas où l'on voudrait faire sortir plusieurs VMNetworks sur le même port). Ensuite il faut identifier les interfaces virtuelles, désignées par le terme « Network Adapter » dans la liste des caractéristiques de la machine virtuelle (là encore, il s'agit d'éteindre l'interface virtuelle et de vérifier en console celle qui s'est éteinte). Une fois identifiée, il suffit d'affecter l'interface virtuelle en question au VMNetwork créé plus tôt. On peut voir ces entités sur la figure 13.

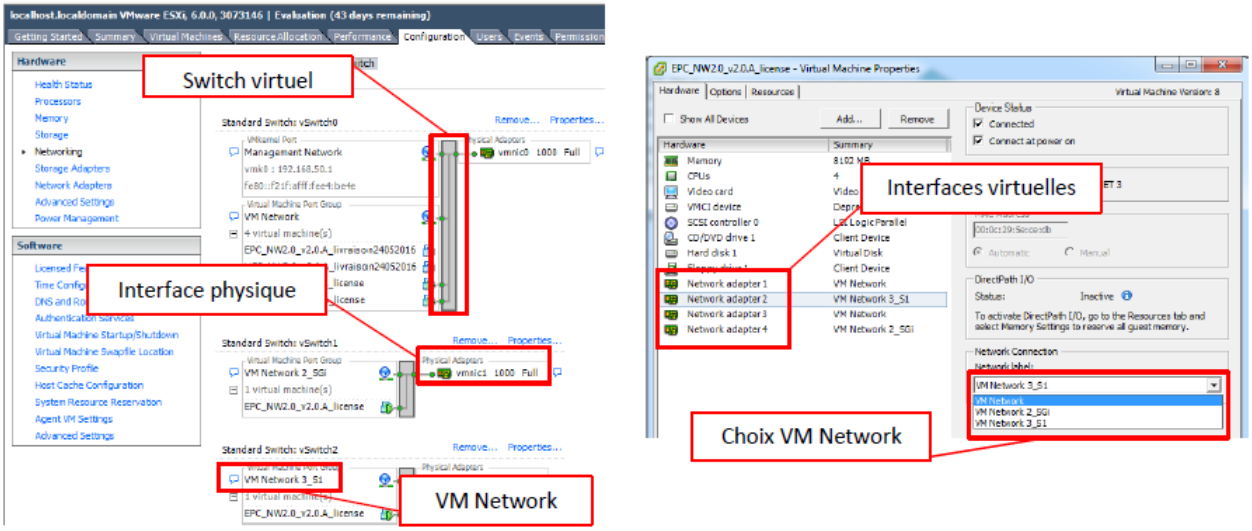


Figure 16 : Gestion des interfaces réseaux dans VSphere

IV. Expérimentations

Le projet **FED4PMR** pour lequel j'ai travaillé durant toute la période de mon stage, piloté par Thales, fédère différents réseaux 4G/LTE. Il s'appuie sur les nouvelles fréquences 4G allouées au Ministère de l'Intérieur pour proposer un système qui offre une large couverture, une capacité de résilience et une forte sécurité. En cas de crise majeure, tous les acteurs ayant un rôle à jouer doivent pouvoir disposer d'un accès prioritaire au réseau disponible de manière instantanée et automatique. Ils doivent pouvoir échanger des données plurimédia sans se soucier des défaillances de leur réseau. Forces de l'ordre, pompiers, SAMU, mais aussi Opérateurs d'Importance Vitale ou collectivités : FED4PMR a pour ambition de faire interagir leurs réseaux de manière à pallier d'éventuelles absences de couverture ou saturations.

1. SNCF (Saint Denis)

Le 8 décembre 2016, Thales a invité une cinquantaine de ses prospects et partenaires à la restitution d'une expérimentation en conditions opérationnelles des systèmes 4G/LTE professionnels développés dans le cadre du projet Fed4PMR, lancé en février 2016. Parmi les invités on pouvait compter plusieurs représentants du Ministère de l'Intérieur, de la Défense, de la Gendarmerie nationale, des Pompiers de Paris, d'EDF, etc.

Il s'agissait de la première expérimentation du projet Fed4PMR qui en compte en tout trois. Cette expérimentation s'est déroulée en conditions opérationnelles réelles et s'est appuyée sur un réseau 4G hybride (4G opérateur, 4G dédié à la fréquence 700 MHz). Elle est le résultat des premiers travaux collaboratifs de développement et d'intégration qui ont eu lieu courant 2016 entre les partenaires du projet dans la construction des briques de base d'un futur réseau PMR haut débit.

De nombreuses applications (appels de groupes, appels d'urgences, échanges de photos, échange de vidéo en temps réel, vidéo mobile, vidéo-surveillance, géolocalisation, poste de commandement multimédia fixe et mobile, interconnexion avec le réseau TETRA…) et terminaux à destination des forces de sécurité et de secours ont pu être testés sur le réseau 4G hybride déployé. Ces nouvelles capacités ont été mis dans les mains d'utilisateurs lors des avant match de rugby aux abords des stations de RER desservant le Stade de France ; ils ont très rapidement pu prendre en main ces nouveaux outils (aspects intuitifs), et ont pu avoir une préfiguration de leurs futurs outils de communications. Cette mise en situation a généré de nombreux échanges entre les utilisateurs et les membres du consortium afin de mieux adapter l'ergonomie du système aux contraintes du terrain et permettra d'accélérer la mise à disposition de ces solutions.

Le projet Fed4PMR adresse le marché des radiocommunications professionnelles très haut débit à usage des ministères de l'Intérieur et de la Défense, des opérateurs de transport et des industries de l'énergie pour des missions civiles et militaires.

2. Ma place

Dans le cadre de mon stage j'ai eu l'opportunité de participer à cette journée d'expérimentation pour le projet Fed4pmr. J'ai aussi participé pendant les deux semaines en

amont de cette journée à la mise en place de l'infrastructure et à la réalisation des tests. J'ai intégré sur le système le service QualIT afin de pouvoir qualifier l'état du réseau pendant les différents tests de communications. En parallèle de ces tests, j'étais aussi responsable de l'entreprise partenaire Ibelem. Je devais leur fournir un accès au service Push Manager par le réseau SFR pour la journée de démonstration afin qu'il puisse présenter leur logiciel aux différents invités et représentants du Ministère de l'Intérieur, de la Défense, de la Gendarmerie nationale, des Pompiers de Paris, d'EDF, etc…

Lors de ma première journée au sein des locaux de la SNCF où allait se dérouler la journée d'expérimentation, Marc m'a présenté l'ensemble de l'infrastructure. Une antenne directrice était mise sur le balcon extérieur du 3ème étage des locaux. Elle était reliée à un convertisseur d'ondes radio en données numérique. L'intérêt de séparer la tête radio du convertisseur est de pouvoir déployer plus facilement l'antenne sur des hauteurs ou zone difficile d'accès. L'inconvénient, c'est qu'il ne faut pas non plus trop les éloigner au vu des pertes considérable dans les câbles coaxiales, câbles reliant l'antenne et le convertisseur. Le convertisseur était ensuite relié par de la fibre optique directement au serveur contenant les VMs EPC, HSS et les services PMR. J'ai volontairement omis de décrire des systèmes comme le système permettant de faire la translation entre des paquets LTE et TETRA positionné entre le serveur et le convertisseur, car je ne les ai pas vu pendant mon stage, j'ai découvert la technologie très brièvement lors de cette première visite. Marc m'a ensuite montré le poste de commandement, relié aux services via un routeur, avec notamment la nouvelle version du Dispatcher et ses fonctionnalités supplémentaires ainsi qu'un logiciel permettant de contrôler une caméra domotique à distance et de récupérer son flux vidéo. Il m'a ensuite montré les différents équipements qui seront présentés lors de la journée d'expérimentation et nous avons discuté sur les différentes intégrations qu'ils restaient à faire.

Durant la deuxième journée, j'ai commencé à installer le service QualIT et je suis allé faire quelques tests avec d'autres ingénieurs dans la rue pour avoir une idée de la robustesse des communications et de la limite du réseau. J'ai été agréablement surpris de la portée d'émission de l'antenne. Le local de la SNCF étant situé en plein milieu des gares RER B et RER D de la Plaine-Saint-Denis, l'ensemble de la zone était couverte. Durant cette journée, j'ai aussi montré Thales Eye à plusieurs ingénieurs de la SNCF qui étaient très intéressés par le concept.

J'ai rencontré le responsable de produit Push Manager lors de ma troisième journée dans les locaux. Je lui ai présenté rapidement l'architecture qui avait été mise en place. Nous avons beaucoup discuté concernant les axes futurs de développement du PushManager car de nombreux retours m'ont été faits de la part de quelques personnes en interne du service après leur avoir fait une présentation du produit. Ces discussions étaient très constructives, et j'ai pu apprendre beaucoup de choses que j'ignorais sur le Push Manager. Il m'a fait une présentation du produit tel que lui il le voyait. J'ai pu observer qu'il tenait une version plus orienté sur les domaines d'activités et les futures utilisations du Push Manager, sans vraiment rentrer dans les détails de configurations et de fonctionnalités. Choses que je ne faisais pas du tout lors de mes présentations, j'étais beaucoup plus fixé sur les aspects techniques du logiciel. J'ai aussi profité de cette journée, pour lui montrer le système qui allait être utilisé lors de la journée d'expérimentation, et les différents qu'il y avait entre la version privée dans la plateforme du ShowRoom et celle qu'il avait l'habitude d'utiliser dans le cloud. En effet, l'objectif était d'utiliser des cartes Sim SFR afin de pouvoir atteindre le serveur PushManager situé dans le ShowRoom. Nous allons voir plus en détail le fonctionnement de ce logiciel dans la partie suivante.

3. Gestionnaire de flotte

Ibelem est un intégrateur de MDM, c'est-à-dire un gestionnaire de terminaux. Ils proposent à leurs client la solution (parmi toutes celle qu'Ibelem proposent) la plus adaptée à leurs besoins. Mais cette société développe aussi son propre gestionnaire sécurisé de terminaux : le Push Manager. Le push Manager est multi OS, en d'autre terme il prend en charge les terminaux sous IOS, Android, Windows et BlackBerry. Une des particularités de ce logiciel est son mode de fonctionnement. Il peut être utilisé en mode SaaS, c'est-à-dire en tant que simple software basé dans un cloud (les DataCenters d'Ibelem sont hébergés en France). Dans ce mode lorsque nous voulons exécuter une action sur un terminal, le Push Manager envoie une notification à ce dernier en passant par les serveurs de Google. Le deuxième mode d'utilisation est le mode dédié. Nous reviendrons sur ce deuxième mode plus tard. L'objectif premier du Push Manager est de permettre une supervision et une configuration à distance de masse. Le logiciel nous offre donc une multitude de possibilités, de configurations, de graphiques afin de nous représenter et de gérer notre flotte. Par exemple, nous pouvons créer des blacklist d'applications mobile. L'utilisateur ne pourra donc pas installer les applications interdites. Une autre particularité est le Push Silencieux. En tant qu'admin du terminal, le MDM peut pousser une configuration, installer des applications silencieusement, c'est-à-dire sans action de confirmation de la part de l'utilisateur.

Dans la plateforme du Showroom, j'ai donc intégré le logiciel sur un de mes serveurs. En annexe 5 se trouve la page d'accueil du logiciel. Comme mentionné au-dessus, le Push Manager possède deux modes de fonctionnement. Etant dans un milieu isolé de toute connexion vers l'extérieur, le mode SaaS est à proscrire. Nous devons utiliser le mode dédié. Ce mode est aussi appelé « Polling » car ce n'est plus le MDM qui envoie des notifications aux terminaux quand il a besoin d'exécuter une action, mais ce sont les terminaux qui vont se réveiller toutes les minutes par exemple, pour demander aux Push Manager si il a des mises à jour, des actions à leur faire faire. Ce mode présente donc un inconvénient : lorsqu'une configuration est poussée via le push Manager, il faut attendre que les terminaux se réveillent pour que le changement se fasse. Cela peut donc prendre un temps plus ou moins long selon la configuration de la durée d'attente entre chaque réveil. L'optimisation de cette durée selon la taille de la flotte joue un rôle important.

En application avec les services PMR, le Push Manager possède un très grand potentiel. Prenons par exemple un déploiement pour une mission d'une troupe de police. Chaque policier avant de partir va devoir s'équiper d'un terminal afin de pouvoir communiquer avec le reste de son équipe. Le policier va donc récupérer un terminal dans un mode de standby avec une configuration minimal. Il va rentrer son identifiant et son code mission via un portail ou une application tierce. Suite à cela, l'ensemble du profil destiné à cet utilisateur pour cette mission sera poussé automatiquement sans que le policier n'ait à faire quoi que ce soit de plus. Une nouvelle interface (Kiosk) va se mettre en surcouche du terminal et laisser apparent seulement les applications nécessaires au bon déroulement de l'opération (application VoIP, diffusion de flux vidéo, géolocalisation etc…). Lorsque l'opération est terminée, le policier déconnecte son profil, et le terminal est automatiquement remis à l'état de standby avec sa configuration minimal.

4. Autres expérimentations

Pour la fin de mon stage, Emmanuelle m'a donné l'opportunité de participer à la démonstration pour le Ministère de l'intérieur dans les locaux de Thales. Ma mission était, avec l'aide de Marc, de déployer une bulle tactique LTE pour accéder aux services PMR. Marc

s'occupait de déployer l'antenne et en parallèle je faisais le raccordement des différents équipements. Les démonstrations s'étalaient sur deux jours. Le premier jour, le GIGN est venu puis le RAID le deuxième. Une des conditions était de déployer en moins de 10 minutes la bulle tactique, c'est-à-dire que les services deviennent opérationnels et que les terminaux s'accrochent sur le réseau. La deuxième journée était beaucoup plus ludique, nous avons accueilli le chef de l'état-major du RAID qui nous a fait un retour de terrain de vrais évènements qu'il a dû gérer comme par exemple l'attentat du Bataclan. Dans ce genre de cas, le temps est une ressource rare.

Je devais aussi effectuer un déplacement pendant deux semaines dans une centrale nucléaire à Bordeaux dans le cadre également d'une expérimentation pour EDF. Au final, je n'ai pas pu y aller à cause d'un manque de financement. J'ai été déçu d'être mis de côté, notamment après avoir préparé la mise en place du PoC pour présenter les différentes possibilités, comme la diffusion de flux vidéo, l'utilisation d'un drone et les services PMR, qu'offre la technologie LTE.

V. Bilans

Bilan personnel

Mes principaux objectifs lors de mon stage, étaient de faire des tests fonctionnels sur un système, et d'y intégrer des applications innovantes. Comme je l'évoquais au début de ce rapport, je considère ces objectifs comme « ouverts », dans la mesure où on pourrait toujours faire plus de tests et surtout, continuer à intégrer d'autres applications. Cependant, via l'ensemble du travail que j'ai décrit dans les paragraphes précédents, je pense avoir atteint ces objectifs. En particulier concernant la mission de réalisation d'une architecture multi-accès avec l'interconnexion de plusieurs réseaux, où j'ai bel et bien rempli cet objectif, même si cette plateforme est amenée à encore évoluer.

Durant mon stage, j'ai eu l'occasion de mettre en œuvre un certain nombre de compétences, acquises au cours de mon cursus d'ingénieur. C'est particulièrement le cas dans le domaine réseau, où j'ai eu l'occasion de configurer du matériel Cisco, et de gérer un réseau (adressage, routage, vlans etc.). Ce sont effectivement des compétences que j'ai pu acquérir à l'UTT, via les travaux pratiques notamment. J'ai également pu mettre en pratique, et donc développer, des notions théoriques abordées en cours, telles que la virtualisation et les VPN. J'ai pu aussi découvrir un sujet que je ne connaissais que très peu sur les architectures de réseaux sans fils (4G). Ce sont des connaissances importantes, qui m'ont permis de mieux comprendre les systèmes avec lesquels j'ai travaillé, et réciproquement, j'ai pu approfondir ma compréhension de ces notions.

Mon stage m'a également permis d'acquérir certains automatismes, par exemple dans le processus de réflexion lors de phases d'intégration ou de tests. En effet, il faut prévoir la manière d'effectuer les tâches ou les tests pour vérifier un paramètre en particulier, et avancer par étape pour trouver (puis résoudre) un problème. J'ai également pu avoir une vision de recul sur les différents projets auxquels j'ai pu assister grâce aux retours de certaines personnes tel que le RAID sur leur façon d'utiliser les technologies comme évoqué précédemment dans le rapport. Il y a également le fait, que les interlocuteurs peuvent être dans des zones géographiques différentes de la nôtre, et qu'ils n'ont pas forcément un accès physique au système. C'était le cas avec Ibelem. Cela signifie qu'il faut cibler leurs demandes ou besoins, afin de leur fournir les bonnes informations. Enfin, ce stage a été l'occasion de continuer à développer rigueur et organisation, à travers la gestion du temps notamment, pour être en mesure de répondre aux attentes et d'effectuer les tâches demandées. Il s'agit donc d'être organisé afin de pouvoir gérer plusieurs choses à la fois.

La gestion du temps a été un paramètre important durant mon stage. Il a fallu que je m'organise pour ne pas me laisser déborder, surtout lorsque j'ai dû gérer plusieurs choses à la fois (travail sur 2 intégrations en parallèle, rédaction de documentations, gestion du matériel, etc.). Ceci était clairement ma faiblesse pendant ce stage. Mon responsable me ramenait souvent de nouvelles technologies, et étant de nature très curieux, je m'y intéressais tout de suite alors que ce n'était pas forcément la tâche la plus importante à faire sur le moment. J'ai réussi néanmoins à finir dans les temps les différentes tâches demandées. N'ayant pas été pleinement confronté à ces difficultés d'organisation pendant mon dernier stage, je n'ai pas pu avoir du recul sur mes capacités de gestion. Je sais maintenant plus précisément quel axe je dois améliorer dans ma vie professionnelle future.

Je retire beaucoup de choses de ce stage. Tout d'abord, d'une manière générale, j'ai vraiment le sentiment que mon stage s'est inscrit dans la continuité de mon parcours télécom, réseaux et sécurité. Le stage de fin d'étude représente une véritable occasion d'appliquer/mettre en œuvre les compétences acquises à l'UTT. J'ai vraiment pu faire le lien entre les notions abordées en cours, et leurs applications concrètes dans un système, une solution, un produit. J'ai également une meilleure vision sur le métier d'ingénieur, où l'une des qualités importantes doit être l'adaptabilité. En effet, il faut savoir faire face aux imprévus, et être capables de gérer plusieurs choses en même temps. Ainsi, j'ai apprécié qu'on m'ait confié plusieurs tâches en parallèle, avec une certaine autonomie. Même si cela peut être assez déroutant au début car le rythme peut être soutenu, cela permet de rentrer dans le vif du sujet assez vite. Cela a été très formateur, car ça m'a permis de voir beaucoup de choses. Mon stage a donc confirmé ma vision qu'un ingénieur aujourd'hui doit être multitâche, et polyvalent.

Je pense que j'ai principalement apporté à l'entreprise mes compétences pratiques et théoriques, dans le domaine des télécoms, réseaux et sécurité. J'ai également mis en place une architecture centralisée, qui offre la possibilité de continuer à intégrer des applications dessus.
Concernant les outils que j'ai pu utiliser, il y en avait certains que je connaissais et maitrisais (au moins en partie) tel que l'environnement Linux et Cisco notamment. Pour d'autres je connaissais simplement leur existence, mais je ne les avais jamais utilisés (VMware ESXi / VSphere, Vpn SSL/IPSec). Enfin, certains m'étaient totalement inconnus, comme l'outil Qual'IT par exemple. Globalement, j'ai découvert beaucoup de logiciels dans le cadre de l'intégration d'applications, notamment sur les thèmes du VPN avec l'Asa de Cisco par exemple. Beaucoup d'équipements avec lesquels j'ai travaillé avaient une interface Web de configuration, permettant de contrôler et paramétrer rapidement ces appareils. C'est le cas pour les eNodeB. Je maîtrise également mieux la gestion des paramètres réseaux dans les smartphones Android.

Jusqu'à présent, j'ai fait mes deux stages chez Thales Communication & Security. Les grandes structures comme Thales, présentent l'avantage d'avoir une grande diversité de compétences et de profils. Il est très enrichissant de pouvoir travailler avec des gens ayant des cursus, des expériences et des champs de compétences différents des nôtres, et donc qui n'ont pas forcément la même vision des choses que nous. Les grands groupes, et en particuliers Thales, possèdent beaucoup de domaines et secteurs d'activités différents. Il y a donc de nombreuses possibilités pour élargir son champ de compétences et varier les expériences, tout en restant au sein du groupe. J'ai effectivement changé complètement de domaine entre mes deux stages chez eux. Le premier était orienté développement logiciel sur des équipements embarqués dans des Rafales. Contrairement au second, où je n'ai que très peu développé et vu beaucoup plus l'aspect réseau, télécoms et sécurité dans un domaine civil.

Finalement, ce stage m'a vraiment permis d'affiner mon orientation professionnelle. Avant ce stage, cela restait assez flou, et je me voyais plus dans de la recherche et développement sur des sujets comme le machine Learning ou la cybersécurité. C'est la curiosité de ce que Thales pouvait proposer à des clients militaires et civils, sur le domaine de la 4G qui a orienté mon choix de stage. Ce sujet était relativement « mystérieux », car c'est un sujet que je n'avais pas vu pendant mon cursus à l'UTT.

Projets professionnels

Je pense qu'avec mon cursus et les différentes expériences que j'ai acquises durant mes stages, je suis en mesure d'évoluer dans ce milieu professionnel. En effet, en plus des capacités techniques assimilées lors de ma formation, le fonctionnement par projet m'a permis de gagner en autonomie. L'autonomie a été une composante importante de mon stage, où j'ai pu montrer ma capacité à faire face à différentes situations. Cela se traduit également par le fait de savoir s'adresser aux personnes les plus aptes à fournir les informations permettant d'avancer dans la résolution d'un problème.

Les principales difficultés de ce milieu se trouvent, à mon sens, lorsqu'on arrive dans un projet. En effet, jusqu'à ce stage et notamment dans les projets scolaire, on commence toujours un projet à partir de zéro, et même si cela n'est pas aisé, on définit nous-même tous les aspects de notre travail. Dans ce milieu professionnel, on arrive en général sur un projet déjà en cours, et il faut un certain temps pour s'adapter aux diverses contraintes, connaître le produit et en maîtriser les différents aspects. De plus, certaines phases peuvent se montrer plus éprouvantes que d'autres, comme les démonstrations ou les livraisons aux clients par exemple.

Ce stage m'a permis de découvrir en partie le métier d'ingénieur IVVQ, notamment car j'ai pu travailler avec quelques ingénieurs IVVQ. L'aspect de mon stage qui consistait à effectuer des tests sur des systèmes, afin de les faire fonctionner correctement, m'a paru proche de ce que faisaient les ingénieurs en IVVQ. Cependant je n'ai pas eu de vision sur l'aspect « process » de l'IVVQ, avec les procédures de rédactions et validation des fiches de tests par exemple. J'ai également pu avoir une nouvelle vision sur le type de produits qu'on peut fournir à des clients militaires et civils (réseaux de transports, aéroports, services de santé, etc.).

Durant ma formation d'ingénieur, j'ai toujours souhaité que mes premières années dans le monde professionnel se fassent sur un poste qui me permettrait de mettre en avant mes compétences techniques. Je pense qu'un poste en IVVQ est bien adapté à cette envie, tout en me permettant de conserver l'aspect pluridisciplinaire des télécoms, réseaux et sécurité de mon profil.

Au cours de mon stage, j'ai bénéficié des processus internes à Thales concernant les stagiaires et apprentis. J'ai ainsi été contacté par plusieurs services intéressés par mon profil. Au cours de ce processus, un des services dans les systèmes ferroviaires intégrés pour des projets au Qatar, m'ont fait une proposition d'embauche pour un poste en tant qu'IVVQ. Attendant quelques jours pour avoir une réponse des autres entretiens passés, j'ai finalement choisis ce poste au sein duquel je travaillerai à l'échelle du sous-système pour l'international. J'ai orienté mon choix sur ce poste car je serai amené à me rendre sur place, je serai en contact avec les clients, le poste est technique avec l'intégration et la mise en place de tous les systèmes de télécommunications, d'infrastructures réseaux et de sécurité avec la mise en place de contrôle d'accès, et de caméras de surveillances. J'intègre l'équipe le 1er mars.

Mon projet professionnel à court terme est donc clairement défini. A moyen terme, je n'ai rien d'aussi précis en tête, cependant j'ai quand même une réflexion sur le sujet…

VI. Conclusion

Ce stage de fin d'étude au sein du groupe THALES a été très formateur. Il m'a permis d'acquérir beaucoup d'expérience tant sur l'aspect humain que scientifique.

Après une première période au cours de laquelle mon intégration au sein du service Wireless NetWork (WNW) s'est faite progressivement et naturellement, j'ai découvert mon environnement de travail ainsi que les activités et systèmes développés par le service. Mon tuteur M. Eric Robert m'a alors présenté les différentes missions sur lesquelles j'allais être amené à travailler.

Par ailleurs, j'ai eu la chance d'accomplir un stage de fin d'étude en relation avec les cours suivis dans ma spécialité réseau et télécoms, ce qui m'a permis de prendre tout de suite confiance quant aux missions, et surtout de mettre à profit mes connaissances scientifiques.

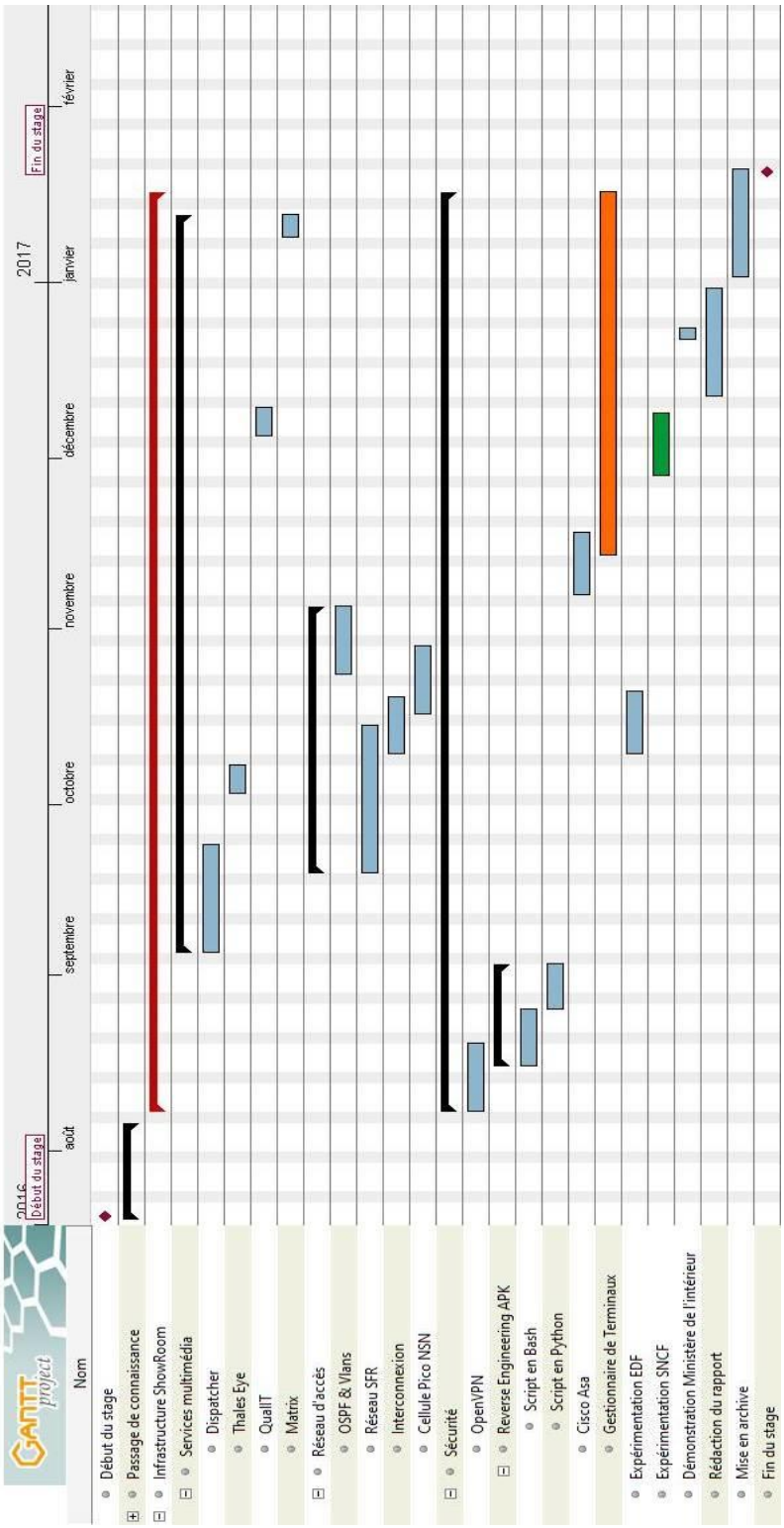
Les missions qui m'ont été confié durant ce stage ont toujours été remplies dans leur globalité. Ma mission principale a été l'implémentation de scénarios de démonstration opérationnelle avec la mise en place de services sur le système PMR 4G/LTE (Nexium Wireless) :

- Intégration de services vidéo/photo entre poste de supervision et terminaux
- Mise en place d'un système d'accès à distance sécurisé VPN
- Intégration du gestionnaire de terminaux Push Manager
- Intégration d'une application de réalité augmentée
- Configuration d'une architecture réseau

Enfin, j'ai eu la chance de pouvoir participer au déploiement du système sur site et aux démonstrations aux clients des différents services intégrés au travers de scénarios opérationnelles.

VII. Annexes

Annexe 1 : Diagramme de Gantt



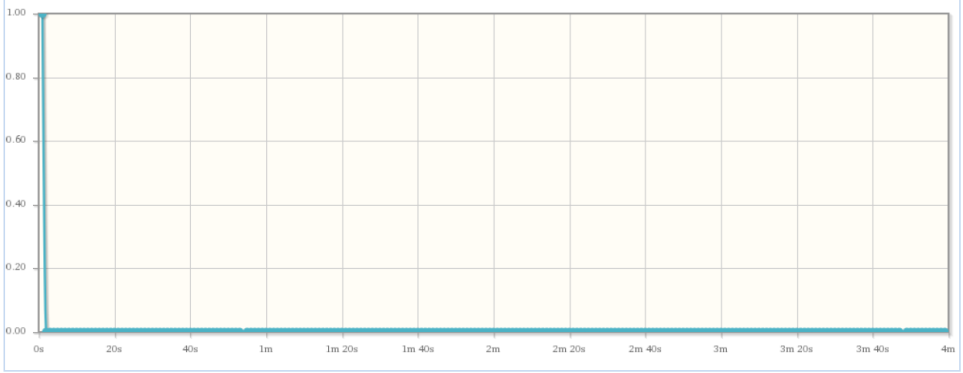
Annexe 2 : Résultats QualIT

Résultat de la paire 1	
Statut	Echec

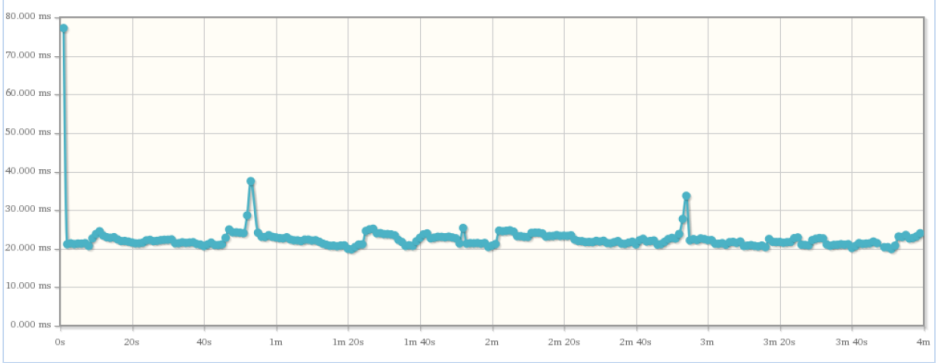
	Nom de la box	Adresse	Management	Zone
Source	LTEDongle19	10.8.37.19	192.168.1.92	Zone base
Destination	HP	10.8.8.33	192.168.1.94	Zone base

Indicateurs mesurés					
Indicateur	**Mesure**		**Seuil**	**Tolérance**	**Statut**
Débit Minimum	0.061				Info
Débit Moyen	0.064				Info
Débit Maximum	0.065				Info
Paquets perdus	1	<	3		Succès
Paquets déséquencés	0				Info
Maximum paquets perdus successifs	1				Info
Pourcentage paquets perdus	0.01 %	<	3 %		Succès
Latence Moyen	22.534 ms				Info
Latence Maximum	77.204 ms	<	150 ms		Succès
Latence Minimum	19.788 ms				Info
Gigue	99.007 ms	<	60 ms		Echec
MOS Minimum	2.33	>	3.2		Echec
MOS Moyen	4.34				Info
MOS Maximum	4.37				Info
Paquets perdus / buffer de gigue	5				Info

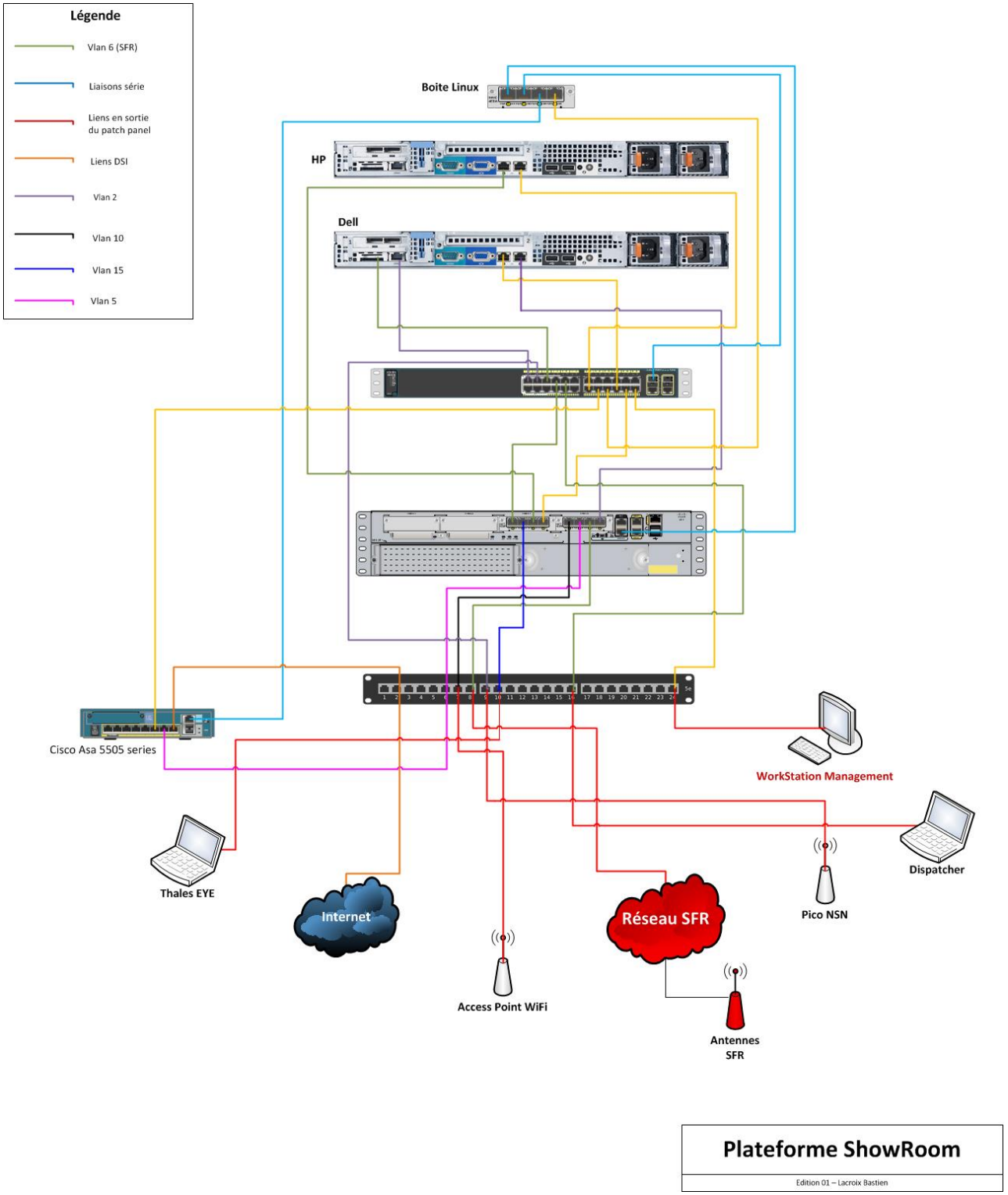
Paquets perdus



Latence



Annexe 3 : Architecture du ShowRoom

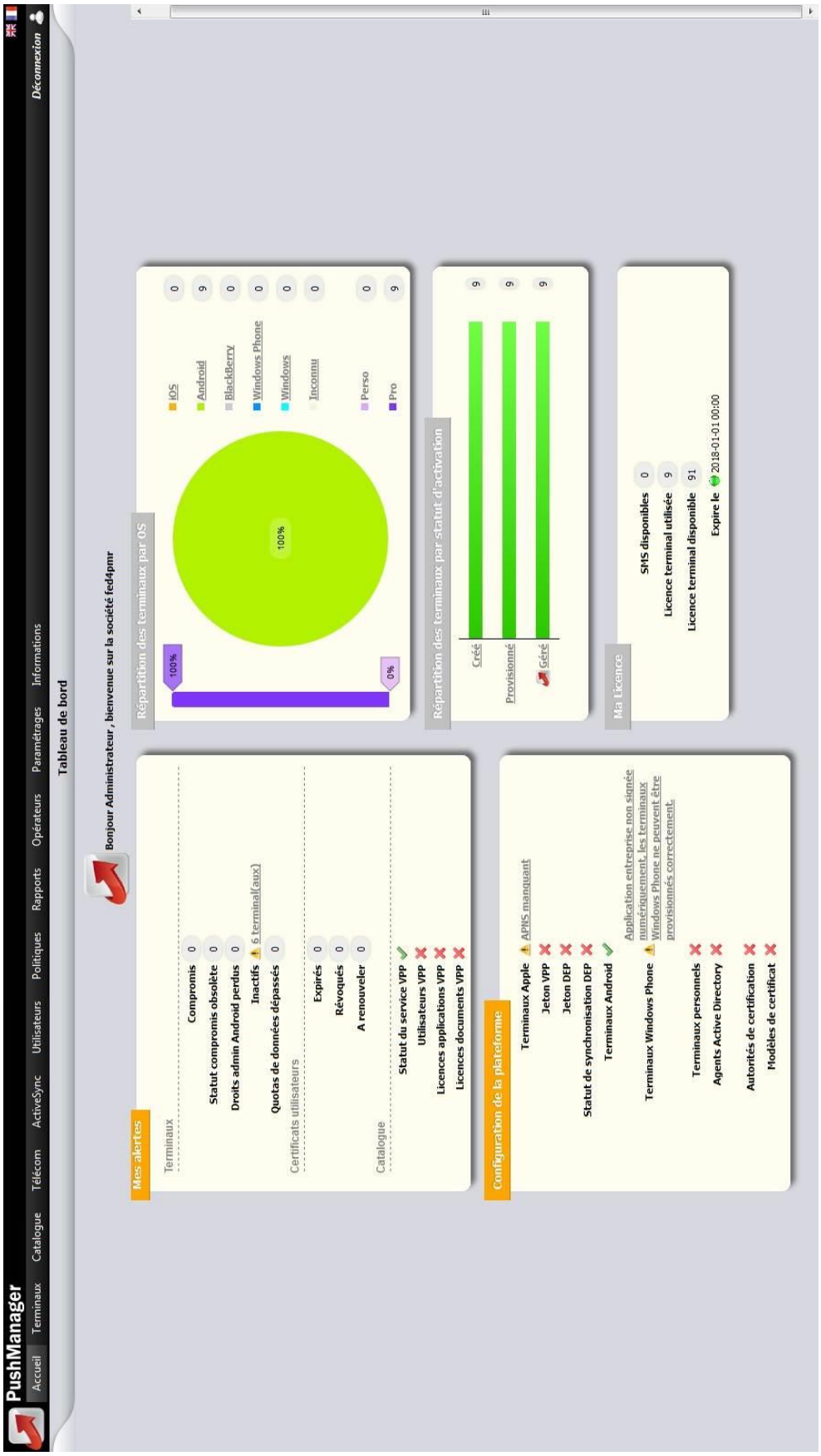


Annexe 4 : Script Python

```
#!/usr/bin/env python
# -*- mode: python; coding: utf-8 -*-

import sys
import os
import csv
import time
import re


print( "--------------------------------------------------------------------")
print( "  ______   __  __   ______   __   __   ______   ______  " )
print( " /\__  _\ /\ \_\ \ /\  __ \ /\ \ /\ \ /\  ___\ /\  ___\ " )
print( " \/_/\ \/ \ \  __ \\ \ \/\ \\ \ \\ \ \\ \___  \\ \  __\ " )
print( "    \ \_\  \ \_\ \_\\ \_____\\ \_\\ \_\\/\_____\\ \_____\ " )
print( "     \/_/   \/_/\/_/ \/_____/ \/_/ \/_/ \/_____/ \/_____/ ")
print( " ")
print( "-------------------------------------------------------------------- ")

apktool = "./apktool.jar"
apk = "NexiumTerminal_2.0.1.185.apk"
apkFolder = "NexiumTerminal_2.0.1.185"
framework = "framework-res.apk"
ScriptFolder = os.getcwd()

os.system("java -jar " + apktool + " if " + framework)
os.system("java -jar " + apktool + " if " + apk)

os.system("java -jar " + apktool + " d " + apk)
print("Decompilation of " + apk + " done.")

with open('Clients.csv', newline='') as csvfile:
        reader = csv.reader(csvfile, delimiter=',', quotechar='|')
        Imsis = []
        Uris = []
        Servers = []
        Calls = []
        Ptts = []
        i=0
        for row in reader:
            if i == 1 :
                os.chdir(ScriptFolder+"\\NexiumTerminal_2.0.1.185\\res\\xml")
                Imsi = row[0]
                Uri = row[1]
                Server = row[2]
                Call = row[3]
                Ptt = row[4]

                Imsis.append(Imsi)
                Uris.append(Uri)
                Servers.append(Server)
                Calls.append(Call)
                Ptts.append(Ptt)

                with open("preferences.xml",'r') as input:
                    clean =
re.sub(r'(<EditTextPreference.*title\=\"\@string\/pref_client_uri\".*)(\"[0-
9]*\")(.*)',r'\1"'+Uri+r'"\3', input.read())

                with open("preferences.xml",'w') as output:
                    output.write(clean)

                with open("preferences.xml",'r') as input:
                    clean =
re.sub(r'(<EditTextPreference.*title\=\"\@string\/pref_serv_ip\".*)(\"[0-9]*[.][0-9]*[.][0-
9]*[.][0-9]*\")(.*)',r'\1"'+Server+r'"\3', input.read())

                with open("preferences.xml",'w') as output:
                    output.write(clean)

                with open("preferences.xml",'r') as input:
                    clean =
re.sub(r'(<EditTextPreference.*title\=\"\@string\/pref_call_priority\".*)(\"[0-9]*[.][0-
9]*[.][0-9]*[.][0-9]*\")(.*)',r'\1"'+Call+r'"\3', input.read())
```

```
                with open("preferences.xml",'w') as output:
                    output.write(clean)

                with open("preferences.xml",'r') as input:
                    clean =
re.sub(r'(<EditTextPreference.*title\=\"\@string\/pref_ptt_priority\".*)(\"[0-9]*[.][0-
9]*[.][0-9]*[.][0-9]*\")(.*)',r'\1"'+Ptt+r'"\3', input.read())

                with open("preferences.xml",'w') as output:
                    output.write(clean)

                os.chdir(ScriptFolder)
                os.system("java -jar " + apktool + " b " + apkFolder)

                pathApk=ScriptFolder+"\\"+apkFolder+"\\dist\\"+apk
                pathKeystore =ScriptFolder+"\\ThalesAndroidKey"
                pathZip = "C:\\Users\\thales\\AppData\\Local\\Android\\sdk\\build-
tools\\24.0.2\\zipalign.exe"
                nameOfNewApk =
"C:\\Users\\thales\\Desktop\\ApkRe\\ModifyApk\\Nexium"+Uri+"_"+Call+"_"+Ptt+".apk"
                os.system("jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore
"+pathKeystore+" -storepass tetratetra "+pathApk+" thales")
                os.system(pathZip+" -v 4 "+pathApk+" "+nameOfNewApk)
            i=1
```

Annexe 5 : Push Manager



VIII. Références

- **Livre** –Yannick Bouguen, Eric Hardouin et François-Xavier Wolff.**,** *LTE et les réseaux 4G*. Ch: **«** *Interférences intercellulaire dans le cadre des eNodeB* **»**. Eyrolles, 2012, 548 p. 978-2-212-12990-8

- **Livre** –Yannick Bouguen, Eric Hardouin et François-Xavier Wolff.**,** *LTE et les réseaux 4G*. Ch: *« L'interface radio du LTE »*. Eyrolles, 2012, 548 p. 978-2-212-12990-8

- **Ebook** – Craig Hunt. *TCP/IP Network Administration*. 3rd Edition. O'Reilly, 2002, 748 p. 978-0-596-00297-8. [26/01/2017]. PDF, 6.8 Mo

- **PowerPoint** – *LTE et évolutions vers la 4G*. Centre de formation Radio Data Com. Lien : http://www.formation-radio.com.

- **Web / Mooc** – Xavier LAGRANGE, Christophe COUTURIER, Philippe MARTINS, Alexander PELOV. *Fun Mine Télécom, Comprendre la 4G – session 2* [en ligne]. Mis à jour le 17 juin 2016. [Consulté le 26/01/2017]. Disponible sur : https://www.fun-mooc.fr/courses/MinesTelecom/04010S02/session02/info

- **Web / Mooc** – Géraldine Texier, Samer Lahoud, Claude Chaudet. *Fun Mine Télécom, Routage et qualité de service dans l'internet* [en ligne]. Mise à jour le 26 janvier 2017. [Consulté le 26/01/2017]. Disponible sur : https://www.fun-mooc.fr/courses/MinesTelecom/04011S03/session03/info