Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Stage au sein du pôle technique télécoms et réseaux d'EDF

Thomas RICHARD

EDF

Responsable entreprise: Thomas REUTENAUER

Responsable académique: Éric SOCCORSI

2019

Table des matières

Introduction

Dans le cadre de ma formation à l'Institut Universitaire de Technologie de Luminy en DUT Réseaux et Télécommunications (Diplôme Universitaire Technologique), j'ai eu l'opportunité d'effectuer un stage professionnel en entreprise d'une durée de 10 semaines, du 8 avril 2019 au 14 juin 2019.

Cette formation étant axée sur les réseaux et les télécommunications, je souhaitais trouver un stage qui relie ces deux domaines. J'ai de ce fait centré mes recherches sur des entreprises pouvant m'offrir une mission répondant à mes attentes.

J'ai donc déposé ma candidature au sein du groupe EDF, Électricité De France, et plus précisément au PTTR, Pôle Technique Télécoms & Réseaux, à Marseille qui m'a accepté et m'a proposé un stage dans le domaine de la ToIP*. La cellule au sein du PTTR dans laquelle je me situe est la CEC, Cellule d'Exploitation Centralisée. Elle met à disposition son savoir-faire dans les télécommunications aux autres chaînes de services. La CEC exploite les équipements réseaux et télécoms tertiaires c'est-à-dire qu'elle s'occupe à la fois des incidents télécoms mais aussi des demandes de services afin de maintenir un niveau de disponibilité maximum pour ses utilisateurs. Une des missions complémentaires de la CEC est d'être un appui pour les projets télécoms régionaux et nationaux.

Mon objectif premier durant ce stage était de découvrir le travail en entreprise en vue de poursuite d'études en alternance. En effet, je souhaite continuer mes études en licence professionnelle ASUR, Administration et Sécurité des Systèmes et des Réseaux, afin d'approfondir mes connaissances actuelles concernant les réseaux. De plus, un de mes autres objectifs durant ce stage était de mettre en application certaines connaissances acquises durant ma formation de deux ans dans l'IUT pour pouvoir répondre au mieux aux missions que l'on m'a proposées.

En effet, j'ai pu réfléchir à une solution de surveillance des charges reçues par les PA RIN*, Point d'Accès au Réseau d'Interconnexion National, sur les sondes* des sites EDF. J'ai aussi utilisé ces sondes pour surveiller le MOS, Mean Opinion Score*, durant une mission de migration d'un site en softphonie. Enfin, j'ai participé à la mise à jour des sondes des sites EDF.

Pour présenter au mieux mon stage, je vais commencer par présenter le groupe EDF et plus précisément la branche dans laquelle j'ai évolué ; je vais également expliquer les tâches réalisées tout au long de ce stage et pour finir je vais faire un bilan pour distinguer les compétences acquises pendant le stage et prendre du recul par rapport à cette première expérience pour moi.

1 Présentation de l'entreprise

Le groupe EDF produit, transporte et distribue l'électricité en France, mais aussi en Europe et dans le Monde. L'entreprise compte plus de 165 000 employés à ce jour. Son chiffre d'affaires était d'environ 69 milliards d'euros en 2018.

Cette entreprise est le premier producteur et fournisseur d'électricité en France et en Europe. La société était la première au niveau mondial, en ce qui concerne la puissance installée, avant la fusion des deux principaux producteurs chinois en 2017.

Le groupe EDF détient différentes filiales. Les principales sont :

- EDF SA, Société Anonyme*, qui se charge de l'aspect production de l'électricité principalement à l'aide des centrales nucléaires, mais aussi des centrales hydrauliques et thermiques, de l'éolien, du solaire et des bioénergies. C'est dans ce groupe que j'effectue mon stage.

- RTE, Réseau de Transport de l'Electricité, qui exploite, maintient et développe le réseau de transport électrique français. Elle achemine l'électricité haute tension sur le réseau public français.

- ENEDIS, anciennement ERDF, Electricité Réseau Distribution France, est chargée de l'aménagement et de la gestion du réseau de distribution d'électricité français.

- Dalkia, qui développe et gère des solutions énergétiques plus écologiques et plus économiques pour ses clients. Cela inclus des prestations de services dans le domaine de l'énergie. Elle possède aussi des filiales comme par exemple Dalkia Wastenergy qui utilise la combustion des déchets ménagers pour produire de l'électricité et de la vapeur, mais aussi Dalkia Biogaz, spécialisée dans les activités de production, traitement et valorisation du biogaz.

- EDF Renouvelables, qui assure le financement, le développement et la construction de toutes sortes d'installations renouvelables comme des éoliennes, des panneaux solaires et un système de stockage de l'énergie. Cette filiale est particulièrement impliquée dans le processus de transition énergétique (diminution de la part du nucléaire voulu par l'Europe).

- Framatome, qui conçoit des composants, du combustible, des systèmes de contrôle-commande et offre des services destinés aux réacteurs nucléaires afin de préserver des niveaux de sûreté et de performances élevés**.**

1.1 Historique de EDF

La société EDF a été créée le 8 avril 1946 et a toujours eu pour but de produire, de transporter et de distribuer l'électricité en France.

Dès le lendemain de la Seconde Guerre Mondiale, l'enjeux était de fournir suffisamment d'électricité à tous les foyers français. Dans les années 1960, les appareils électriques se popularisent et la demande énergétique augmente. De ce fait, en 1963, on assiste à la mise en service de la première centrale nucléaire en France qui se situe à Chinon.

A cause du choc pétrolier en 1974, la production d'électricité nécessitant beaucoup d'hydrocarbures, la France prend une décision, celle de privilégier le nucléaire pour garantir son indépendance énergétique.

Aujourd'hui, le nucléaire représente encore 73% de la production d'électricité en France, mais devrait atteindre 50% d'ici 2035.

A partir de 1984, EDF décide d'exporter son savoir-faire en terme de nucléaire à l'international. Le premier pays accueillant une centrale nucléaire en partenariat avec EDF fut la Chine, avec la construction de la centrale de Daya-Bay.

Suite à une directive européenne de juin 2003, Électricité de France change de statut et devient une société anonyme à capitaux publics le 19 novembre 2004. Elle fait son entrée en Bourse le 21 novembre 2005.

Aujourd'hui, EDF est le premier producteur et fournisseur d'électricité en France et en Europe. Depuis 2017, EDF n'est plus le premier mondial. En effet, EDF s'est fait détrôner par l'union de la compagnie chinoise Guodian Group et Houiller Shenhua, ces deux entreprises voulaient créer le premier fournisseur d'électricité du monde.

1.2 Ma localisation au sein d'EDF

1.2.1 Organisation dans EDF SA

EDF SA est une très grande entreprise qui compte énormément de branches différentes (Figure 1).

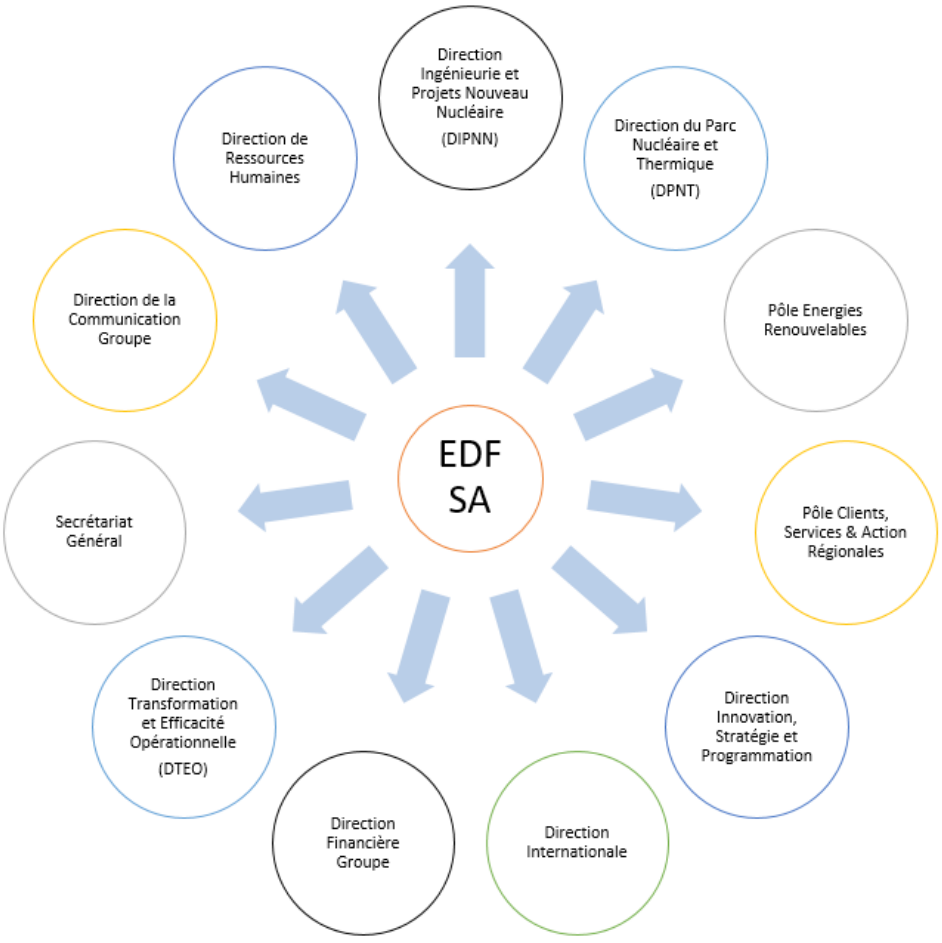


Figure 1 : Organigramme représentant les branches dans EDF SA.

Pour commencer, je me situe dans la DTEO, Direction de la Transformation et Efficacité Opérationnelle (Figure 2), qui regroupe tous les services de support.

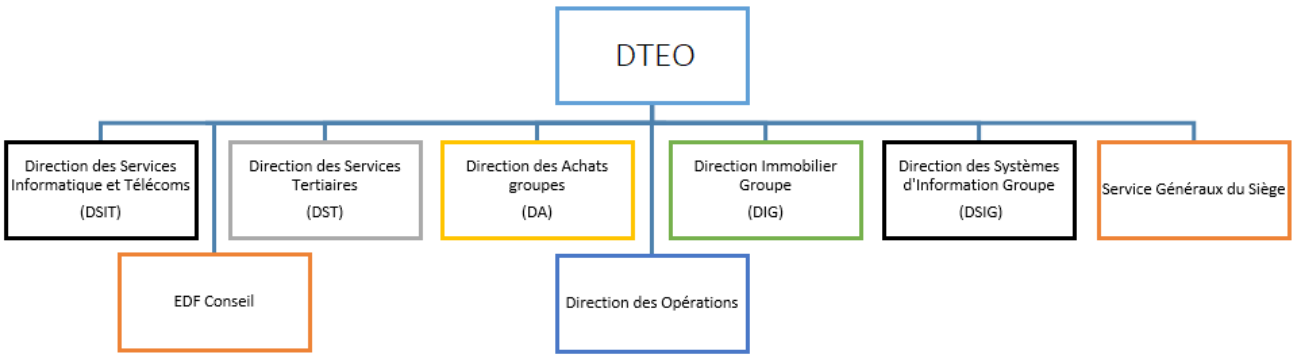
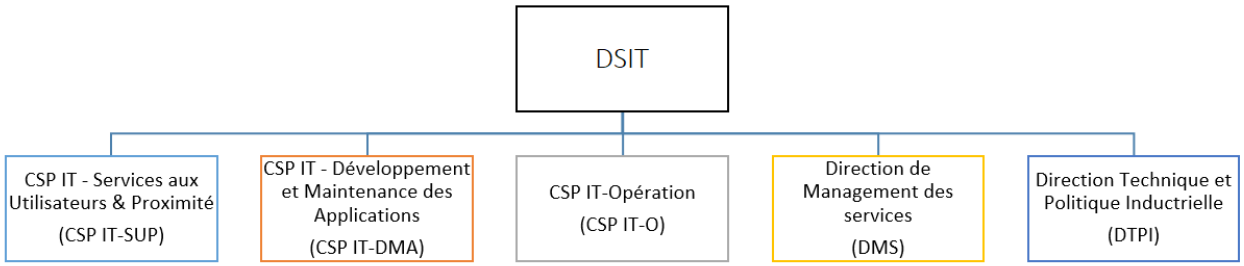


Figure 2 : Organigramme de la DTEO.

Ensuite, l'organisme dans lequel je suis est la DSIT, Direction des Services Informatiques et Télécoms (Figure 3). Ce service s'occupe de la gestion des infrastructures, du datacenter jusqu'au poste de travail, elle s'occupe aussi du développement, de la maintenance et l'exploitation des Systèmes d'Information Métiers*, et fait de l'expertise (sécurité, architecture, logiciels, …).



« CSP IT » signifie « Centre des Services Partagés Informatique et Télécoms »

Figure 3 : Organigramme de la DSIT.

Dans la DSIT se trouve la CSP IT-SUP, CSP IT-Services Utilisateurs et Proximité (Figure 4), qui est responsable du bon fonctionnement et de l'évolutivité de l'environnement de travail IT, Informatique Télécoms. Il délivre notamment des outils collaboratifs (comme par exemple Lync*, que tout le monde utilise au sein de l'entreprise) et des services de messagerie, de terminaux bureautiques et de télécommunication.

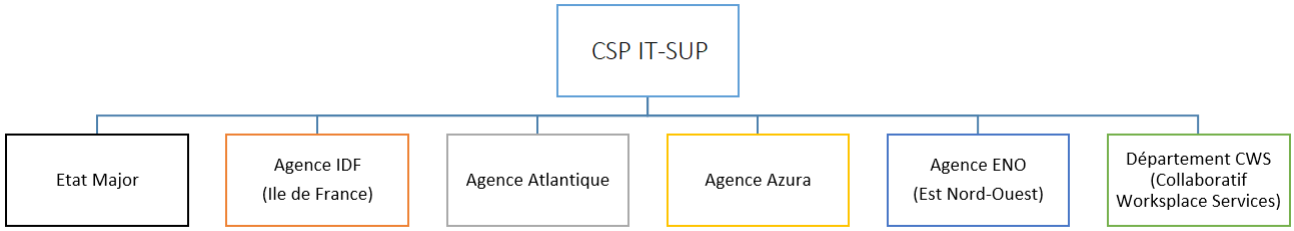


Figure 4 : Organigramme de la CSP IT-SUP.

A l'intérieur de la CSP IT-SUP, plusieurs agences sont présentes en fonction des régions géographiques. On est affecté à l'agence AZURA (Figure 5). Elle délivre des servies bureautiques aux utilisateurs des régions Auvergne-Rhône Alpes, Provence-Alpes-Côte d'Azur et Languedoc Roussillon. Elle permet une modernisation des postes de travail informatique, elle est aussi en charge du déploiement des projets informatiques et télécoms sur son périmètre géographique et du pilotage de certains projets nationaux qui lui sont confiés.

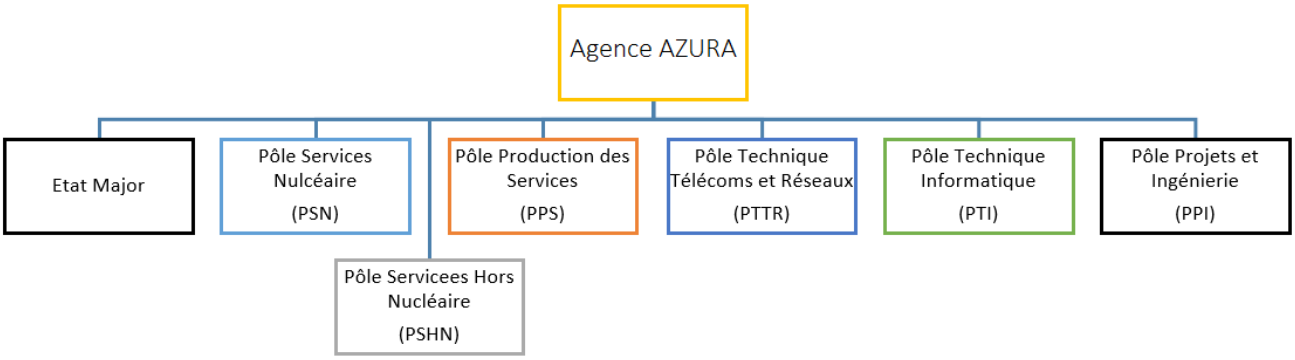


Figure 5 : Organigramme de l'agence AZURA.

L'agence AZURA centralise plusieurs pôles, dont le PTTR qui fait de l'expertise et de l'appui technique dans les télécoms et les réseaux. La cellule dans lequel je suis en stage est la CEC qui est orientée télécoms.

1.2.2 Présentation de la CEC.

Le rôle de la CEC dans EDF est de fournir son savoir-faire en ce qui concerne les télécoms, aux différentes chaînes de service de la DSIT. Ces chaînes de services sont :

- La CS TAC, Chaîne de Service Téléphonie Accueil Commerce.
- La CS TTA, Chaîne de Service Téléphonie Tertiaire Administrative.
- La CS TTI, Chaîne de Service Téléphonie Industriels.

Cela implique la gestion des incidents télécoms qui pourraient survenir de temps en temps, mais aussi contribuer aux demandes de services télécoms comme par exemple l'ajout ou le retrait d'un ou plusieurs postes téléphoniques.

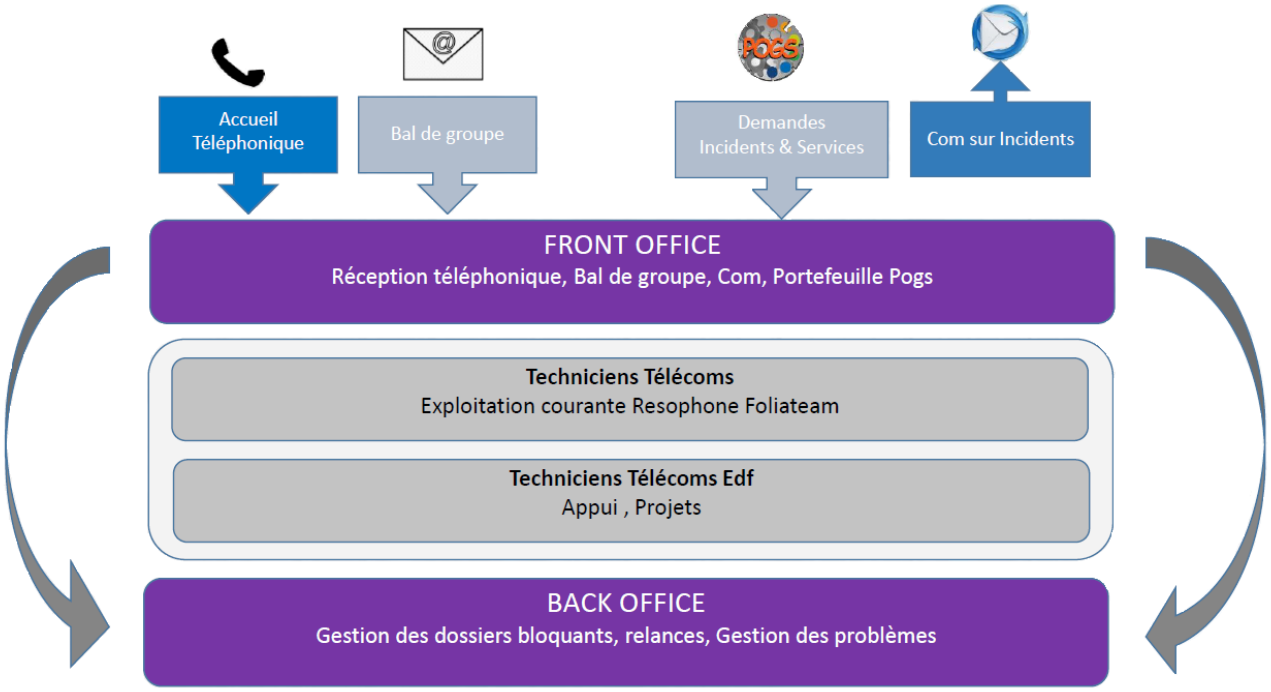


Figure 6 : Schéma expliquant le fonctionnement général de la CEC.

La CEC est divisée en deux groupes complémentaires qui sont le Front Office et le Back Office.

Le Front Office s'occupe de recevoir les appels téléphoniques que la CEC reçoit. Ce n'est pas une hotline classique, les appels que le Front Office reçoit proviennent soit des opérateurs télécoms nationaux comme SFR et Orange, soit des internes d'EDF comme la MOA, Maitrise d'Ouvrage*, ou alors des interlocuteurs désignés, des prestataires par exemple.

Le Front Office gère aussi les demandes POGS, Pilotage Opérationnel de la Gestion des Services*, c'est-à-dire qu'il s'occupe de la gestion des demandes de services, d'incidents ou des demandes de changement (RFC, Request For Change*). Il repartit ces POGS au Back Office qui sont les techniciens et experts.

Le Front Office communique aussi en temps réel sur l'état de service des infrastructures exploitées par l'équipe.

Le Back Office quant à lui, est composé de techniciens télécoms EDF qui font de l'expertise et de l'appui aux projets télécoms régionaux et nationaux.

L'un des projets sur lequel travaillent les techniciens EDF est ISYCOM pour Interconnexion des SYstèmes de COMmunication. Ce projet a pour but d'anticiper l'obsolescence des liaisons opérateurs utilisées par de nombreux systèmes (principalement par les services téléphoniques, Lync, les services multimédia…).

Pour ce faire, il faut remplacer les accès primaires, appelé T2*, qui permettent de quinze à trente communications téléphoniques simultanées, par des accès Trunk SIP. Le « SIP » de l'anglais Session Initiation Protocol, est un standard basé sur l'IP qui permet de transporter des flux de multimédia (Voix, Vidéo, Data) sur les réseaux IP locaux (RIN) et sur Internet. Un de ses avantages est que tous les sites reliés au réseau EDF peuvent communiquer ensemble sans passer par un réseau extérieur.

Des partenaires EDF sont également présents à la CEC et sont dans le Back Office, ce sont aussi des techniciens télécoms, mais appartenant à la société Resophone-Foliateam. Ces techniciens s'occupent principalement des niveaux 1 et 2 de gravité qui correspondent à la création, la suppression et le dépannage des postes.

Les deux autres niveaux, les 3 et 4, équivalent à l'expertise et à l'appui des projets auxquels participent les techniciens EDF.

On peut se référer à la Figure 6 au-dessus, qui résume le fonctionnement de la CEC.

2 Ma mission principale

Au cours de ces dix semaines de stage, j'ai eu l'opportunité de découvrir le métier de technicien télécoms chez EDF. J'ai pu découvrir l'environnement de travail et comprendre de façon générale les difficultés que l'on pouvait rencontrer dans la gestion des incidents et la contribution aux demandes de services télécoms.

La mission principale qui m'a été confiée avait pour but d'avertir l'équipe de techniciens EDF lorsqu'une surcharge du réseau sur un des PA RIN d'un site EDF surviendrait.

2.1 Présentation du logiciel OmniPeek

Afin de répondre à la mission, j'ai eu à ma disposition le logiciel « OmniPeek », qui est un sniffer de réseau conçu par la société Savvius. Un sniffer de réseau est un outil informatique utilisé pour analyser et contrôler sur un segment le trafic du réseau. Il permet aux administrateurs et aux ingénieurs réseau de diagnostiquer et de détecter rapidement les causes des incidents et autres problèmes sur le réseau.

OmniPeek utilise pour cela des sondes réseau (Figure 7), aussi conçues par Savvius, qui capturent le trafic en temps réel d'une ou plusieurs interfaces réseau. Les sondes sont installées sur des sites d'EDF distants et le Datacenter principal.

Figure 7 : Photo d'une sonde Savvius.

La sonde est reliée à un TAP réseau qui permet de rediriger le trafic vers la sonde sans perturber le réseau.

Depuis OmniPeek, on peut voir que quatorze sondes sont positionnées sur des sites EDF un peu partout en France et que deux autres sondes sont positionnées dans le Datacenter qui gère toutes les données concernant la voix qui arrivent de l'opérateur téléphonique.

Ma mission concerne une surcharge du réseau dans son intégralité et non pas une surcharge uniquement de la voix. Les sondes placées dans le Datacenter ne capturant que les données voix, mon travail ne va affecter que les sondes installées sur les sites.

Les sondes sont listées dans l'onglet « Capture Engines » dès lors qu'on lance OmniPeek (voir Annexe 1). Si l'on clique sur l'une des sondes, on pourra s'y connecter avec un identifiant et mot de passe. Une fois connecté à la sonde voulue, on peut y retrouver tout un tas d'informations comme le nom de la sonde, son adresse IP, le système d'exploitation, le nombre de captures présentes sur la sonde, etc… (voir Annexe 2)

Maintenant, pour observer ce que la sonde capture, il faut cliquer sur l'onglet « Captures » (que l'on peut voir sur l'Annexe 2) et sélectionner la capture désirée.

Une fois la capture sélectionnée, on a accès à toutes les données que l'on souhaite (Figure 8). Sur la gauche, se trouvent plusieurs onglets qui classent les différentes données acquises par la sonde pour que l'on puisse sélectionner précisément ce que l'on veut analyser.

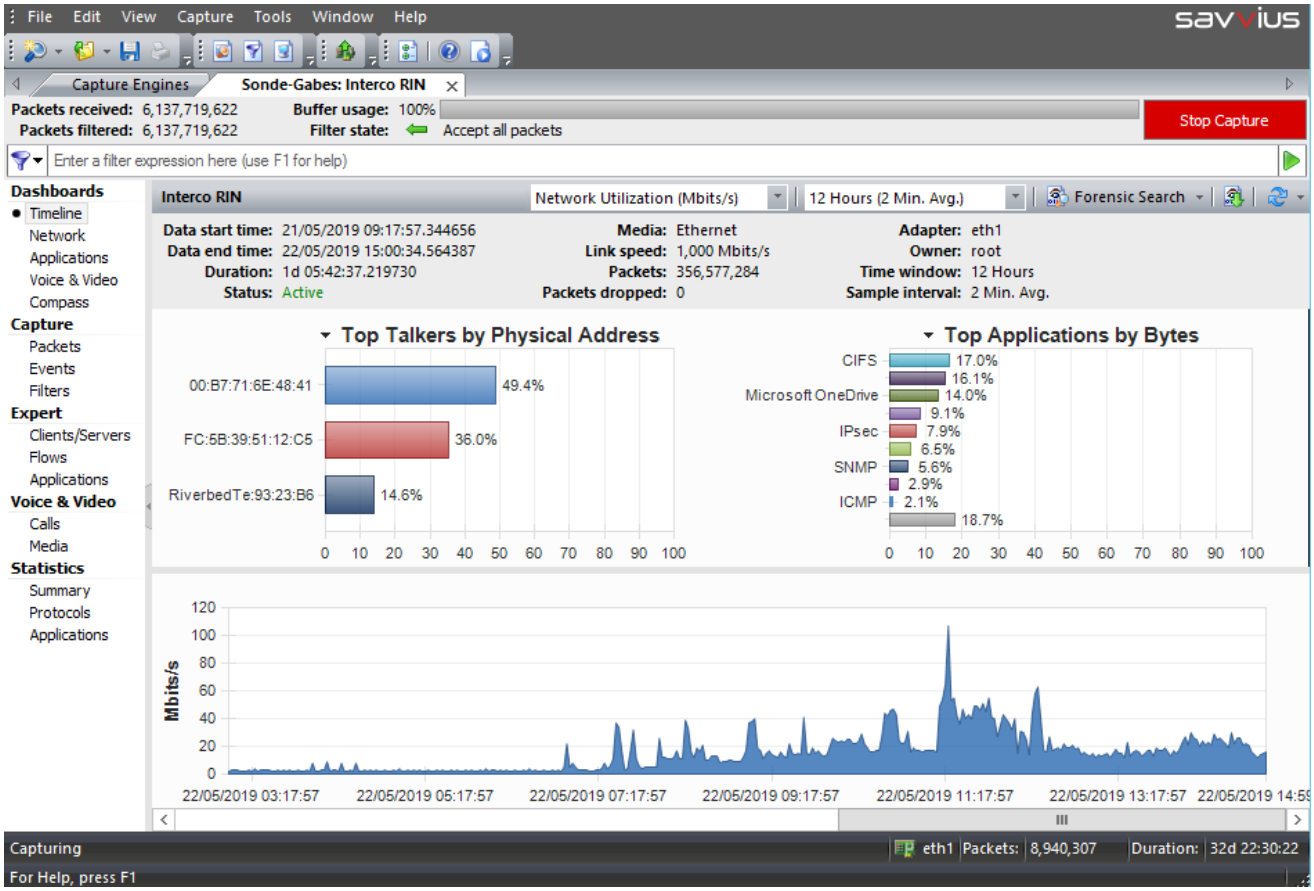


Figure 8 : Onglet de capture recueillant toutes les données capturées.

Par exemple, sur la Figure 8, un des graphiques que l'on peut observer, nous montre l'utilisation de la bande passante utilisée par le réseau (en Mbits/s) en fonction du temps.

Bien évidemment, le logiciel OmniPeek ne se résume pas qu'à ce que je viens de présenter. Le spectre des possibilités est beaucoup plus large, une documentation de plus de six cents pages existe sur internet, on peut la retrouver dans la bibliographie de ce rapport.

2.2 Mise en place des alarmes sur les sondes

Ma problématique était de trouver une solution permettant d'alerter l'équipe de techniciens EDF lorsqu'une surcharge du réseau sur un des PA RIN d'un site EDF survenait. Cette surcharge est traduite par une utilisation prolongée de plus 80% de la bande passante disponible sur un site.

J'ai alors fait des recherches, que ce soit sur OmniPeek directement, sur Internet ou sur l'intranet de EDF, pour essayer de trouver une solution à cette problématique. Après quelques heures de recherche et de familiarisation avec le logiciel, j'ai donc trouvé la possibilité de mettre des alarmes sur les captures qu'effectuent les sondes.

2.2.1 Configuration des alarmes

OmniPeek est un outil de diagnostic réseau. On peut y retrouver des alarmes prédéfinies qui permettent de notifier en temps réel si une anomalie concernant le réseau est présente, mais elles ne sont pas appliquées par défaut. On peut retrouver la liste de toutes les alarmes présentes sur une sonde dans l'onglet « Settings » puis « Alarms » (voir Annexe 3). Le logiciel nous permet aussi de créer nos propres alarmes si celles prédéfinies ne nous conviennent pas.

Une alarme surveille forcement une statistique relative à la capture. En effet, la sonde capture le trafic qui passe en entrée et sortie du réseau. Elle en ressort des statistiques concernant le réseau, la voix, des éventuelles erreurs et des information générales sur la capture (voir Annexe 4).
Dans le cas de ma problématique, l'alarme va devoir surveiller la donnée « Current Utilization (bits/s) », qui donne la valeur de la bande passante utilisée en temps réel par le réseau.

N'ayant pas trouvé d'alarme dans la liste des alarmes prédéfinies faisant ce que je voulais, c'est-à-dire envoyer une alerte lorsque 80% de la bande passante disponible sur le réseau était utilisée pendant plus d'une minute, j'ai dû me lancer dans la création d'une alarme qui répondait à cette demande. Mais avant de créer l'alarme, il me fallait connaitre la bande passante disponible pour chaque site pour pouvoir ensuite calculer 80% de cette valeur.

Pour connaitre la bande passante maximale disponible, j'ai utilisé le logiciel EDF Guepar NG qui recense tous les sites EDF en France avec tout un tas d'informations sur les sites en question. Malheureusement les sites sont répertoriés en fonction de leur référence RIN* et non leur nom, par exemple la référence RIN du site de Marseille Gabès est « 13MARS011AOG », ce qui rend la recherche des informations plus difficile.

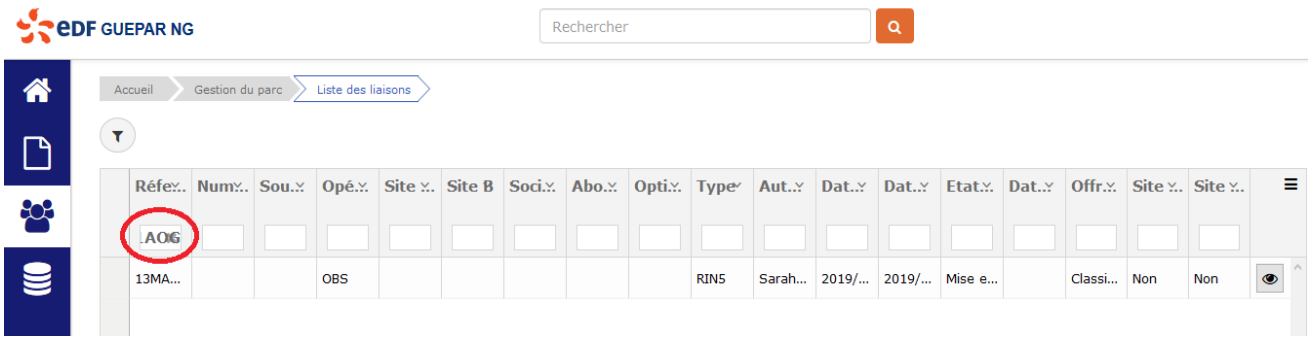


Figure 9 : Recherche du site de Marseille Gabès sur Guepar NG.

On rentre la référence RIN du site dont on recherche la bande passante dans la zone de texte que j'ai entouré en rouge sur la Figure 9 et le logiciel en ressort le site qui correspond. Il faudra juste cliquer sur l'œil à droite pour avoir le détail des informations sur le site, dont la bande passante maximale disponible.

Mais, afin de rendre les recherches de bande passante plus faciles, j'ai eu accès au logiciel WhatsUp Gold, un logiciel de surveillance réseau qui offre une visibilité complète sur l'état des périphériques réseau, des systèmes et des applications, qui m'a permis de retrouver les références RIN des sites en fonction de leurs noms.

Le logiciel se présente de la façon suivante :

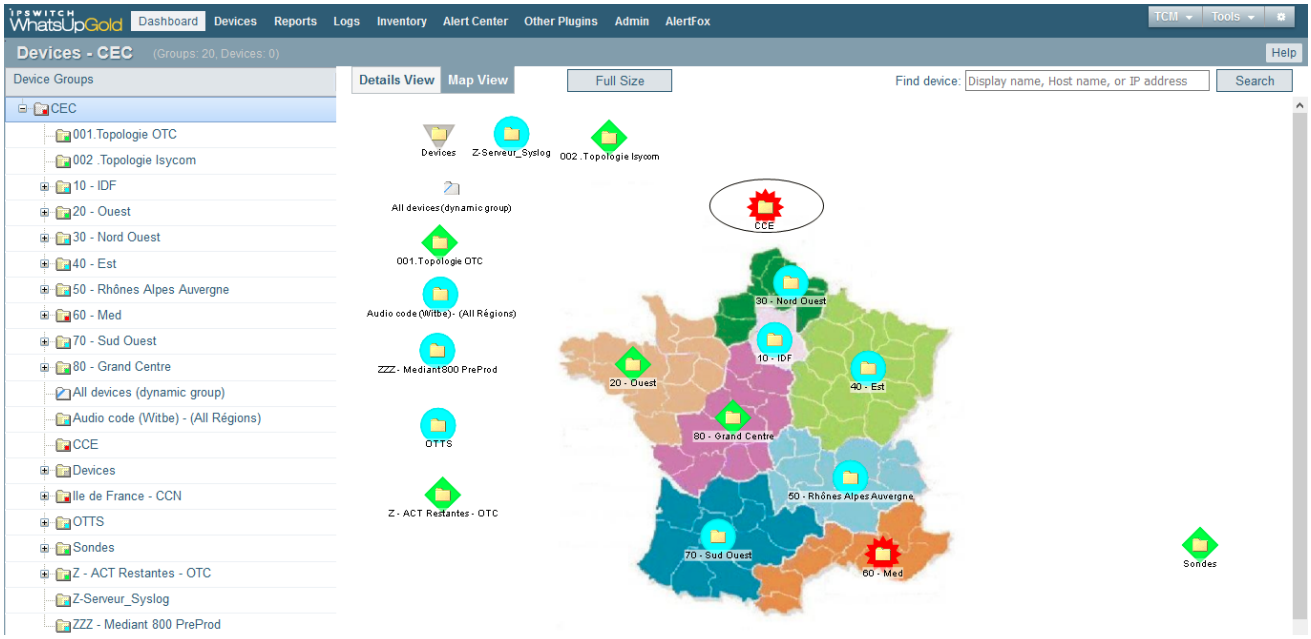


Figure 10 : Page d'accueil de WhatsUp Gold.

On peut voir sur la Figure 10 une carte de France qui classe les sites en fonction des régions géographiques. On recherche alors le site que l'on veut dans les dossiers sur la gauche ou alors directement sur la carte et de ce fait, on clique sur le site en question et on a accès à sa référence RIN.

Connaissant les références RIN des sites dont je m'occupe, j'ai pu retourner sur Guepar NG pour rechercher leur valeur des bandes passantes comme je l'ai fait plus haut avec Marseille Gabès.

Pour plus de clarté, j'ai créé un tableau (voir Annexe 5) qui rassemble les différents sites, leurs bandes passantes maximales respectives ainsi que 80% de cette bande passante. Ce qui va m'être utile lors de la création des alarmes.

J'ai écrit dans la partie de présentation d'OmniPeek qu'il y avait quatorze sondes présentes, mais je n'ai énoncé que treize sites dans le tableau car il y a en réalité 2 sondes sur le site de Toulon. La première capture le réseau comme le font les autres sur les autres sites, mais la seconde quant à elle ne capture que le trafic provenant d'un ordinateur qui rencontre beaucoup de problèmes liés à la voix. Je n'ai donc pas pris en compte cette seconde sonde à la demande de mon tuteur.

Une fois toutes les données recueillies, je pouvais commencer la création des treize alarmes. Le travail était assez répétitif, je vais donc expliquer comment j'ai procédé sur la sonde de Marseille Gabès, le site où se déroule mon stage. La seule différence entre les alarmes va être la valeur de la bande passante à ne pas dépasser, elle varie de 16 Mbits/s à 80 Mbits/s selon les sites (voir Annexe 5).

Exemple de configuration de l'alarme sur le site de Marseille Gabès :

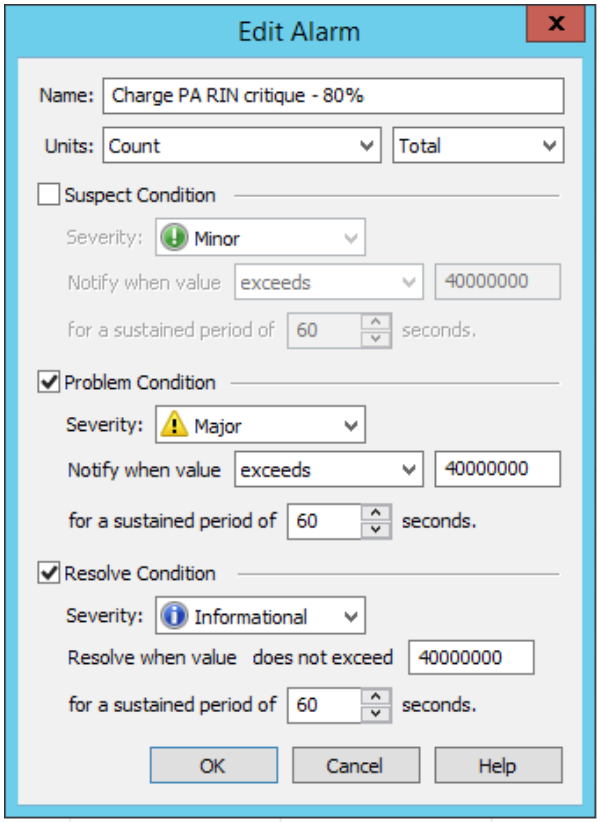


Figure 11 : Interface de création de l'alarme (exemple sur Marseille Gabès).

Comme on peut le voir sur la Figure 11, il a un certain nombre de champs à remplir. Les premiers champs concernent le nom de l'alarme et des informations sur l'unité de mesure. Ces informations doivent correspondre avec l'unité de mesure de la statistique que l'alarme surveille. Le nom a été choisi arbitrairement pour expliquer au mieux ce que l'alarme fait. Ensuite, il y a trois zones sensiblement similaires, « Suspect Condition », « Problem Condition » et « Resolve Condition ».

- La case « Suspect Conditon », si elle est cochée, alertera d'une condition suspecte.
  J'ai fait le choix de ne pas la cocher car on a jugé inutile de recevoir une alarme pour une condition suspecte. Cette partie se remplit de la même façon que la partie « Problem Condition » expliquée ci-dessous.

- La case « Problem Condition », si elle est cochée, alertera d'une condition problématique pour le paramètre de statistique choisi, ici « Current Utilization (bits/s) »
  Dans cette application, on lui affecte un état de gravité majeure (« Severity : Major »). La partie « Notify when value » nous donne le choix de sélectionner « exceeds » ou « does not exceeds », ce qui signifie respectivement « dépasse » et « ne dépasse pas », et nous demande aussi de rentrer une valeur. Je choisis alors « exceeds » et 40 000 000 bits/s. Pour terminer, je dois rentrer un nombre de seconde pour lesquelles la condition de dépasser 40 Mbits/s doit être valide. En définitive, on recevra une alerte lorsque la bande passante utilisée dépasse 40 Mbits/s pendant 60 secondes.

- La case « Resolve Condition », si elle est cochée, alertera lorsqu'une condition suspecte ou problématique sera résolue. On lui affecte un état de gravité informationnelle (« Severity : Informational »). Cette partie se configure de la même manière que les deux précédentes à la seule différence que cette condition se déclenchera quand on passe en dessous de 40 Mbits/s.

Une fois avoir cliqué « OK », il faut retourner dans l'onglet « Alarms » (voir Annexe 3) et rafraichir la page pour voir l'alarme que l'on vient de configurer.

Je n'avais plus qu'à créer les douze autres alarmes sur les autres sondes tout en changeant à chaque fois la valeur de la bande passante en fonction du site.

Les alarmes ainsi créées ne pouvaient pas encore alerter. En effet, pour que notre alarme soit fonctionnelle, il faut dans un premier temps stopper la capture en cours, puis aller dans les options de capture et cocher l'alarme en question (voir Annexe 6). Finalement on peut relancer la capture. Cette manipulation doit se faire pour les treize sondes et de préférence à des heures où l'activité des appels est faible, donc tôt le matin ou alors tard le soir, pour ne pas stopper la capture et ne pas manquer de capturer des appels importants ; à l'exception de la sonde de Marseille Gabès, qui fonctionne comme les autres, mais qui est une maquette qui permet de faire toutes sortes de tests.

Les alarmes étant désormais fonctionnelles, on recevait les alertes dans l'onglet « Events » sur OmniPeek (voir Annexe 7). Cet onglet est conçu pour répertorier tous les évènements se passant sur la sonde quelle que soit la gravité, comme par exemple une alarme qui s'active. La plupart du temps, les évènements sont à titre informationnel. Comme on peut le voir sur l'annexe 7, plus de 14 000 évènements sont informationnels contre seulement 4 évènements qui sont de gravité majeure.

Cet onglet est pratique pour constater ce qu'il se passe sur une sonde, notamment dans notre cas pour savoir si une alarme s'est activé ou non, mais il faut être connecté sur OmniPeek pour y avoir accès or les techniciens EDF ne sont pas tout le temps sur le logiciel pour surveiller si un site subit une surcharge ou non.

Il fallait que je trouve un autre moyen plus efficace de les alerter en temps réel sans qu'ils soient constamment sur OmniPeek.

2.2.2 Configuration des actions

Après quelques recherches, j'ai trouvé le moyen d'envoyer par mail les alertes que les alarmes créent. Les mails sont en effet une solution très avantageuse car les techniciens EDF ont toujours leur boite mail ouverte et reçoivent déjà des alertes d'autres logiciels par mail. De plus, Outlook envoie des notifications depuis le centre de notifications de Windows 10 à chaque fois que l'on reçoit un mail.

La solution était la mise en place d'actions sur OmniPeek. Elles permettent de s'informer de ce qu'il se passe sur la sonde autrement que depuis OmniPeek. Pour avertir, les actions envoient des notifications en fonction d'une source que l'on choisit et de la gravité « l'Event » engendrée par la source.

Les types d'actions disponibles sont :

- L'envoi de mails.
- L'envoie de la notification dans un fichier log.
- L'exécution d'un programme.
- L'écriture de la notification dans un fichier texte
- L'envoi de messages Syslog.
- L'envoi de la notification sous forme de messages SNMP Trap.

Il y a donc six types d'actions différentes qui ont toutes leur utilité mais pour la création des actions et surtout parce qu'on doit alerter simplement et en temps réel, je me suis focalisé sur les mails.

Les sources disponibles sont :

- La sonde.
- La capture.
- Les recherches Forensic.
- Les alarmes.
- Les fonctions d'analyse expert.
- Le module d'analyse FPT.
- Le module d'analyse Web.

On peut donc recevoir des notifications de 7 sources différentes et contrairement au type d'action, on peut sélectionner plusieurs sources pour une action. Dans notre cas, on ne sélectionnera que les alarmes.

La configuration de l'action est simple, on va tout d'abord créer une nouvelle action en se rendant dans l'onglet « Settings » puis « Notifications » et en cliquant sur le bouton « Insert » (voir Annexe 8).

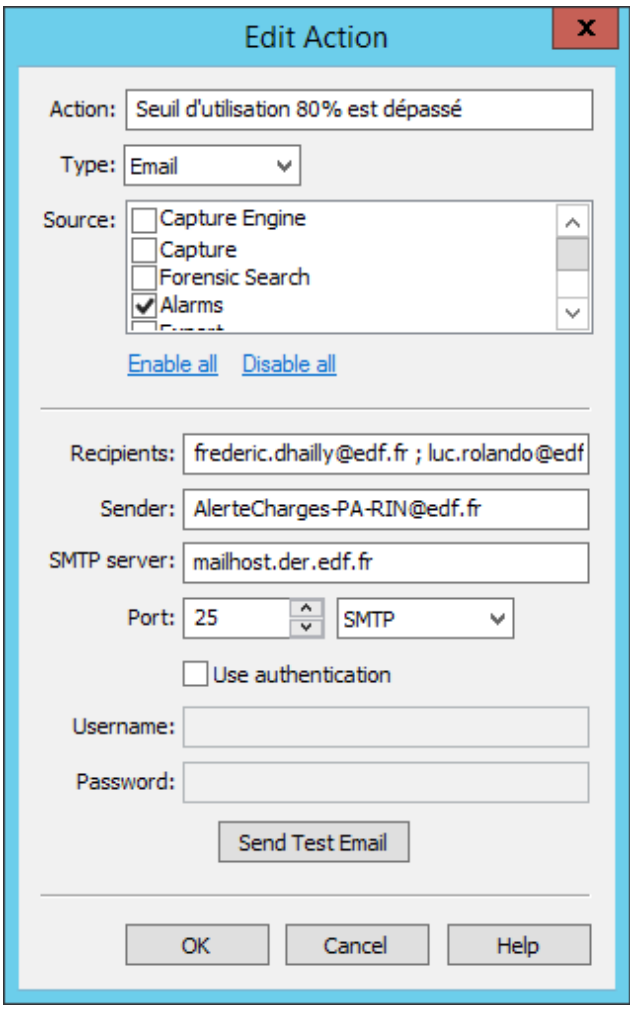


Figure 12 : Interface de création de notre action.

Une fois notre fenêtre de création ouverte (Figure 12), on peut nommer l'action, lui attribuer un type. Dans ce cas, pour mettre en place l'envoi de mail, on choisit alors « Email » puis une ou plusieurs sources et on choisit « Alarms » pour recevoir uniquement des mails d'alerte.

Maintenant il faut configurer l'envoi des mails.

- En premier temps, on rentre tous les destinataires des alarmes, séparés par un point-virgule.
- Dans un deuxième temps, on choisit l'adresse mail de l'envoyeur de façon à identifier rapidement les mails d'alarmes et les mail classiques (l'adresse est factice, on ne peut pas lui répondre).
- Dans un troisième temps, j'ai dû demander l'adresse du serveur SMTP, Simple Mail Transfer Protocol*, de EDF pour permettre l'envoi des mails.
- Finalement choisir le protocole SMTP et le port 25 qui est utilisé par ce dernier.

Notre action étant configurée (Figure 12), on doit maintenant cocher les cases qui correspondent à la gravité des conditions de l'alarme pour que l'action soit fonctionnelle. Seulement deux conditions ont été sélectionnées lors de la création des alarmes, la première étant de gravité majeure (qui correspond au pictogramme jaune) et la seconde de gravité informationnelle (qui correspond au pictogramme bleu). Il va donc falloir cocher les deux cases devant l'action comme suivant l'annexe 8.

La configuration des actions est la même pour toutes les sondes, j'ai dû répéter ce travail pour les treize sondes.

Tout étant fonctionnel, voici à quoi ressemble un mail d'alerte (Figure 13) :

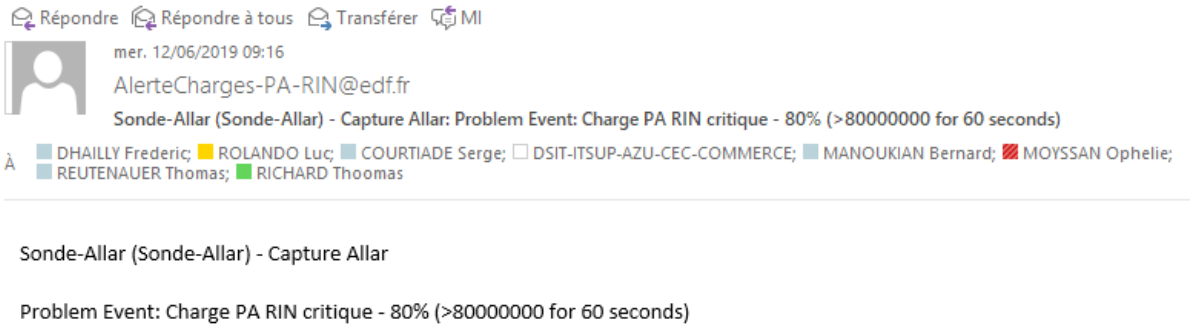


Figure 13 : Mail d'alerte d'une surcharge sur le site d'Allar.

Le mail est en deux partie, la première qui indique la sonde et donc le site concerné et la deuxième partie qui indique « Problem Event : Charge PA RIN critique – 80% » qui signifie que la condition problématique de l'alarme s'est activée.

On reçoit aussi un mail de résolution (Figure 14) :

Figure 14 : Mail de résolution de l'alerte du site d'Allar.

La différence avec le mail précédant est « Resolve Event : Charge PA RIN critique – 80% » qui signifie que la condition de résolution de l'alarme s'est activée.

2.2.3 Problèmes rencontrés et solutions

Suite à la première journée passer à recevoir des alarmes, on s'est aperçu que les sites atteignaient trop souvent le seuil qu'on avait choisi car on recevait des mails d'alarmes toutes les cinq minutes environ, ce qui rend la boite mail surchargée elle aussi.

En allant vérifier sur OmniPeek on s'est aussi aperçu, grâce aux captures des sondes, que certains sites dépassaient même 100% de la bande passante théoriquement disponible. J'ai demandé à un ingénieur réseaux s'il pouvait m'expliquer comment est-ce cela était possible. La réponse était en fait que certains sites EDF avaient Orange comme opérateur télécoms, d'autres sites avaient SFR et que le but était à terme de passer tous les sites chez Orange pour différentes raisons. Le problème en fin de compte était qu'Orange fournit à chacun des sites EDF une valeur de bande passante garantie mais rien n'empêche de dépasser cette valeur.

La valeur de la bande passante, pour les sites de chez Orange, que j'ai relevé sur Guepar NG était en réalité la valeur que l'opérateur garantie et non pas la valeur maximale disponible.

Je ne pouvais pas laisser les alarmes en l'état, on a donc décidé de modifier leur configuration pour être averti lorsque la valeur garantie par Orange était atteinte pendant une durée prolongée de 5 minutes.

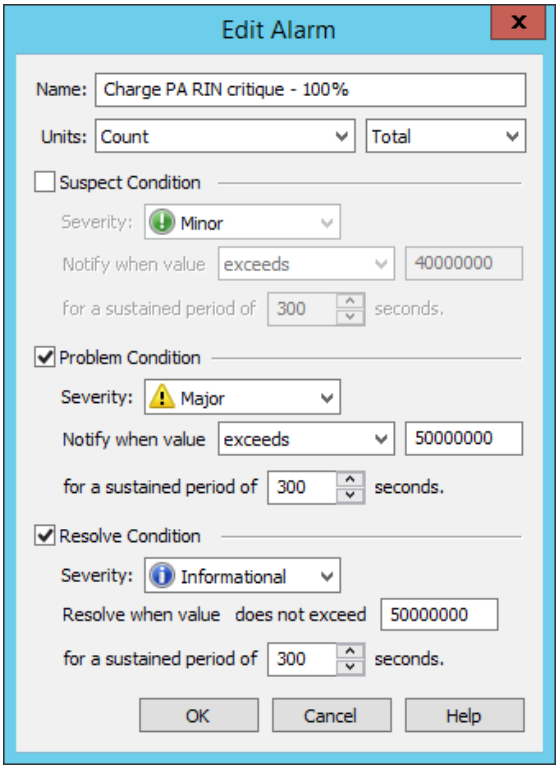


Figure15 : Nouvelle configuration des alarmes (exemple sur Marseille Gabès).

Sur l'alarme de Marseille Gabès, j'ai changé 40 000 000 bits/s (40 Mbits/s) par 50 000 000 (50 Mbits/s) pour correspondre à la valeur lue sur Guepar NG et j'ai changé 60 secondes par 300 secondes pour obtenir le délai de 5 minutes (Figure 15).

J'ai bien sûr fait les modifications sur toutes les sondes en changeant les valeurs en fonction de leur bande passante respective.

Suite à ces modifications, on ne recevait plus autant de mails d'alarmes, ce qui permet de passer en revue toutes les alertes quand elles se déclenchaient.

La mission terminée, j'ai rendu un document expliquant en détail comment est-ce que j'ai configurer les alarmes pour que les techniciens EDF puissent les modifier ou en créer de nouvelles si besoin.

3 Les missions secondaires

3.1 Surveillance du MOS

La semaine du Lundi 20 Mai, une mission de surveillance du MOS en temps réel, sur le site EDF localisé à Tours, m'a été confiée. En effet, tous les téléphones des agents travaillant là-bas utilisaient la téléphonie sur IP, mais un des objectifs chez EDF est de migrer tous les téléphones fixes vers de la softphonie. Un softphone est un logiciel pour faire de la téléphonie par internet depuis un ordinateur. A la CEC, les techniciens EDF utilisent le logiciel Lync (ou Skype entreprise) comme logiciel de softphonie. Cela permet de passer des appels téléphoniques d'ordinateur à ordinateur ou, d'ordinateur à téléphone qu'il soit fixe ou mobile. La softphonie offre plusieurs autres fonctionnalités comme la visioconférence, une messagerie instantanée, le transfert d'appels et de fichiers ou une synchronisation avec sa boîte mail, pour par exemple, créer ou rejoindre une réunion depuis le logiciel.

Cette migration est délicate car le moindre problème peut engendrer une chute significative du MOS pour pas mal de communications téléphoniques sur le site. Cette chute du MOS est traduite par une baisse de qualité de la voix, c'est-à-dire des grésillements, une communication hachurée, etc…

Si la baisse de la qualité voix devient trop importante et est causée par EDF, la migration doit se mettre en pause pour essayer de résoudre le problème. Alors que, si le problème de qualité de la voix était causé par l'opérateur télécoms SFR, dans ce cas précis on ne pouvait rien y faire, ce n'était donc pas la peine d'avertir les techniciens sur Tours pour mettre en pause la migration.

Ma mission était alors de surveiller l'évolution du MOS sur le site de Tours à travers le logiciel OmniPeek et d'avertir les personnes concernées en fonction de ce qu'il se passait.

Pour cela, depuis OmniPeek, je devais me connecter à la sonde de Tours puis aller dans l'onglet « Forensics » et sélectionner « Call Quality » dans le menu déroulant en haut de la page pour pouvoir observer l'évolution du MOS en temps réel (voir Annexe 9).

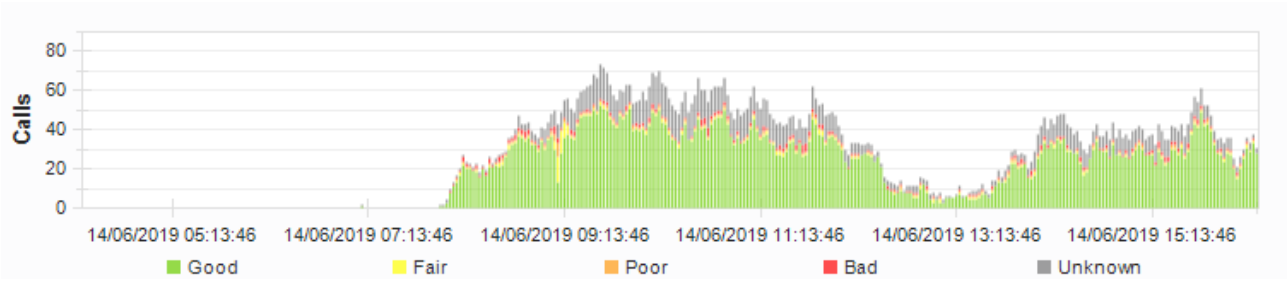


Figure 16 : Graphique représentant le nombre d'appel passé en fonction du temps et du MOS.

Le graphique de la figure 16 évolue en temps réel sur OmniPeek et peut être zoomé jusqu'à avoir un intervalle de temps de 5 minutes, dans cet exemple le graphique recouvre quasiment une journée pour avoir une vue d'ensemble.

La couleur correspond au MOS : vert étant une bonne qualité d'appel et rouge étant une mauvaise qualité (Figure 17).

Figure 17 : Conrrespondance entre la couleur sur le graphique et la réelle valeur du MOS.

Lorsque je détectais une anomalie sur le graphique, je devais dans un premier temps, prendre une capture d'écran du graphique présentant le problème et ensuite effectuer une « recherche forensic » permettant de rechercher toutes sortes de données que la capture enregistre pour identifier si le problème provient d'EDF ou de SFR.

Pour ce faire, il suffisait de sélectionner la partie du graphique contenant le problème et cliquer sur le bouton « Forensic Search » pour lancer la recherche (voir Annexe 10).

Sur l'annexe 10 on peut aussi observer à quoi ressemble le graphique du MOS quand un problème de qualité voix survient.

Une fois la recherche terminée, on trie les données en ne gardant que les communications téléphoniques. On obtient alors un tableau regroupant tous les appels passés pendant la durée du problème. On trie tous ces appels en fonction de leur MOS pour se focaliser uniquement sur les appels dont la qualité est mauvaise. Je devais aussi prendre une capture d'écran de chaque tableau de données.

Current calls: 157
Media flows: 363

Call Number	SSRC	Name	End Cause	Codec	Media Type	Duration	Packet ...	MOS-CQ
146	79249101	RTP 10.107.137.209:20020-->10.2...	truncated	RTP 118 (unsupported)		00:01:52.802091		
150	2920C602	RTP 10.107.140.150:20036-->10.2...	truncated	RTP 118 (unsupported)		00:01:18.656588		
150	27061A01	RTP 10.29.244.89:20010-->10.107....	truncated	RTP 118 (unsupported)		00:01:04.163039		
102	3CAE5D05	G.711 10.149.193.156:20592<--10....	BYE	G.711 A-law	Voice	0.720099	0.000	1.50
79	2BDBA30C	G.711 10.149.193.156:29846-->10....	truncated	G.711 A-law	Voice	6.353595	8.150	2.31
87	670CAA85	G.711 SBC NOE:62664-->10.29.243...	BYE	G.711 A-law	Voice	4.564394	8.297	2.36
66	4B804F09	G.711 SBC NOE:59800-->10.29.243...	BYE	G.711 A-law	Voice	3.241681	11.043	2.41
75	E4AB40D7	G.711 SBC NOE:60248-->10.87.26....	over timeout	G.711 A-law	Voice	00:01:41.060361	7.224	2.46
82	4A304709	G.711 10.149.193.156:29862-->10....	BYE	G.711 A-law	Voice	15.581015	6.795	2.46
72	A84EB209	G.711 10.149.193.151:27900-->10....	BYE	G.711 A-law	Voice	22.741824	6.591	2.51
72	DBBB62E3	G.711 SBC PACY:33300-->10.29.24...	BYE	G.711 A-law	Voice	4.375761	6.818	2.56
64	115ADC75	G.711 SBC NOE:58796-->10.29.243...	BYE	G.711 A-law	Voice	51.482467	6.396	2.61
93	E46ECB0C	G.711 10.149.193.148:26200-->10....	BYE	G.711 A-law	Voice	13.422474	5.952	2.66
34	D69570ED	G.711 SBC NOE:55616-->10.29.244...	over timeout	G.711 A-law	Voice	00:05:08.360462	9.008	2.71
39	FA34A090	G.729A 10.85.142.28:22270-->10.8...	over timeout	G.729A	Voice	00:04:11.327583	5.749	2.71
63	73E77163	G.711 SBC PACY:30908-->10.87.29...	over timeout	G.711 A-law	Voice	00:01:51.052978	5.612	2.71
66	9E309303	G.711 10.149.193.242:28932-->10....	BYE	G.711 A-law	Voice	31.680960	5.200	2.71
82	262C3729	G.711 SBC PACY:34648-->10.29.24...	BYE	G.711 A-law	Voice	50.540209	5.936	2.71
87	8FF93504	G.711 10.149.193.148:28162-->10....	BYE	G.711 A-law	Voice	24.176962	5.702	2.71
9	B76978B1	G.711 SBC NOE:32868-->10.29.244...	over timeout	G.711 A-law	Voice	00:02:48.056438	5.266	2.81

Figure 18 : Tableau rassemblant tous les appels passés pendant la durée du problème.

Le MOS est inscrit sur la droite du tableau (Figure 18). Pour savoir si le problème vient de l'opérateur ou de EDF, il faut regarder les adresses IP. Dans ce cas-là, le problème vient du côté opérateur car on reçoit des données provenant des SBC* NOE ou PACY et en direction de l'adresse IP 10.29.24X.X qui correspond au vlan data du site de Tours. L'inverse signifierait que le problème vient de EDF.

Le problème venant de l'opérateur, je n'ai pas alerté les personnes sur Tours pour arrêter la migration.

Les problèmes de qualité se faisant rares, je n'ai pas eu à alerter les techniciens pendant toute la durée de la migration. Finalement, plus de 130 agents ont migré vers la softphonie cette semaine-là.

3.2 Mise à jour des sondes

Les sondes sont des outils extrêmement pratiques lorsque l'on veut surveiller le trafic sur un réseau. Je les aurais manipulés quasiment toute la durée du stage et j'ai trouvé vraiment intéressant de savoir comment est-ce qu'on les mettait à jour et à quoi servait cette mise à jour.

La mise à jour 12.5 des sondes Savvius sur les sites EDF est arrivé le 29 mai 2019. Elle offre plusieurs correctifs de bugs et améliorations, mais surtout une nouvelle interface web dont on accède en entrant l'adresse IP de la sonde sur un navigateur web (Figure 19).

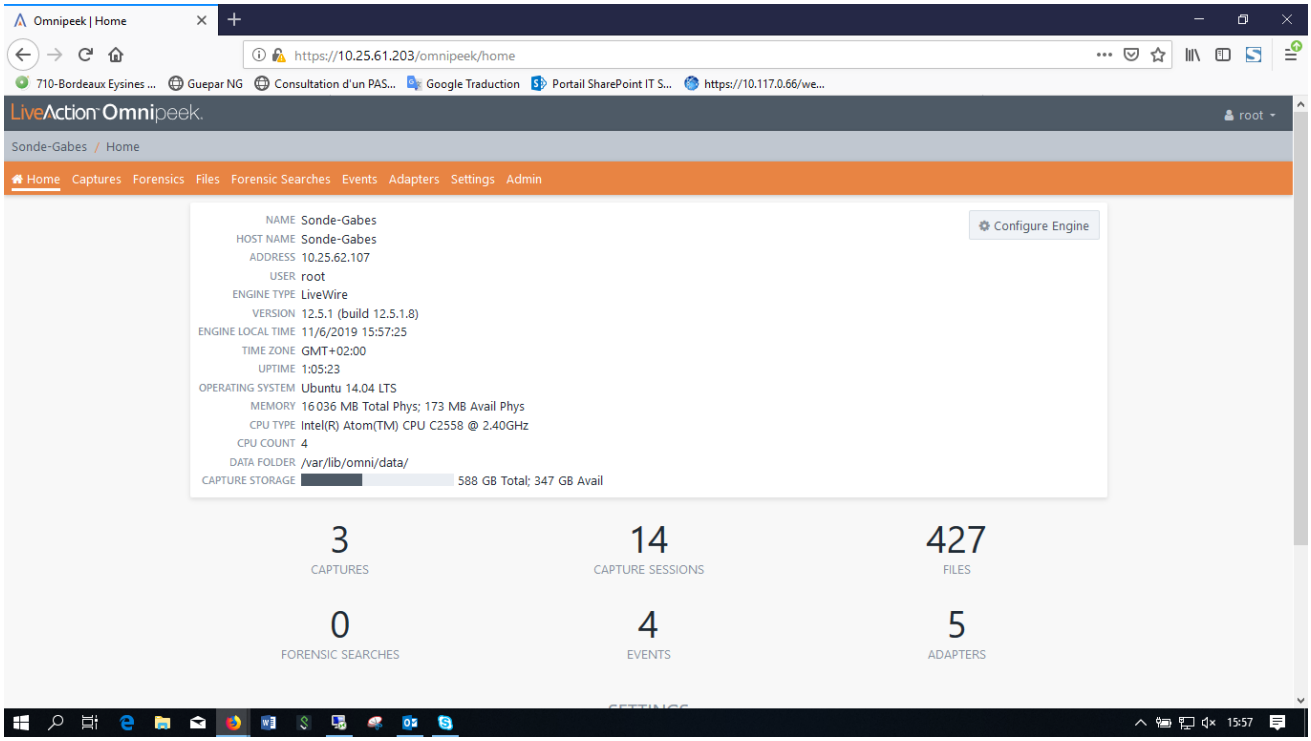


Figure 19 : Interface web d'OmniPeek pour la sonde du site de Gabès

Sur la Figure 19, on peut y voir écrit « LiveAction OmniPeek ». En effet la société Savvius, qui était détentrice des sondes et de OmniPeek, a été rachetée par LiveAction. La nouvelle société a décidé, avec la mise à jour 12.4, de mettre en place une interface web pour accéder à OmniPeek. La mise à jour 12.5 ne fait qu'ajouter des fonctionnalités qui sont présentes sur OmniPeek mais qui n'était pas encore présentes sur la page web. Toutes les fonctionnalités présentes sur OmniPeek ne sont pas encore présentes sur cette version web, mais elles seront rajoutées à terme avec les futures mises à jour.

Pour qu'une sonde soit mise à jour, il faut qu'elle redémarre. Cela entraine donc un arrêt de la capture qu'elle effectue pendant quelques minutes. C'est pour cela que, tout comme la mise en fonctionnement des alarmes, les mises à jour ce font tôt le matin ou tard le soir.

On m'a alors montré comment est-ce qu'une mise à jour d'une sonde se passe. La démonstration s'est faite sur la sonde de Marseille Gabès pendant la phase de test le mercredi 29 mai. Cette phase de test consiste à mettre à jour une seule sonde pour vérifier si la mise à jour applique bien les correctifs sans ajouter de nouveaux bugs. Quelques jours plus tard après avoir vérifié le bon fonctionnement de la sonde, suite à la mise à jour, nous pouvions commencer à mettre à jour les autres sondes.

Contrairement à la mise à jour de test qui s'est faite en journée sur la sonde de Marseille Gabès, car cette sonde est une maquette qui permet de faire des tests, les autres sondes ont dû être mises à jour le lundi 3 mai, entre 7h30 et 8h30 du matin, avant l'augmentation de l'activité des sites.

Pour mettre à jour une sonde j'ai dû utiliser le logiciel WinSCP qui a permis d'accéder au fichier de la sonde en s'y connectant, car en effet, la mise à jour est sous forme de fichier que l'on doit copier et coller dans le dossier précis.

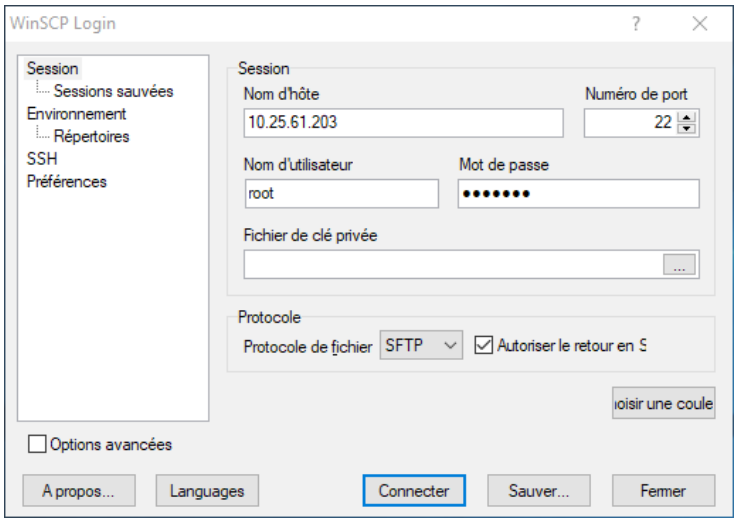


Figure 20 : Interface de connexion de WinSCP

On rentre l'adresse IP de la sonde que l'on veut mettre à jour, l'adresse de la Figure 20 correspond à la sonde de Marseille Gabès. Il faut aussi un nom d'utilisateur et son mot de passe pour se connecter. Une fois connecté, on se rend dans le dossier racine, puis dans tftpboot pour y copier les deux fichiers de mise à jour (Figure 21). C'est deux vont faire redémarrer la sonde quelques minutes après la copie.

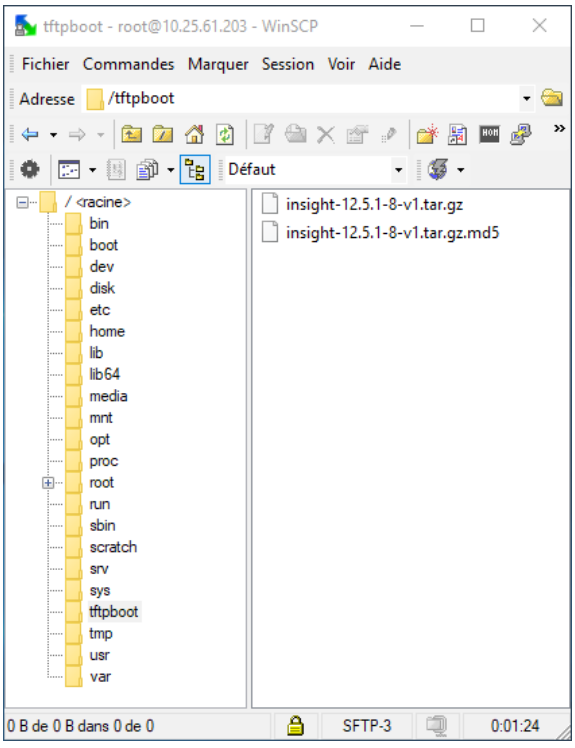


Figure 21 : Dossier tftpboot avec les deux fichiers de mise à jour copiés à l'intérieur.

Une fois la copie des deux fichiers terminée, on peut lancer un ping sur la sonde pour voir quand elle va redémarrer. On ouvre alors l'invité de commande Windows et on entre la commande « ping 10.25.61.203 -t ». Le « -t » à la fin permet de faire un ping en continue. Le ping affichera « Délai d'attente de la demande dépassé. » lorsque la sonde redémarrera.

Finalement quand le ping reprend, cela signifie que la sonde a bien redémarré, il ne reste plus qu'à vérifier sur Omnipeek la version de la sonde, regarder que tout fonctionne correctement et vérifier que la capture a bien repris.

Il fallait répéter ce processus quatorze fois en tout pour mettre à jour toutes les sondes. On s'est alors réparti le travail avec mon tuteur pour en faire sept chacun le lundi 3 mai au matin.

Conclusion

Pour conclure, ce stage de fin d'études de dix semaines que j'ai effectué au sein du PTTR chez EDF, m'a permis de mettre en pratique et d'approfondir mes connaissances théoriques, acquises durant ma formation, à travers les différentes missions qui m'ont été confiées. En effet j'ai beaucoup appris durant ces dix semaines, autant sur le plan du savoir et du savoir-faire, avec de nouvelles connaissances acquises et la manipulation de différents logiciels, que sur le plan du savoir-être en entreprise.

Cela m'a aussi permis par la même occasion de découvrir réellement le monde du travail en entreprise car ce fût une première expérience professionnelle pour moi.

Malgré certains problèmes qui sont survenus durant l'accomplissement de mes missions, j'ai su rebondir grâce à l'aide de toute l'équipe et j'ai tout de même pu terminer toutes les taches qui m'ont été confiées.

Le système d'alertes par mail que j'ai pu configurer est terminé et est fonctionnel. Il est conçu pour durer au sein du pôle et peut être modifié si besoin grâce à une documentation détaillée que j'ai créée pour que tous les techniciens puissent savoir de quelle façon j'ai mis en place le système. Ils pourront ainsi modifier les alarmes sans difficulté si nécessaire.

Les deux autres missions auxquelles j'ai participé m'ont permis de découvrir d'autres aspects tout à fait intéressant du métier de technicien télécoms chez EDF.

Ce stage a été très enrichissant pour moi, et m'a permis de comprendre que les réseaux et les télécommunications sont vraiment ce que je souhaite faire plus tard. En effet, l'an prochain je souhaite faire une licence professionnelle en alternance et m'orienter vers le secteur de l'administration des réseaux.

Remerciements

Je tiens à remercier l'équipe du Pôle Technique Télécoms et Réseaux d'EDF pour son accueil et son implication durant ces 10 semaines de stage au sein de son service.

Je remercie tout particulièrement mon tuteur de stage, **Mr Thomas REUTENAUER** pour son investissement, son accompagnement tout au long du stage et son partage de connaissances qui m'ont permis de mener à bien mes missions.

Je tiens également à remercier **Mr Ramzi ZARROUGA**, Chef du Pôle Technique Télécoms et Réseaux, qui m'a accordé sa confiance en m'acceptant en tant que stagiaire.

Je n'oublie pas **Mr Gérard ZINGONI** qui m'a recommandé auprès du Chef de service en appuyant ma demande et qui m'a permis de réaliser ce stage à ses côtés.

Glossaire

ToIP, Téléphonie sur IP, permet de raccorder son réseau téléphonique à une ligne Internet en utilisant le protocole réseau IP.

PA RIN, Point d'Accès au Réseau d'Interconnexion National. Les PA RIN sont des routeurs qui font le lien entre le RIN et le RLE (réseau local d'entreprise).

RIN, Réseau d'Interconnexion National, est un réseau LAN étendu qui relie tous les sites EDF entre eux (utilisant MPLS, MultiProtocol Label Switching).

Sonde, une sonde permet de capturer le trafic passant sur le réseau, y compris les flux, les conversations, les applications, les protocoles et de mesurer la performance afin de pouvoir gérer et dépanner les sites où sont les sondes de façon optimale.

MOS, Mean Opinion Score, est une note donnée pour caractériser la restitution sonore. Cette note varie de 1 pour une très mauvaise qualité jusqu'à 5 pour une qualité comparable à la version d'origine.

SA, une SA ou société anonyme est une société de capitaux. Elle réunit des personnes dont la participation est fondée sur les capitaux qu'elles ont investis dans l'entreprise.

Systèmes d'informations métiers, c'est l'ensemble des ressources de l'entreprise qui permettent la gestion de l'information.

Lync, Microsoft Lync Server est un serveur de communications en temps réel destiné aux entreprises, fournissant l'infrastructure nécessaire à l'utilisation de la messagerie instantanée, la présence, la voix et la visioconférence.

MOA, Maîtrise d'ouvrage, est la personne ou le groupe qui exprime un besoin.

POGS, est un outil de gestion des incidents et des demandes (de travaux ou d'informations) basé sur ITIL qui est l'approche de gestion des services informatiques la plus reconnue au monde.

RFC, Request For Change, la demande de changement (RFC) est une demande formelle de mise en œuvre d'un changement.

T2, Une liaison T2 est ce qui replie l'opérateur télécoms a l'IPBX (un standard téléphonique IP) de l'entreprise.

Référence RIN, est un numéro d'identification propre à chaque PA RIN et respectant une nomenclature bien précise.

Serveur SMTP, est un serveur qui va permettre l'envoi des mails.

SBC, Session Border Contrôler, est un équipement de sécurité utilisé dans les réseaux de voix sur IP. Les SBC s'assurent de l'acheminement et du contrôle des communications suivant des règles préétablies (NOE et PACY étant les noms des SBC).

Bibliographie

Vivre EDF Online, Intranet EDF : https://www.myelectricnetwork.fr/group/guest/

Site internet d'EDF : https://www.edf.fr/#

OmniPeek User Guide : https://mypeek.savvius.com/elements/mypeek_documentation/manuals/OmniPeek_UserGuide.pdf

Wikipédia : https://fr.wikipedia.org/

LiveAction : https://www.savvius.com/

Wavetel :https://www.wavetel.fr/produits/produits-expertise-pour-la-cybersecurite/sonde-de-capture-reseau-savvius-insight

Support Microsoft Lync : https://support.office.com/fr-fr/article/pr%C3%A9sentation-de-lync-basic-a1821c3d-7631-483c-8791-3d16b10b844d