Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Développement d'une infrastructure de téléphonie IP

Sébastien ICARD

Groupe SNEF

Responsable entreprise : Mathieu MARZULLO

Responsable académique : Roland DEPEYRE

2021

Table des matières

1. Introduction

La voix sur IP (VoIP, Voice over IP) est une technologie de communication vocale en pleine émergence. Elle fait partie des dernières évolutions du monde de la communication. En effet, au lieu de disposer à la fois d'un réseau informatique et d'un réseau téléphonique commuté (RTC), l'entreprise peut donc, grâce à la VoIP, tout fusionner sur un même réseau. Comme toute innovation technologique, la VoIP non seulement simplifie l'exploitation des réseaux mais permet aussi une réelle économie pour les entreprises.

Le réseau sans fil plus communément appelé Wi-Fi est devenue omniprésent depuis l'arrivée des smartphones et des ordinateurs portables. Il est maintenant indispensable pour une entreprise d'en posséder un dans ses locaux. Cependant, cela peut représenter des failles de sécurité s'il s'avère qu'il n'est pas administré correctement. Il faut donc s'assurer qu'il n'y ait pas d'utilisateur non désiré pouvant accéder au réseau de l'entreprise.

Dans le cadre de mon DUT Réseaux et Télécommunications à l'Université d'Aix-Marseille, j'ai pu réaliser mon stage de fin d'étude au sein du pôle Télécom du GROUPE SNEF.

Pendant cette période de mise en situation de 10 semaines, je me suis familiarisé avec un environnement technique, qui m'a permis d'approfondir mes connaissances dans le milieu professionnel. En effet, j'ai pu mettre en pratique les compétences étudiées pendants ma formation. Ainsi différentes missions sur le thème de la VOIP et du Wi-Fi m'ont été confiées. Grâce à ce stage, j'ai travaillé sur des projets qui m'ont permis d'entrevoir en quoi consiste la profession de technicien réseaux et télécommunications.

Dans un premier temps nous exposerons l'entreprise SNEF et son secteur d'activité. Avant de décrire plus précisément le service qui m'a accueilli tout au long de ce stage. Enfin nous étudierons les missions que j'ai réalisées dans les domaines des télécommunications, des réseaux et de l'informatique. Enfin, nous dresserons un bilan de ces dix semaines de stage.

2. Présentation de l'organisme d'accueil

2.1. Le Groupe SNEF

En 1905, naissait sur le port de Marseille, une petite compagnie spécialisée dans l'installation électrique à bord des navires : la société Electric-Flux. Elle deviendra un partenaire de la marine nationale. Puis, tout en se développant, elle s'est ensuite transformée en Société Nouvelle Electric-Flux en 1955, fusionnant avec la Générale Électromécanique.

En 1997, c'est un véritable groupe qui se constitue, rayonnant aussi bien en France qu'à l'Étranger.

Au-delà d'une activité historique centrée sur le « Génie Électrique », le groupement s'est diversifié dans ses métiers, devenant ainsi un acteur reconnu du génie électrique, de l'instrumentation et du contrôle commande.

S'adaptant aux mutations technologiques, le Groupe SNEF a anticipé les nouveaux besoins notamment dans ce passage à l'ère du tout numérique et a largement accru son champ de compétences.

Leader indépendant depuis plus de 110 ans, il est présent dans de nombreux secteurs de l'industrie et des services.

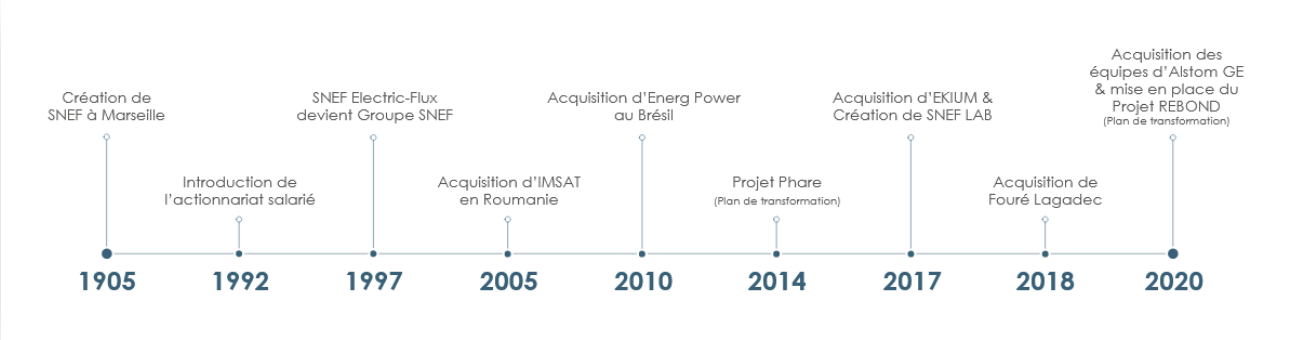

Figure 1 – Graphique Histoire – Extrait du Site www.snef.fr

Son offre de services et d'expertises s'appuie sur ses différentes filiales (CIEL, FIRAC, SNEF Technologies, SEM…) et/ou marques (SNEF Connect, SNEF Clim, Maintenance, Design & Build, Telecom, Nucléaire).

Le groupe SNEF est composé à 100% de capitaux français et réalise un chiffre d'affaires de 1,5 Milliard d'Euros en 2020. De taille humaine, il n'accueille pas moins de 12.500 collaborateurs qui sont « SNEF et fiers de l'être ». L'entreprise est attachée à une forte culture du résultat et du sens du service.

Le réseau tissé est composé d'agences de proximité implantées sur le territoire métropolitain.

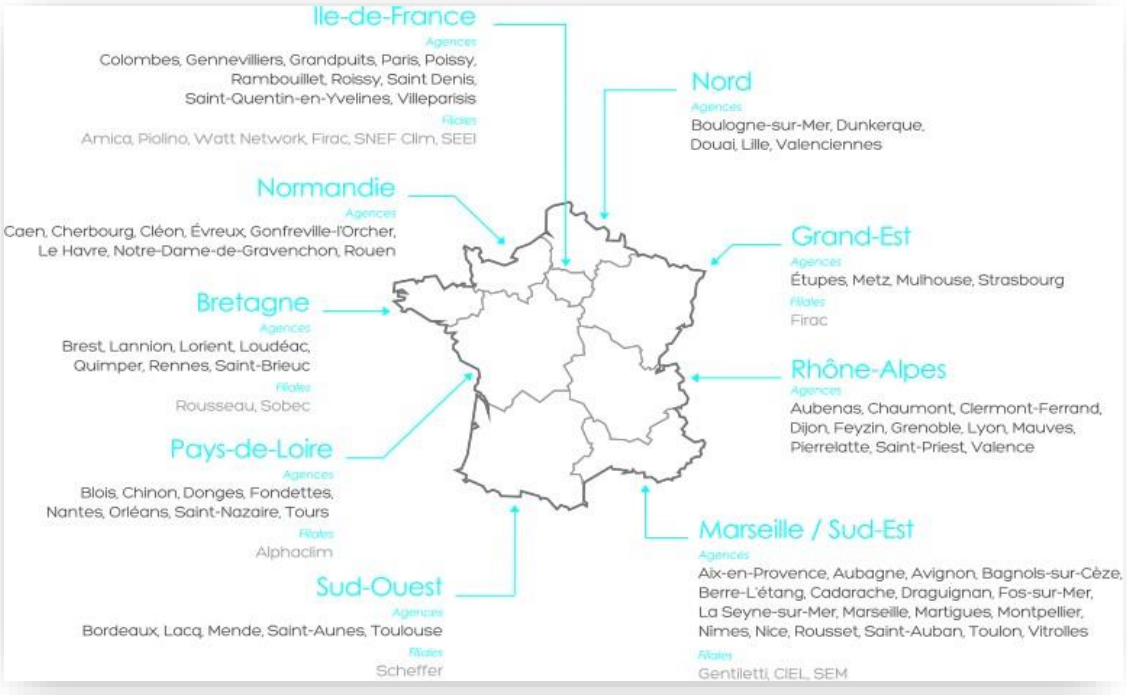

Figure 2 – Graphique Implantations FRANCE –

Par ailleurs, le groupe SNEF qui se développe à l'international depuis 40 ans, est présente dans une vingtaine de pays, que ce soit en Europe de l'Est/Ouest, en Afrique, au Moyen-Orient, en Amérique du Sud/ Nord et en Australie.

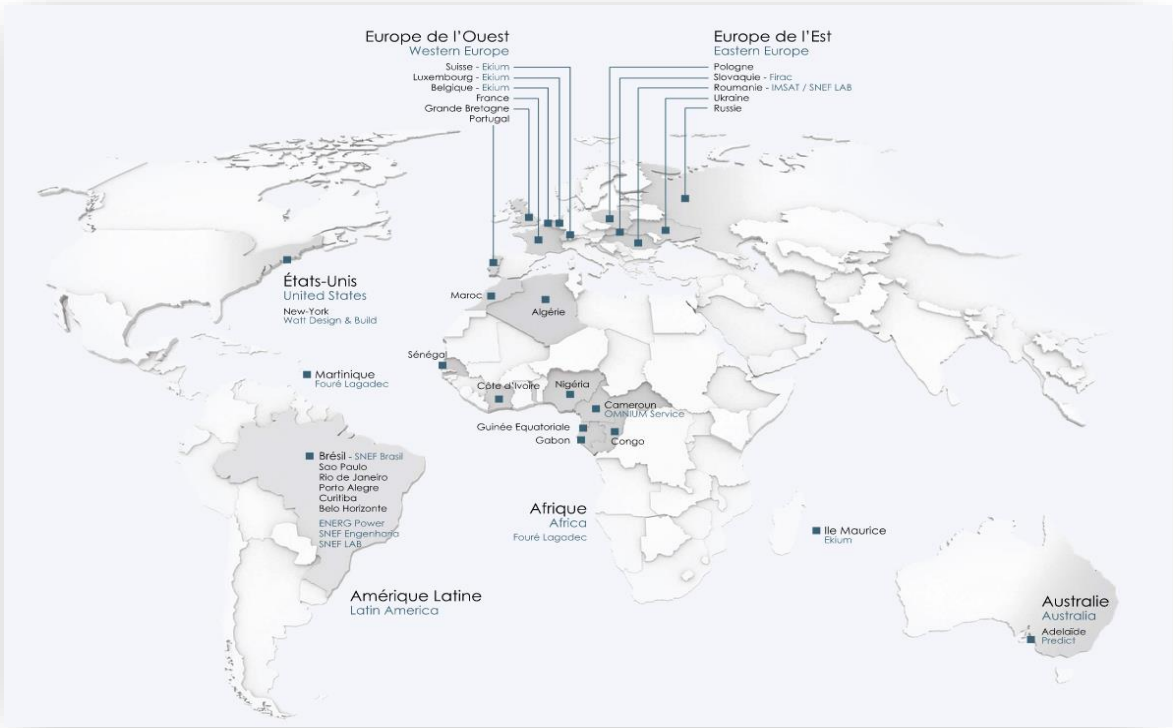

Figure 3 – Graphique Implantations MONDE –

2.2. Mon secteur d'activité

Mon stage s'est déroulé au siège social du groupe SNEF dans le pôle Télécom. Ce service est responsable du déploiement et de la mise en place de stratégie concernant les postes téléphoniques, les équipements informatiques, et les réseaux des agences du groupes SNEF. L'organigramme (Figure 4) nous montre l'organisation du service dans lequel j'ai réalisé mon stage.

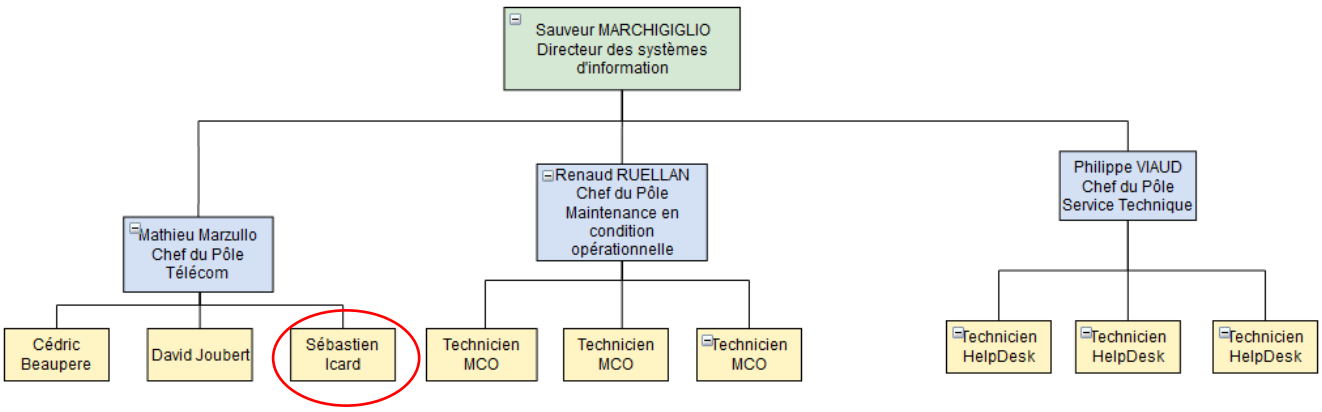

Figure 4 -Organigramme du service d'accueil

3. Mes Missions

Au cours de mon stage j'ai pu réaliser plusieurs missions que je vais détailler dans les parties suivantes.

Le premier projet que l'on m'a confié était associé à l'installation et la configuration d'un système de téléphonie. La première mission a été de rédiger la documentation. J'ai ensuite complété cette documentation en y ajoutant une partie dédiée à l'installation du système de téléphonie sur un environnement hébergé par des machines virtuelles, afin de déployer ou dépanner les systèmes dans les différentes agences de la SNEF.

Ma deuxième mission a été d'intégrer ce système de téléphonie dans une maquette comprenant des switches, un firewall qui permet aussi le routage, des téléphones IP et des ordinateurs.

Un deuxième projet m'a été confié portant sur le déploiement du réseau Wi-Fi dans les agences SNEF. Tout d'abord j'ai dû mettre en place un système d'authentification fiable par l'active directory aux bornes WI-FI. Enfin il m'a été demandé de trouver une solution pour la mise en place d'un portail captif visant à accueillir les personnes extérieures de la SNEF.

4. Téléphonie IP

4.1. Installation d'un environnement virtuel

Dans le cadre de ma première mission, nous allons tout d'abord redéfinir ce qu'est une machine virtuelle. En informatique, cela correspond à une illusion d'un appareil informatique. Dans notre cas nous allons créer une machine virtuelle hébergeant le serveur de téléphonie IP.

Pour cela nous installons d'abord VMware ESXi qui est une solution de virtualisation permettant la création et l'administration de VM (Virtual Machine).

Grâce à son interface graphique accessible depuis le web, la gestion des VM sur VMware ESXi est grandement simplifiée. Travailler avec des machines virtuelles possède de multiples avantages, hormis le gain financier, la virtualisation offre une grande facilité de déploiement ou de migration des installations, ce qui n'est pas négligeable en termes de gestion de serveur. Elle permet aussi d'effectuer des sauvegardes de ces VM ce qui offre une sécurité supplémentaire en cas de dysfonctionnement.

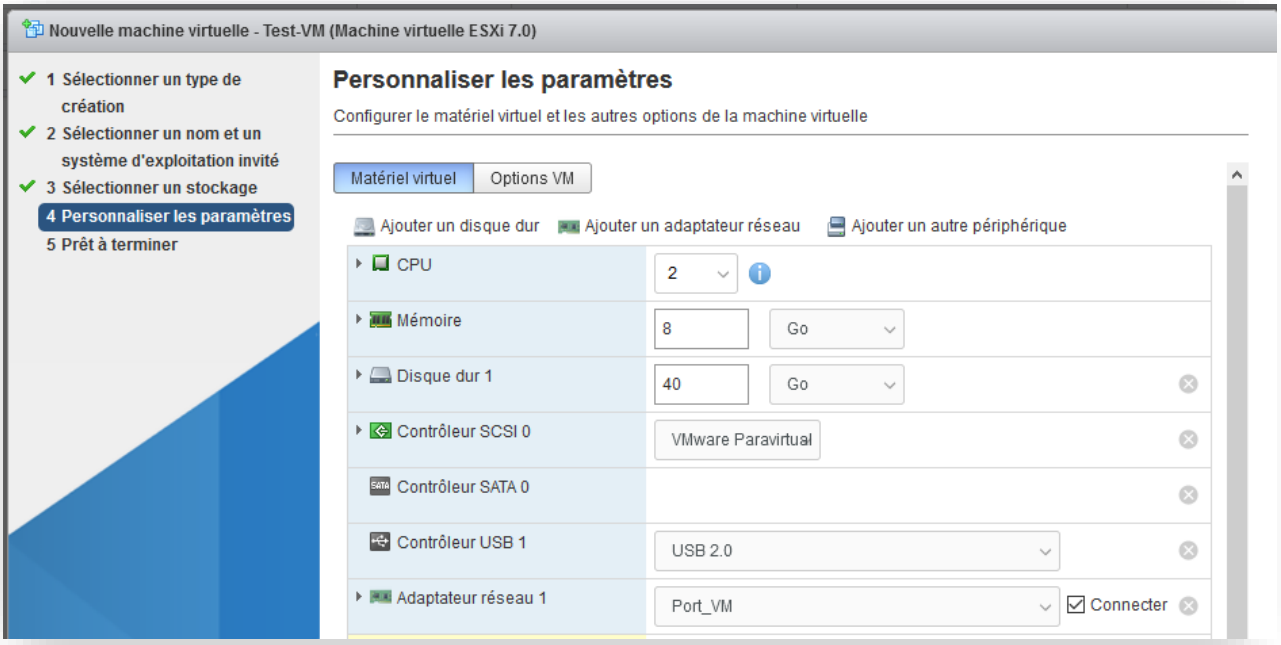

Figure 5 – Allocation des ressources de la VM

On peut donc gérer finement les ressources allouées à la VM (Figure 5). Nous définissons le nombre de CPU (central processing unit), la taille de la mémoire, la quantité d'espace de stockage, ainsi que l'adapteur réseau qui sera configurer sur notre machine. Ces informations sont essentielles au bon fonctionnement de notre VM, il faut donc lui donner les bonnes ressources afin de réaliser les tâches qui lui seront confiées.

Nous finissons par sélectionner l'image disque à utiliser pour démarrer la machine et enfin pouvoir s'en servir tel un serveur de téléphonie. Dans notre cas nous utiliserons CentOS 8 qui est une distribution GNU/Linux destinée aux serveurs.

4.2. Mise en place d'un serveur de téléphonie

Pour la mise en place du serveur de téléphonie nous installons sur notre système la solution Asterisk, qui est un autocommutateur téléphonique privé libre et propriétaire pour systèmes GNU/Linux. Pour faciliter son administration nous utiliserons FreePBX, une interface utilisateur graphique (GUI) open-source basée sur le web qui gère Asterisk.

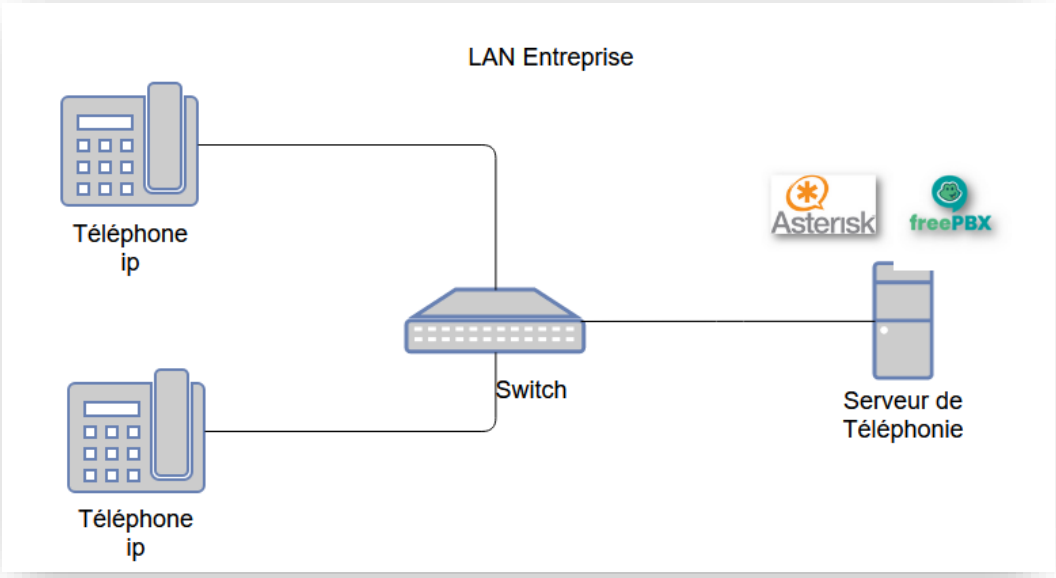

Figure 6 – Architecture du système de téléphonie

La figure 6 présente l'architecture du système de téléphonie souhaité dans un premier temps. Nous souhaitons relier des téléphones IP à un switch afin qu'ils accèdent au serveur de téléphonie qui hébergera nos solutions Asterisk et FreePBX.

4.2.1. Installation d'Asterisk

Pour l'installation d'Asterisk il est nécessaire d'installer des modules complémentaires (Janson, PJSIP, etc…) pour son bon fonctionnement, voire Annexe 1. Nous avons décidé d'installer la dernière version d'Asterisk (Version 18). Pour cela nous avons téléchargé la version souhaitée sur le site d'Asterisk, puis nous l'avons installée sur le système CentOS 8. Il faut être vigilant aux pares-feux présents sur le système d'exploitation. A cette occasion, j'ai découvert le problème car ils bloquaient les requêtes RTP (Real-Time Transport Protocol) qui est un protocole de communication informatique permettant le transport de données soumises à des contraintes de temps réel, tels que des flux média audio ou vidéo. Ce problème empêchait donc mes téléphones IP de se connecter à Asterisk. Dans mon cas j'ai pu désactiver complétement les pares-feux car la sécurité du réseau est déjà gérée par des pares-feux physiques.

4.2.2. Installation de FreePBX

De même, pour l'installation de FreePBX 15 des modules complémentaires sont nécessaires (php, nodejs, MariaDB, Apache) : voir en Annexe 1. Une fois l'installation terminée, nous avons pu nous connecter à l'interface utilisateur graphique afin de gérer Asterisk en tapant l'adresse du serveur dans un navigateur web.

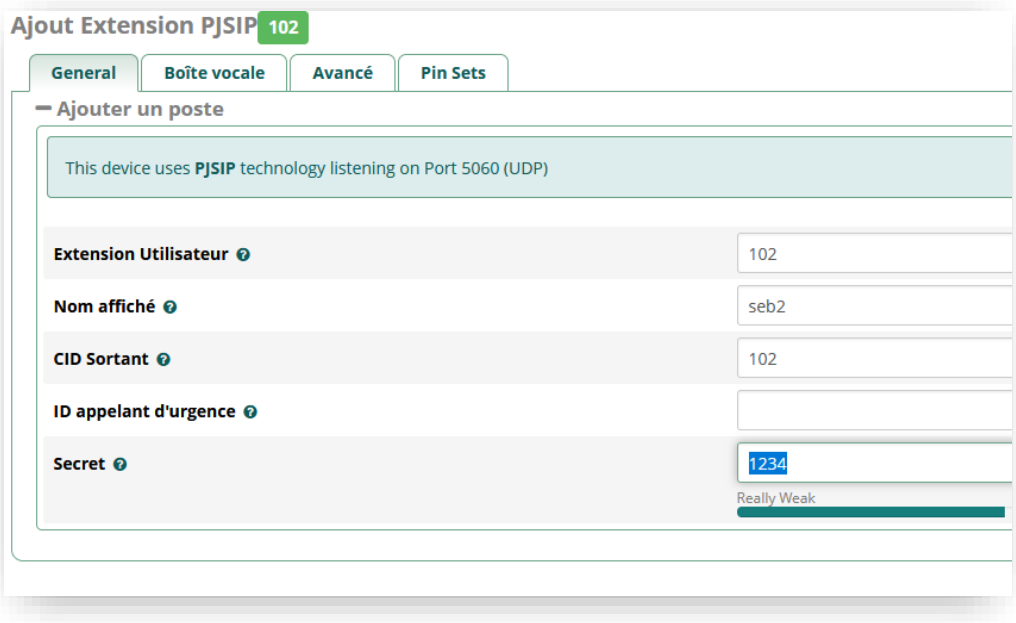

Figure 7 – Création d'une extension pour un utilisateur

Il a alors été possible de créer des comptes appelés « Extensions » (Figure 7) qui seront à renseigner sur les téléphones IP. Ces extensions permettent de se connecter au serveur de téléphonie et d'avoir un numéro qui permet de joindre les autres postes du réseau ou bien d'être joignable depuis ces postes.

4.2.3. Appel depuis et vers l'extérieur

Pour permettre au poste d'émettre et de recevoir des appels vers l'extérieur il faut configurer un trunk SIP qui permet de connecter un système de téléphonie interne, ici Asterisk directement à un réseau opérateur. Quand un utilisateur passe un appel vers l'extérieur il est redirigé vers les services de l'opérateur qui s'occupera d'acheminer l'appel vers le numéro extérieur. Inversement quand un appel est émis vers un poste interne l'opérateur transmettra l'appel vers notre serveur de téléphonie.

Nous avons donc configuré sur notre serveur un Trunk Sip afin d'indiquer les identifiants, mot de passe et serveur auquel se connecter pour effectuer la liaison avec l'opérateur (W3tel dans notre cas). Ensuite il faut créer une route sortante pour router le trafic à destination de l'extérieur et donc la faire pointer vers notre Trunk Sip. Et pour finir il faut créer les routes entrantes afin que le serveur puisse rediriger les appels venus de l'extérieur vers le bon poste téléphonique, c'est à ce moment que nous attribuons un numéro de type 04.xx.xx.xx.xx au téléphone. Jusqu'ici les postes avaient un numéro seulement en interne (généralement 101,102, etc…) on appelle cela un SDA (**S**élection **D**irecte à l'**A**rrivée).

4.2.4. Configuration des téléphones IP

Nous devons maintenant configurer les téléphones en les enregistrant auprès du serveur de téléphonie.

Figure 8 – Téléphone IP GrandStream GXP2140

Nous utilisons des GrandStream GXP2140, ils peuvent être configurés directement dans les paramètres du téléphone (Figure 9) ou depuis un navigateur web à l'aide d'une interface graphique.

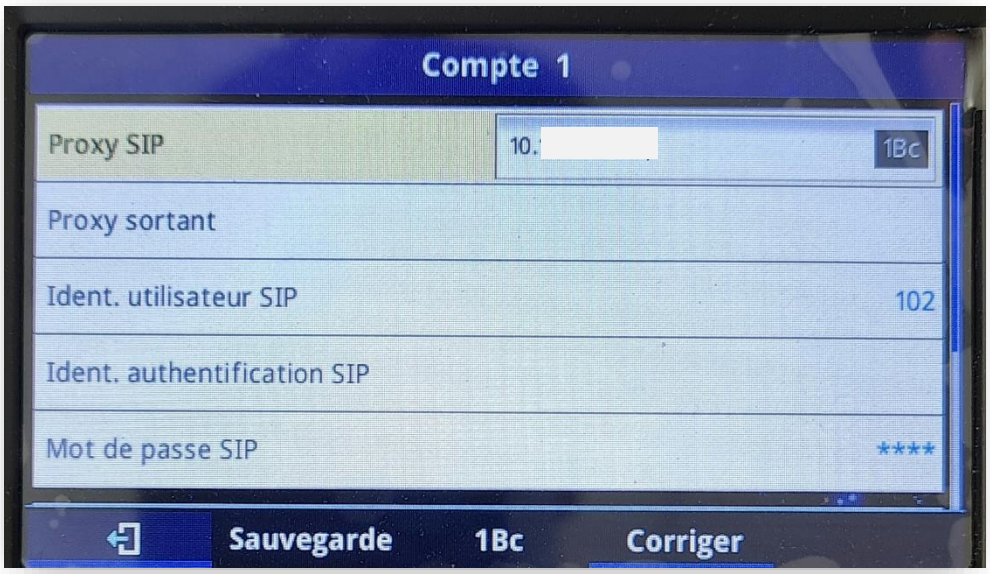

Figure 9 – Configuration de l'extension

Une fois le compte configuré, il est désormais possible de passer et de recevoir des appels en interne comme en externe. Les adresses IP ont été cachées pour éviter de créer un risque de sécurité au niveau de l'entreprise.

4.3. Intégration du système dans une maquette

Une maquette réaliste m'a été confiée, elle réplique une architecture d'une agence type de la SNEF. Un Firewall, un switch, un serveur, deux téléphones IP ainsi qu'un ordinateur portable ont été mis à ma disposition. Le but est de mettre en place des vlan (**V**irtual **L**ocal **A**rea **N**etwork) dédiés à chaque utilisation. Un vlan est un réseau local virtuel logique et indépendant. Il permet donc de séparer les flux ce qui améliore la gestion du réseau et du trafic. Il offre aussi une sécurité puisqu'il permet de séparer les utilisateurs.

Nous avons donc un vlan « User » destiné à accueillir les ordinateurs, un vlan « Voix » réservé au téléphone, un Vlan « Admin » pour l'administration du switch et du serveur ESXi et enfin un vlan « DMZ » pour accueillir le serveur de téléphonie. Le routage inter-vlan est assuré par un firewall qui est géré par l'administrateur réseau. Les ordinateurs sont reliés avec une prise Ethernet directement aux postes téléphoniques qui sont eux-mêmes reliés au switch (Figure 10). Il faut donc que le switch différencie le téléphone IP de l'ordinateur afin de les placer dans leurs vlan respectifs.

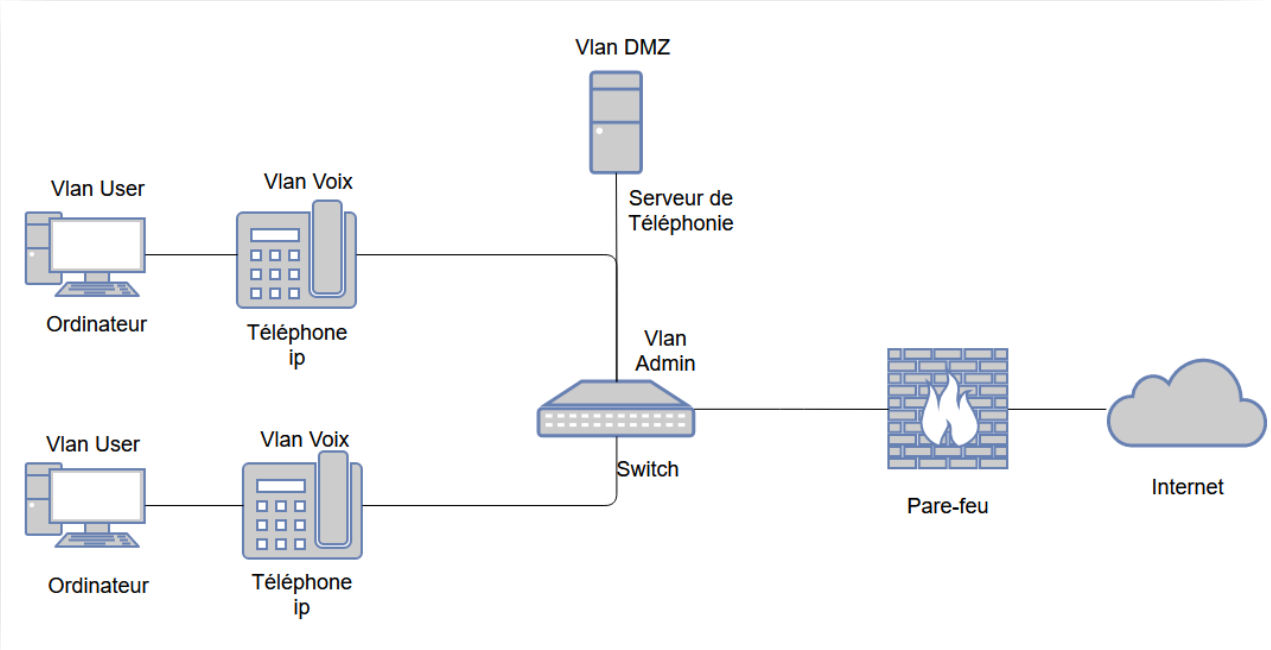

Figure 10 – Architecture de la maquette SNEF

4.3.1. Voice Vlan sur switch Cisco

Pour permettre au switch de placer chaque équipement dans son vlan associé nous allons utiliser une configuration sur les ports appelées « Voice Vlan ». Le Voice Vlan peut être configuré de deux manières. On peut le déployer afin qu'il se base sur l'envoie de paquet LLDP (**L**ink **L**ayer **D**iscovery **P**rotocol) ou CDP (**C**isco **D**iscovery **P**rotocol) qui sont des protocoles permettant la découverte des topologies Réseau. Ou nous pouvons le configurer pour qu'il analyse les adresses Mac des équipements. Une adresse Mac est une adresse unique attribuée à chaque carte réseau. Chaque fournisseur possède un ou plusieurs OUI « **O**rganizationally **U**nique **I**dentifier », c'est un numéro qu'il placera au début de ses adresses Mac. De cette manière nous pouvons donc reconnaitre par une adresse Mac, le fournisseur de l'équipement qui lui est associé.
J'ai décidé de configurer le Voice Vlan avec la reconnaissance d'OUI. Il faut donc indiquer dans la configuration du switch les OUI auxquels il devra être attentif afin de placer son équipement associé dans le vlan « Voix ».

```
voice vlan id 50
voice vlan state oui-enabled
voice vlan oui-table add 0001e3 Siemens_AG_phone________
voice vlan oui-table add 00036b Cisco_phone______________
voice vlan oui-table add 00096e Avaya___________________
voice vlan oui-table add 000b82 GS2
voice vlan oui-table add 000fe2 H3C_Aolynk_______________
voice vlan oui-table add 0060b9 Philips_and_NEC_AG_phone
voice vlan oui-table add 00d01e Pingtel_phone____________
voice vlan oui-table add 00e075 Polycom/Veritel_phone___
voice vlan oui-table add 00e0bb 3Com_phone_______________
voice vlan oui-table add c074ad GS
```

Figure 11 – Ajout des OUI fournisseurs de téléphone IP

Etant donné que nous utilisons des téléphones Grandstream leurs OUI sont :

- C0 :74 :AD
- 00 :0B :82

Je les ai donc renseignés dans la table OUI comme nous pouvons le voir (Figure 11) au nom de « GS » et « GS2 ». La configuration complète du switch se trouve dans l'annexe 1.

5. Gestion du réseaux Wi-Fi

5.1. Système d'authentification au borne Wi-Fi par l'active directory

Le deuxième projet abordé durant mon stage consiste à la mise en place d'une méthode d'authentification à une borne Wi-Fi par l'Active Directory. L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc… Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leur utilisation grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l'accès aux ressources répertoriées.

Un AD (**A**ctive **D**irectory) se configure sur une machine qui possède le système d'exploitation Windows Server. Ce système permet de configurer plusieurs « rôles » notamment un AD mais aussi une autorité de certification, un DNS (**D**omain **N**ame **S**ystem), ou bien un serveur NPS (**N**etwork **P**olicy **S**erver) par exemple. Pour répondre au besoin du projet nous avons utilisé un serveur NPS en tant que serveur RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice). Le protocole RADIUS permet de faire la liaison entre des besoins d'identification et une base d'utilisateurs en assurant le transport des données d'authentification de façon normalisée. L'opération d'authentification est initiée par un client du service RADIUS, dans notre cas c'est la borne Wi-Fi. Le serveur la traite en accédant à l'AD. Selon notre configuration il vérifiera que le nom du poste qui essaye de se connecter à la borne Wi-Fi est bien enregistré dans l'AD.

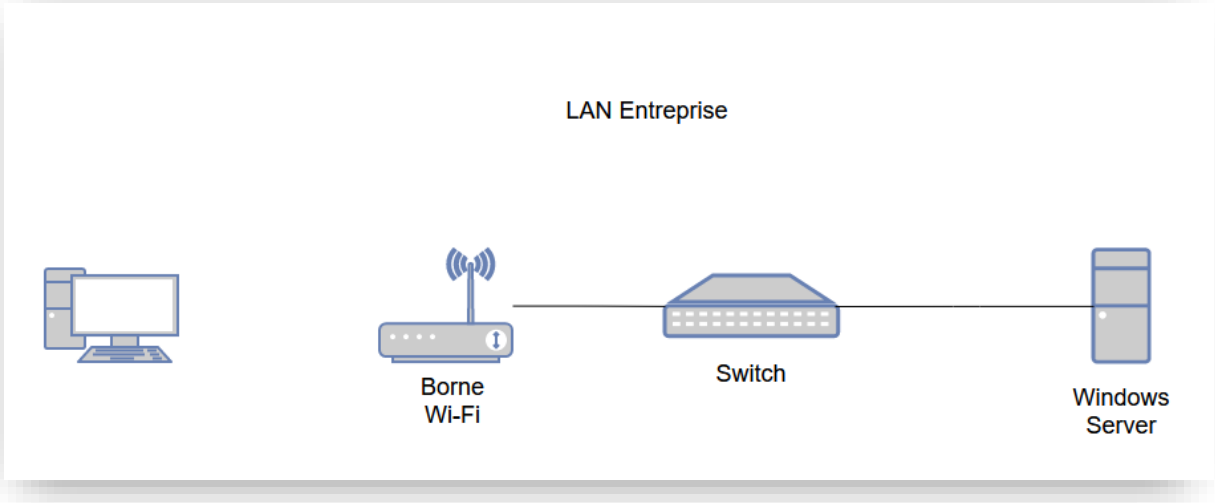

Figure 12 – Architecture du système d'authentification

En Figure 12, voici la solution que j'ai proposée pour réaliser le projet. Quand le poste utilisateur essaye de se connecter à la borne Wi-Fi, cette dernière cherche à contacter le serveur NPS en lui fournissant les informations dont elle dispose (Nom du poste, nom de l'utilisateur, domaine de l'ordinateur, etc…). Le serveur NPS vérifie les règles qui lui ont été données, ici il doit s'assurer que le nom du poste est bien enregistré dans l'AD. Il contacte donc l'AD pour vérifier les informations qui lui ont été transmises, si les informations correspondent il envoie l'ordre à la borne Wi-Fi d'accepter la connexion provenant du poste utilisateur. La configuration complète de la solution est disponible dans l'annexe 2.

5.1.1. Configuration du client RADIUS

Il faut d'abord créer le client sur le serveur RADIUS pour qu'il accepte la connexion.

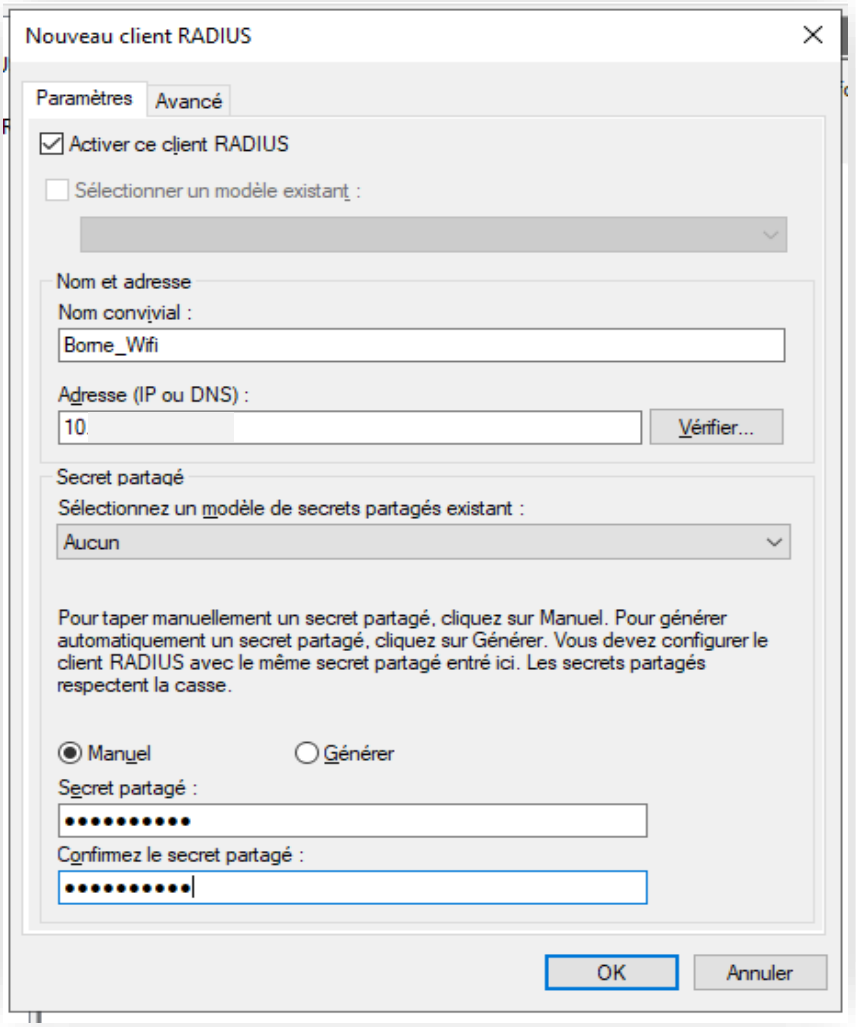

Figure 13 – Client RADIUS

On renseigne ici (Figure 13) l'adresse IP du client (Borne Wi-Fi) ainsi que le mot de passe qui sera échangé lors de la communication entre la borne Wi-Fi et le serveur RADIUS. Sans cette configuration le serveur refusera la demande effectuée par le client.

Du côté de la borne on indique quel est le serveur à contacter pendant l'authentification, en lui précisant donc l'adresse IP de ce serveur et le mot de passe définit pour communiquer. Ensuite on crée un point d'accès avec comme méthode d'autentification le « Serveur d'authentification » je l'ai nommé ici ARUBA (Figure 14).

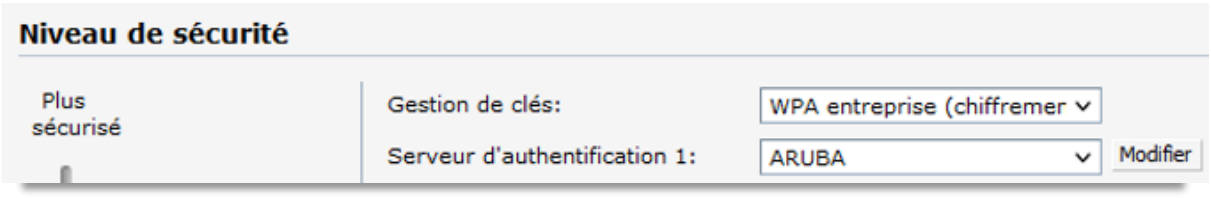

Figure 14 – Méthode d'authentification

5.1.2. Stratégie d'authentification sur le serveur NPS

Il faut maintenant définir la stratégie d'authentification permettant d'accepter ou de refuser une connexion. Nous définissons donc les conditions à respecter pour que la connexion soit acceptée, dans le cas contraire l'accès est complétement refusé. Nous voyons ici (Figure 15) qu'il est nécessaire que la demande de connexion soit associée à une connexion sans fil de type IEEE 802.1X qui est un standard lié à la sécurité des réseaux informatiques. Il permet de contrôler l'accès aux équipements d'infrastructures « réseau » (et par ce biais, de relayer les informations liées aux dispositifs d'identification). En addition à la première condition il est aussi obligatoire que le poste souhaitant se connecter appartienne au groupe « Ordinateur du domaine » qui répertorie tous les ordinateurs ayant accès au domaine.

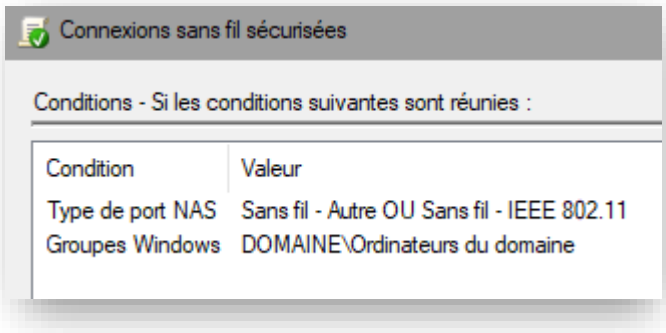

Figure 15 – Conditions d'authentification

Il suffit maintenant de créer un certificat et de le définir dans la méthode d'authentification, pour pouvoir se connecter depuis un ordinateur appartenant au domaine.

5.1.3. Création de certificats pour l'authentification

Nous installons une autorité de certification, nommée AD CS (**A**ctive **D**irectory **C**ertificate **S**ervices) sur Windows Sever. En cryptographie, une autorité de certification est un tiers de confiance permettant d'authentifier l'identité des correspondants. Une autorité de certification délivre des certificats décrivant des identités numériques et met à disposition les moyens de vérifier la validité des certificats qu'elle a fournie. Pendant l'échange entre le poste et le serveur NPS grâce à ce certificat la connexion est sécurisée. Les certificats représentent une grande partie de la sécurisation web. Leur utilisation est très rependue comme dans le protocole HTTPS (HyperText Transfer Protocol Secure).

Nous créons donc un certificat dédié aux ordinateurs et nous l'insérons dans le serveur NPS ainsi quand le poste utilisateur souhaitera s'authentifier auprès du serveur, le certificat lui sera présenté afin de savoir si l'authentification se déroule auprès d'une source de confiance. On peut l'afficher afin de vérifier qu'il correspond bien à celui que nous avons positionné sur le serveur. Dans le cas contraire nous assisterions à une possible usurpation d'identité et ce certificat tel une carte d'identité nous permettrait de nous en assurer. Il est plus courant de faire appel à une autorité de certification de confiance indépendante qui permet de garantir l'identité du service distant. Puisque dans notre cas l'autorité de certification se trouve sur le même serveur que notre service NPS.

5.1.4. Certificat du Firewall

Le firewall de la maquette possède son propre certificat pour accéder au web ainsi un utilisateur qui ne dispose pas de ce certificat ne peut pas accéder au web par mesure de sécurité. J'ai donc pu expérimenter les GPO (Group Policy Object) traduit en français par Stratégie de groupe. Ce sont des fonctions de gestion centralisée de la famille Microsoft Windows. Elles permettent la gestion des ordinateurs et des utilisateurs présents dans un AD. Elles sont très souvent utilisées en entreprise puisqu'elles permettent de définir des paramètres sur des postes. On peut s'en servir pour supprimer l'accès à certains fichiers ou paramètres. Mais ici nous allons nous en servir pour déposer le certificat du firewall sur tous les ordinateurs du domaine. Sur le Serveur hébergeant l'AD nous importons le certificat dans une stratégie de groupe dédiée à tous les ordinateurs du domaine, quand l'utilisateur va se connecter l'AD s'occupera de le déposer dans le magasin des autorités de certification racine de confiance. De cette manière les postes peuvent naviguer sur le web sans problème.

Les possibilités d'administration et de gestion offertes par les GPO sont presque sans limite et permettent d'améliorer grandement la sécurité.

5.2. Création d'un réseau invité sur la borne Wi-Fi

La dernière tâche qui m'a été confiée dans le cadre de ce projet autour du réseau Wi-Fi des agences SNEF, est la création d'un réseau invité visant à accueillir le personnel. Comme vu précédemment chaque employé disposant d'un pc appartenant à l'AD aura la possibilité d'accéder au réseau Wi-Fi de l'entreprise, cependant les personnes extérieures ne peuvent pas y parvenir. C'est pourquoi il est nécessaire de créer un réseau avec authentification par portail captif, qui est une technique consistant à forcer les clients d'un réseau à se connecter au travers d'une page web spéciale avant d'accéder à internet normalement.

Pour se faire nous souhaitons donner la tâche de création des comptes invités aux standardistes. Il faudra donc avoir une solution qui possède des comptes restreints pour la sécurité du réseau. Les comptes doivent avoir une date d'expiration pour ne pas permettre un accès permanent aux invités. Enfin il doit être possible de garder une trace (log) des connexions au réseau car dès lors qu'une organisation accueille des visiteurs, elle a l'obligation légale de conserver les logs (Directive européenne 2006- 24-CE et Décret français du 24 mars 2006).

J'ai étudié plusieurs solutions sur le marché afin de trouver celle qui répondrait le mieux aux besoins de mon entreprise. J'ai réussi à obtenir par le biais d'un commercial de l'entreprise Aruba une version d'évaluation de leur solution de gestion centralisée des bornes Wi-Fi sur différents sites appelée « AirWave ». Après l'installation et la configuration un problème s'est présenté à moi. Il m'était impossible de créer des comptes invités avec une expiration programmée. Il faudrait donc supprimer les comptes manuellement, ce qui rajouterait une tâche d'administration assez lourde, ainsi qu'une possible faille de sécurité en cas d'oubli de suppression. AirWave sera conservé pour l'administration des bornes Wi-Fi en général. Cela permet de ne plus se connecter sur chaque borne, mais de les regrouper dans un seul et même endroit, avec la possibilité de créer des groupes et d'y effectuer des modifications applicables à toutes les bornes y appartenant.
J'ai finalement trouvé une solution en complément permettant de gérer un portail captif pour les réseaux publics, nommé « UCOPIA ». Cette solution répond à tous les besoins de l'entreprise énumérés précédemment.

5.2.1. UCOPIA

Après avoir contacté l'entreprise, nous avons convenu d'un entretien de présentation de la solution. À la suite de cet entretien, j'ai pu obtenir une version d'évaluation pour la mettre en place dans la maquette et tester le produit. Cette version est présentée sous forme de VM, je l'ai donc installée sur mon serveur. Une fois paramétré j'ai accès à une interface de configuration graphique depuis le web. Nous fixons l'adresse ip pour éviter les changements d'adresse qui empêcherait un bon fonctionnement de la solution. Nous configurons un serveur RADIUS qui permettra l'authentification et la communication entre la borne Wi-Fi et le portail captif. Du côté de la borne Aruba nous créons un nouveau réseau local sans fil destiné aux invités, avec les spécifications nécessaires pour atteindre le portail captif présent sur la VM UCOPIA. Une option permet l'enregistrement des activités afin de renvoyer les logs vers UCOPIA grâce au protocole Syslog qui est un service de journaux d'événements d'un système informatique. Une fois les différentes configurations effectuées il est possible de mettre en place le portail captif, je l'ai personnalisé aux couleurs du groupe SNEF(figure 16)

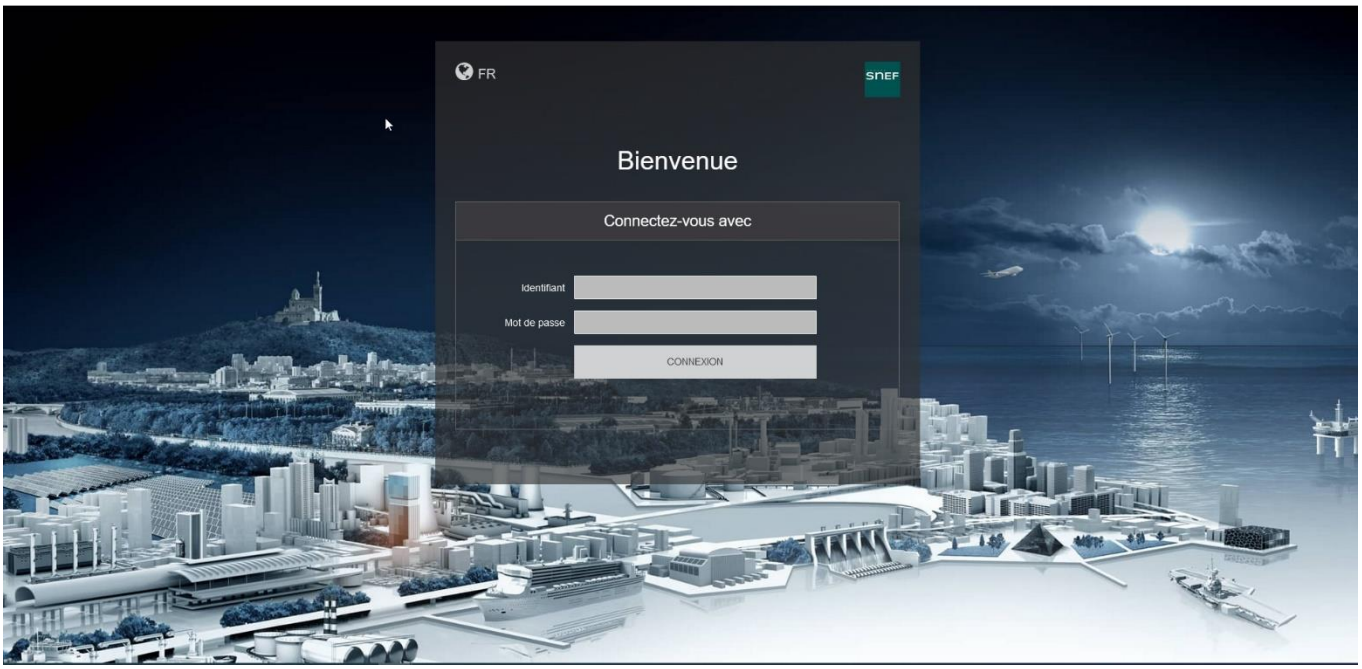

Figure 16 – Portail captif

Il y a différentes méthodes d'authentification et de création de comptes :

5.2.2. Méthodes d'authentification

Nous retrouvons 3 types d'authentification :

- Standard
- Avec facturation
- Réseaux sociaux

Le type standard est le plus adapté à notre utilisation nous y retrouvons donc 4 authentifications, avec identifiant, connexion automatique (reconnaissance des appareils), shibboleth (destiné aux universités et centres de recherches) et SAML qui est un standard informatique définissant un protocole pour échanger des informations liées à la sécurité.

Notre choix se porte sur l'identification standard par identifiant qui demande donc une création au préalable des comptes. Ainsi nous souhaitons donner la possibilité aux administrateurs et aux standardistes de créer des comptes pour le personnel externe à la SNEF. Pour des raisons de sécurité évidente il faut cloisonner les utilisations afin de ne pas donner l'accès aux configurations global du portail captif aux standardistes.

5.2.3. Création des comptes invités

Depuis l'espace de gestion il est possible de créer des comptes avec un grand nombre de paramètres, par exemple les plages horaires dans lesquels le compte peut être utilisé, la période de validité du compte ou encore les services accessibles depuis ce compte (Web, mail, etc…).

Mais tout l'intérêt de la solution réside dans la possibilité de déléguer ce travail. Nous allons donc créer un compte dit d'administration avec accès seulement à l'outil de création des comptes. Une fois créé le standardiste ou la personne désignée pour effectuer ce travail se connecte avec les identifiants qui lui seront communiqués et aura accès à un outil très simple (Figure 17).

Figure 17 – Portail captif

La configuration complète de la solution est disponible dans l'annexe 3.

6. Conclusion

Ce stage a été très enrichissant car il m'a permis de découvrir dans le détail le secteur du réseau et des télécoms. Il m'a permis de participer concrètement à ses enjeux au travers de mes missions variées comme celle de la mise en place d'un système de téléphonie IP ou bien la gestion des bornes Wi-Fi que j'ai particulièrement appréciée. Ces missions m'ont permis de faire des recherches et d'être confronté à des problèmes du monde professionnel comme la sécurité ou la disponibilité. Elles m'ont de plus apportées de nouvelles connaissances qui viennent compléter celles déjà acquises durant ma formation.

J'ai pu remplir les objectifs qui m'ont été fixés durant ces 10 semaines de stages. La découverte du monde professionnel et ses enjeux restent une de mes découvertes personnelles les plus importantes et enrichissantes. J'ai su m'intégrer à l'équipe et lier de vraies relations.

Le bilan de ce stage est pour moi excellent et restera une vraie expérience tant sur le plan technique que sur le plan humain.

7. Remerciements

Je souhaite remercier Mathieu Marzullo, mon maître de stage qui m'a formé et accompagné tout au long de cette expérience professionnelle avec beaucoup de patience et de pédagogie. Il a su me donner gout au métier de technicien réseau et télécom, en étant toujours présent et à l'écoute. Grace à sa confiance et à l'autonomie qu'il m'a laissées j'ai pu vraiment m'épanouir durant ce stage.

Je tiens aussi à remercier Renaud Ruellan, Youssef Smahi, Heddi Zenasni et Cédric Beaupere pour l'aide, les conseils et la gentillesse dont ils ont fait preuve.

Je voudrais remercier Roland Depeyre, mon tuteur académique pour son accompagnement et son investissement tout au long de ma période de stage.

Enfin, je remercie l'ensemble de l'équipe SNEF pour l'accueil et la bienveillance dont ils ont fait preuve.

8. Glossaire

IP, Internet Protocol est une famille de protocoles de communication.

VoIP, Voice over IP », est une technologie informatique qui permet de transmettre la voix sur des réseaux compatibles IP.

Wi-Fi, est un ensemble de protocoles de communication sans fil.

VM, Virtual Machine ou machine virtuelle est une illusion d'un appareil informatique.

CPU, central processing unit est un processeur.

GNU/Linux, est une famille de systèmes d'exploitation open source.

CentOS, est une distribution GNU/Linux destinée aux serveurs.

Asterisk, est un autocommutateur téléphonique.

GUI, graphical user interface est une interface graphique.

FreePBX, est une interface utilisateur graphique qui gère Asterisk.

Switch, est un équipement qui relie plusieurs segments dans un réseau informatique.

Firewall, ou pare-feu en français est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau.

SIP, Session Initiation Protocol est un protocole de communication standard.

Trunk SIP, en français « jonction SIP » est une technologie de voix sur protocole Internet.

SDA, sélection directe à l'arrivée est une technique en télécommunications qui permet d'atteindre directement un interlocuteur depuis l'extérieur.

LAN, Un réseau local, en anglais Local Area Network, est un réseau informatique.

VLAN, Virtual Local Area Network est un réseau local virtuel.

DMZ, Demilitarized Zone est une zone démilitarisée, un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet par un pare-feu.

Adresse MAC, parfois nommée adresse physique, est un identifiant stocké dans une carte réseau.

OUI, Organizationally Unique Identifier est un nombre de 24 bits assigné par l'IEEE. Ce numéro identifie un fabricant ou une organisation de façon unique dans une adresse MAC.

AD, Active Directory est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows.

RADIUS, est un protocole client-serveur permettant de centraliser des données d'authentification.

802.1X, est un standard lié à la sécurité des réseaux informatiques.

HTTPS, permet au visiteur de vérifier l'identité du site web auquel il accède, grâce à un certificat d'authentification émis par une autorité tierce, réputée fiable.

GPO, Group Policy Object permettent de centraliser la gestion des configurations des postes d’un domaine.

Log, désigne un historique d'événements.

Bibliographie

Aruba. (s.d.). *Forum pour les borne Wi-Fi*. Récupéré sur https://community.arubanetworks.com/community-learning

Asterisk. (s.d.). Récupéré sur Forum Asterisk: https://community.asterisk.org/

CentOS. (s.d.). Récupéré sur CentOS: https://www.centos.org/

Cisco. (s.d.). *Configuration du Voice Vlan sur switch cisco.* Récupéré sur https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_40_se/configuration/guide/scg/swvoip.pdf

FreePBX. (s.d.). Récupéré sur Forum FreePBX: https://www.freepbx.org/

Microsoft. (s.d.). *Forum Windows Serveur*. Récupéré sur https://social.technet.microsoft.com/Forums/fr-fr/home

StackOverflow. (s.d.). *Forum StackOverflow*. Récupéré sur https://stackoverflow.com/

VMWare. (s.d.). *Site VMWare ESXi*. Récupéré sur https://www.vmware.com/fr/products/esxi-and-esx.html