Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Découverte du monde de l'intégration réseaux et de services chez les clients Entreprise Orange

Louis DJADI

Orange France

Responsable entreprise : Philippe Gey

Responsable académique : Delphine Rousseau

2019

Table des matières

1 Introduction

Du 8 avril au 14 juin 2019, j'ai pu effectuer un stage au sein de l'entreprise Orange situé à l'impasse des Frères Pratesi, Aix-Jas de Bouffan, au service nommé Pôle Intégration Offres Complexes (PIOC). Tout au long de ce stage, j'ai pu découvrir le monde de l'intégration de services pour des clients entreprise.

Pour être initié à cet objectif de stage, j'ai dû remplir différentes missions que l'on m'a attribué en commençant tout d'abord par la réalisation d'une maquette réseau, que j'expliquerai plus en détail par la suite, ainsi que les différentes missions SAV Clients auxquelles j'ai pu assister mon tuteur M. Nicolas Fraisse.

En vue de rendre compte de manière fidèle les 2 mois passés au sein de la société Orange, ce rapport se divisera alors en 3 parties. Dans un premier temps, je présenterai l'entreprise et plus précisément le service dans lequel j'ai pu travailler. Dans un second temps, j'introduirai les différents SAV auxquelles j'ai participé. Et enfin, je présenterai le travail maquette que j'ai pu entreprendre tout au long de mon stage

2 Présentation entreprise et du service

a. Présentation entreprise Orange

Créée en 1994 dans un monde prédigital, la marque Orange est maintenant présente dans 29 pays et sert 250 millions de clients à travers le monde. En 2017, la marque Orange a été estimée à 21.5 milliards de dollars, se classant alors à la 51ème place des marques mondiales. Elle forme une communauté internationale de 153 000 personnes qui reflètent la diversité des marchés qu'elle sert.

Le secteur des technologies de l'information et de la Communication évolue en permanence nécessitant d'adapter les métiers et les compétences. Pour anticiper ces changements, Orange conduit une politique de Gestion Prévisionnelle de l'Emploi et des Compétences (GPEC) appropriée et prépare ainsi aux évolutions du secteur de manière responsable et durable.

En Europe, elle assure le déploiement de la 4G et de la Fibre avec 70% du chiffre d'affaires consolidé a été réalisé dans ce continent en 2016 dont 45% en France. Le nouvel objectif d'Orange est d'aménager une couverture 4G supérieure à 95%.En Afrique et Moyen-Orient, 1 africain sur 10 est un client Orange. C'est pour cela que Orange décide de lancée la 4G dans 10 pays africains et réalise un chiffre d'affaires de 5.2 milliards d'euros – soit une progression de 2.6% – en servant plus de 120 millions de clients.

Avec toute cette influence, Orange est l'un des principaux opérateurs européens du mobile et du fixe et l'un des leaders mondiaux des services de télécommunications aux entreprises. Le Groupe est présent auprès du grand public dans 29 pays et auprès des entreprises dans 220 pays et territoires. Chaque pays est responsable de ses résultats et du pilotage de son activité.

C'est la garantie d'avoir pour la France, l'organisation la mieux adaptée à ses clients, notamment pour répondre aux enjeux liés au réseau, dans un contexte de complexification de rôle d'opérateur.
Au 1er avril, cette organisation évolue pour consolider une vision au plus près du terrain, pour les clients et les salariés. 4 nouvelles Directions Orange (DO*) voient le jour en métropole : les DO Grand Ouest, Grand Nord-Est, Grand Sud-Est et Grand Sud-Ouest. Ici nous allons parler de la DOGSE* (Direction Orange Grand Sud-Ouest) et tous ses sous-services.

La DOGSE a pour mission d'être garante et intégratrice de la stratégie d'Orange sur l'ensemble de son territoire. A ce titre elle participe à l'élaboration de la stratégie nationale et aux orientations et projets qui en découlent, l'incarne et la met en œuvre localement.

En lien avec les directions Nationales, elle participe à la construction des stratégies business, clients et réseaux du territoire et est responsable de la performance d'Orange sur son territoire par le pilotage de l'activité et des entités qui lui sont rattachées, ainsi que de la gestion des ressources humaines, de l'emploi, de la communication, de la RSE*, de l'immobilier occupants, de la compliance et représente Orange sur le territoire. En termes de chiffres bruts, Vingt-trois départements et 3 grandes régions composent la nouvelle DO : Auvergne Rhône-Alpes, Provence Alpes-Côte d'Azur et la Corse.

Elle compte 13 500 000 habitants sur 121 000 km². Au total sur le territoire, ce sont 14 600 salariés des domaines réseaux, clients, SI, fonctions supports... qui portent les compétences nécessaires au bon fonctionnement des offres et services, au plus près des clients.

Dans la sous-direction de la DOGSE, nous avons la DIOCE* dans laquelle nous pouvons distinguer deux grandes missions. D'une part, le management des équipes intégration offres complexes pour l'UI* Est (techniciens, experts & RPI) ainsi qu'un rôle transverse pour améliorer la QSE en qualité de Référent B2B* pour la DO Est.

L'intégration complexe correspond aux différentes solutions qui associent plusieurs briques techniques (voix, data ou sécurité), dans des environnements clients très variés (multisites, multi-utilisateurs comme les hôpitaux ou les réseaux bancaires). On parle souvent d'OSM (Offre Sur Mesure).

La création de ce département fait partie de la stratégie UI 2019. Ces départements doivent permettre de répondre à un des enjeux du domaine qui est d'accompagner les clients Entreprises dans leur transformation Digitale. Le DIOCE travaille avec l'ensemble des forces de vente Entreprise du Groupe Orange, que ce soit OBS et ses filiales (OCWS par ex) ainsi que la Direction Entreprise France (DEF). Ces entités sont en charge de vendre des offres pour lesquelles les employés du DIOCE assurent le déploiement et/ou le contrat d'entretien.

Le département s'inscrit à de nouveaux enjeux en créant une dynamique et un collectif pour que les personnes qui composent ce nouveau département se connaissent mieux et travaillent toujours mieux ensemble. Ensuite, le principal enjeu est l'amélioration de notre QS Entreprise, avec de nombreux sujets comme le pilotage, les délais, les compétences et in fine le développement du chiffre d'affaires.

Orange dirige toute la partie client entreprise par l'infrastructure OBS (Orange Business Services). OBS se divise alors en plusieurs secteurs d'activités tels que la DGC*, la RPI*, OCB*, etc ; mais surtout le secteur dans lequel j'ai pu travailler, apprendre et perfectionner mes compétences : le Pôle Intégration Offres Complexes (PIOC).

b. Pôle Intégration Offres Complexes

Le Pôle Intégration Offres Complexes est, comme son nom l'indique, un service d'intégration et d'implémentation d'infrastructures réseau au sein d'un ou plusieurs bâtiment(s) client entreprise. Elle compte 12 techniciens à son service et propose alors différentes offres au client.

Cependant, ce service comprend que la partie technique de l'intervention. En effet, une affaire client passe de service en service jusqu'à arriver dans les mains du technicien.

Tout d'abord, le client crée une demande d'offre chez Orange, l'affaire est alors créée et vendue chez les commerciaux (AERM, AESOM pro et DGC). Après une période d'accord administrative, le dossier est implémenté dans l'emploi du temps en ligne Orange nommé « LISA ».

Il est désigné alors sur cet emploi du temps à qui revient le dossier et à quels créneaux horaires le technicien doit intervenir dans la semaine. A la fin de sa tâche accomplie, le technicien fait alors signer un PV* au client attestant bien de la main-d'œuvre effectuée dans la journée.

3 Les différentes missions abordées

a. SAV client entreprise

L'une des premières missions incombé au technicien est bien le SAV. Un client chez Orange, lorsqu'il signe un contrat pour sa nouvelle installation réseau, à accès durant un nombre d'années déterminé par son contrat au contact du service technique lorsque son réseau tombe en panne.

Un technicien doit alors venir dans les délais les plus courts possible pour assister le client, analyser le problème, dépanner dans le cas où ce problème est bien du ressort du technicien et enfin donner un bilan de la main-d'œuvre effectué avec, si possible, un avis sur l'amélioration de l'architecture réseau dans l'avenir ou encore des conseils de gestion du local technique réseau.

Par exemple, durant une journée de mon stage, nous avons pu voir le cas de l'entreprise BCA expertise qui, lorsque nous sommes arrivées, avait un commutateur qui tombait en panne.

Nous avons donc dû réagir en conséquence en installant un nouveau commutateur en bon état en adaptant la configuration à celle de la topologie réseau effective. De plus, nous avons réorganisé le brassage des câbles afin d'avoir une meilleure ergonomie et accessibilité aux différents équipements du local technique.

b. L'Intégration réseau

Cette 2ème partie du métier consiste donc à l'intégration complète d'une infrastructure réseau chez un client. Après demande et reçu de tout l'équipement nécessaire à la mission, le technicien PIOC va alors se rendre directement chez le client pour une installation complète de son réseau.

Cela peut passer de petites installations pour des PME et dont l'intégration peut se faire en moins de quelques semaines, mais aussi pour de grandes entreprises avec des réseaux qui doivent alors se connecter en multisites pour plusieurs bâtiments de l'entreprise par exemple.
Dans ces cas-là, l'intégration peut prendre des mois avant la finition.

Pour citer un exemple d'intégration chez une PME, je vais décrire l'architecture réseaux que nous devions installer mon tuteur et moi chez l'entreprise restaurant BALADI. Il nous a été demandé l'installation de 2 commutateurs, 2 bornes Wifi et d'un firewall de la marque constructeur Fortinet.

L'objectif de cette mission était alors de couvrir l'intégralité du terrain BALADI (restaurant salle intérieure et terrasses) à leur réseau internet. Nous avions donc fixé de manière stratégique les 2 bornes Wifi dans le restaurant pour établir un recouvrement total de la zone demandé.
De plus, nous avons configuré le firewall pour renforcer la sécurité du réseau interne pour éviter toute intrusion de malfaiteurs dans le réseau.

c. Les études

Une étude conduite par un technicien correspond à une analyse complète d'une future infrastructure réseau au sein d'une entreprise. Le technicien aura alors pour objectif de tester par des matérielles d'émetteurs Wifi et DECT combien de bornes devra-t-il installer, dans quelle position, à quel endroit précis dans le bâtiment. Il devra prévoir et demander en conséquence l'installation de prise murale Ethernet au client en cas de besoin voire même l'installation de prise électriques.

On distingue principalement 2 types d'étude au sein du service PIOC :

- L'étude de **couverture Wifi** : correspond donc à l'étude du recouvrement signal radio Wifi dans les zones concernées
- L'étude de **couverture DECT*** : correspond à la couverture signal radio d'un téléphone DECT sans fil dans une zone spécifié par le client.

Le technicien doit alors, lorsqu'il a fini l'analyse complète de son étude chez le client, rédiger un rapport d'étude dans lequel il fera une description de l'état des lieux, des photos des locaux de l'entreprise avec les emplacements des futures bornes DECT et/ou Wifi ainsi que les différentes modifications que doit ajouter le client (comme les prises murales par exemple).

4 Travail maquette réalisé

Durant ces 10 semaines, j'ai pu, comme nous avons pu le voir, d'abord découvrir les différentes tâches qui occupent le service en passant de l'intégration complète d'une infrastructure réseau chez le client au SAV pour régler toute panne d'un équipement, d'une configuration d'équipement réseau ou juste de câblages.

Cependant, j'ai aussi pu perfectionner mes compétences techniques dans le domaine de l'architecture réseau. En effet, j'ai pu travailler à la création d'une maquette réseau dont l'objectif était dans un 1er temps me faire découvrir et m'adapter à de nouveaux équipements auxquelles je n'avais jamais été confronté et dans un second temps de pouvoir gérer une mini infrastructure réseau en autonomie pour la conception, la recherche de documentation technique et la résolution des différents problèmes rencontrés.

C'est pour cela que pour parfaire au maximum mes compétences techniques, j'ai dû travailler avec plusieurs équipements de marques et modèles différents. De plus, la maquette que l'on m'a alors proposé de faire s'adapte dans un contexte d'intégration chez un client d'une PME* par exemple.
Sur le « schéma maquette réseau » (annexe 2), nous pouvons voir l'utilisation de différents équipements réseaux. Je vais donc dans un premier temps vous faire découvrir les commutateurs utilisés, leur modèle et leur configuration. Puis dans un second temps je vais vous décrire la borne Wi-Fi utilisée et la configuration abordée dans cette maquette. Enfin je vous présenterai le firewall utilisé, le choix du modèle abordé et sa configuration complète.

a. L'interconnexion réseau : les commutateurs Alcatel

i. Switch Alcatel OS6350-P24.

Figure 1 Switch Alcatel OS6350-P24

L'Alcatel-Lucent OmniSwitch 6350 peut créer et gérer les réseaux de petites/moyennes entreprises. Les capacités réseaux de l'OmniSwitch inclut la sécurité avancée, la QOS* et fonctionnalités de haute disponibilité pour les données client, voix et sans fil de classe affaires les technologies. Ces commutateurs sont simples à déployer, configurer et gérer. Il offre d'excellentes performances pour les applications à bande passante élevée tout en consommant très peu d'énergie. Dotée des toutes dernières innovations technologiques, la gamme de commutateur OmniSwitch 6350 contribue également à la protection des investissements clients pour l'avenir, grâce à un choix d'options flexibles de mise à niveau.

ii. Switch Alcatel OS6450-P24

Figure 2 Switch Alcatel OS6450-P24

L'Omniswitch 6450 incite un design optimisé pour la flexibilité, l'évolutivité et la faible consommation d'énergie. Il utilise le système d'exploitation AOS pour fournir un réseau hautement disponible, sécurisé, auto protecteur, facile à gérer et enfin respectueux de l'environnement.
Il est utilisé principalement pour des types de déploiement tel que des groupes de travail entreprises, des applications de services résidentielles et gérées commercialement ou encore par des fournisseurs de service.

iii. Configuration

Pour la partie configuration, mon but était de créer une configuration simple de réalisation tout en appuyant sur l'aspect sécurité de l'architecture réseau.

J'ai donc d'abord commencé par créer des VLAN* que nous allons utiliser pour séparer les différents réseaux. Le VLAN a pour objectif la non-intercommunications entre les différents réseaux qui parcours l'infrastructure permettant une meilleure sécurité.

A noter que tout au long du rapport j'appellerai Switch1 en tant que switch Alcatel OS6350-P24 et le Switch2 en tant que switch Alcatel OS6450-P24 de la maquette.

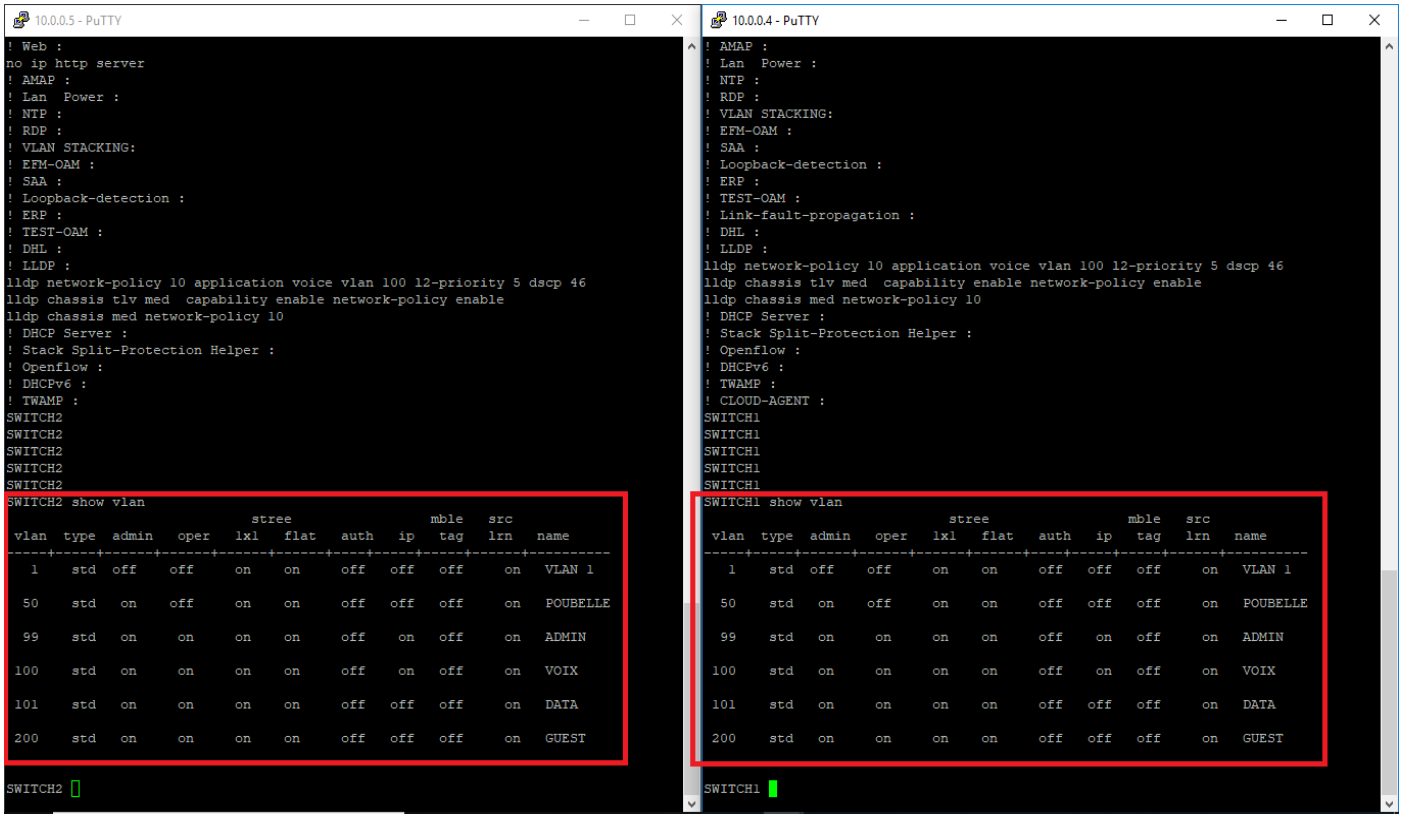


Figure 3 liste des VLAN créer sur Switch1 et Switch2

Nous pouvons voir alors très distinctement 6 VLAN différents :

- **Le VLAN 1** correspondant au VLAN créer par défaut dans un switch en configuration-+usine de base
- **Le VLAN 50** nommé VLAN « Poubelle » est le VLAN sur lequel il n'y est rattaché aucun réseau apparent. Cela permet de couper/éteindre (shutdown) les ports qui ne sont pas utiles dans notre architecture et renforce l'aspect sécurité permettant de ne pas accéder au réseau ou à la configuration présente dans le switch
- **Le VLAN 99** correspondant au VLAN ADMIN et qui a pour but de pouvoir configurer toute l'architecture réseau en se connectant au réseau ADMIN. Il est donc à accès restreint que pour le/les administrateur(s) réseau(x) occupant. Il est dans le réseau 10.0.0.0/24
- **Le VLAN 100** correspond au VLAN VOIX. C'est donc sur le réseau 172.16.1.0/24 que les téléphones pourront communiquer entre eux.
- **Le VLAN 101** correspond au VLAN DATA. Le réseau 192.168.24.0/24 permet à tous les périphériques PC connecté directement au switch d'accéder à internet via une connexion à la Livebox.
- **Le VLAN 200** correspond au VLAN GUEST. C'est le réseau Wifi utilisé pour les visiteurs d'une entreprise par exemple.

Après avoir créé les VLANs, nous devons les configurer sur les interfaces utilisées. On doit donc tout d'abord configurer un lien LACP* connectant le Switch1 au Switch2. Un lien LACP est un protocole standardisé implémenté par différents constructeurs. Il permet de contrôler le groupement de plusieurs ports physiques en un canal logique de communication. Ici, nous allons regrouper 2 ports physiques par switch entre eux dans un groupement LACP.

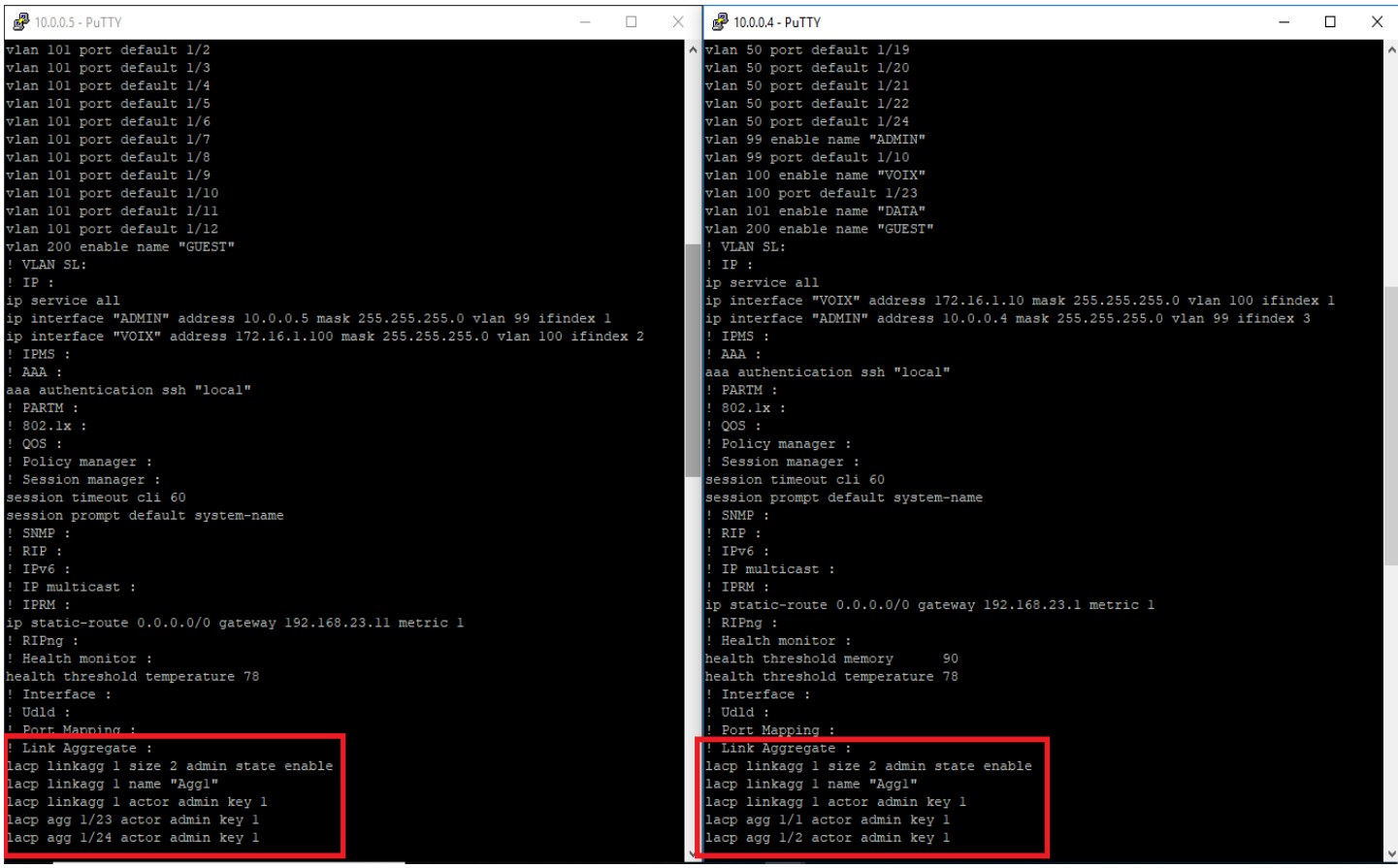


Figure 4 Configuration LACP

Pour la configuration, j'ai, comme nous pouvons le voir, d'abord créé un groupe « linkagg » (agrégat de liens) numéroté 1. Dans ce groupe, que je nomme « Agg1 », j'intègre les interfaces 23 et 24 du Switch2 et les interfaces 1 et 2 du Switch1. Je leur attribue la même admin key numéroté 1 pour que lien s'initialise entre les 4 interfaces. Une des deux interfaces sur chaque switch aura alors pour statut « interface primaire », elle aura pour rôle d'être utilisée en priorité pour le trafic entre les deux switchs. L'autre interface s'affichera en « interface secondaire » et assurera donc une redondance dans le cas d'une panne de la première interface.

De plus, j'établis une connexion SSH dans laquelle je pourrai me connecter à distance (via l'adresse ip interface ADMIN 10.0.0.5 pour Switch2 et 10.0.0.4 pour Switch1) à l'interface console du Switch. L'administrateur réseau pourra alors juste en se connectant au réseau Wifi configurer les Switchs ou réparer les pannes présentes sur le réseau.

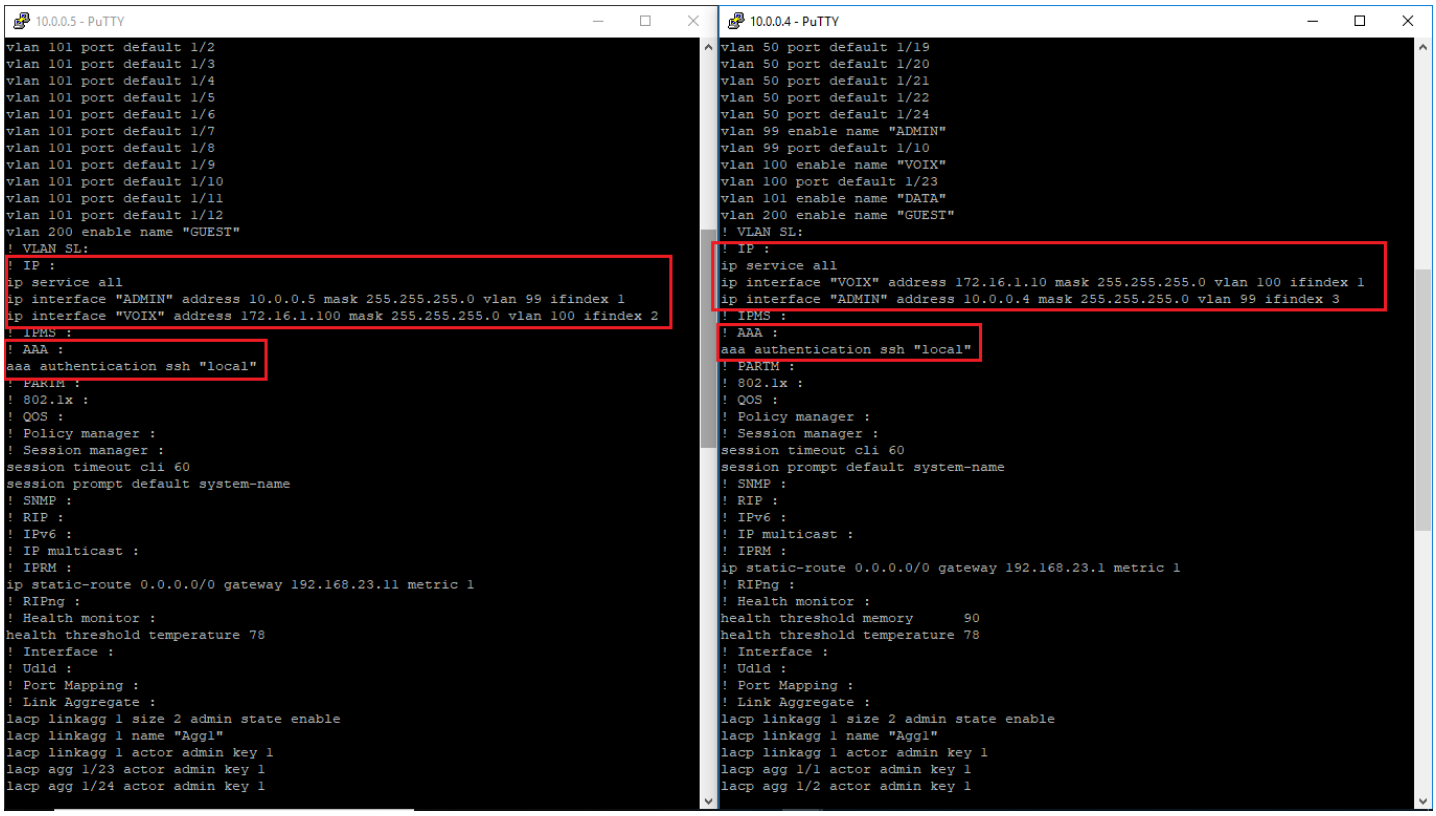
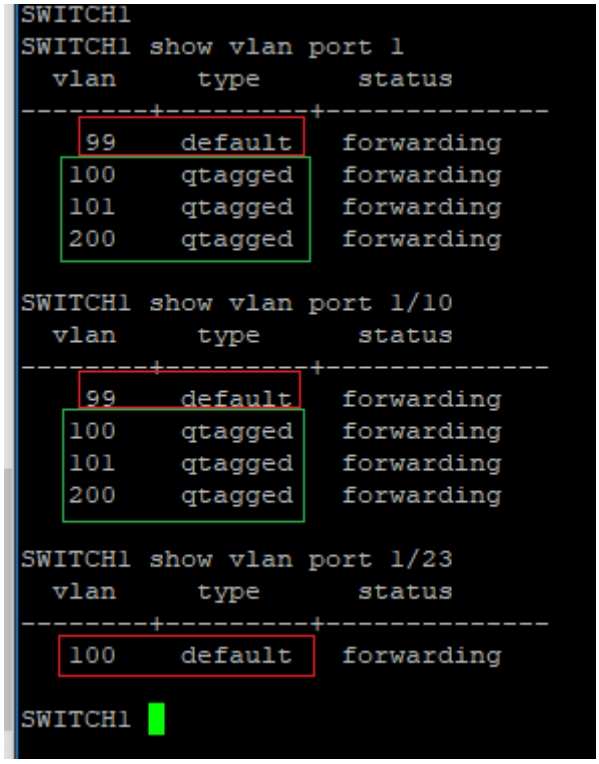


Figure 5 Création ip interfaces et accès SSH

Maintenant que la partie gestion interfaces est terminée, il faut affecter les VLANs aux différentes interfaces du Switch souhaité. Nous allons ici nous concentrer principalement sur les interfaces utilisées et importantes dans la maquette.



Le Switch1 sur la maquette réseau correspond principalement à l'accès DATA et VOIX de l'architecture. On peut donc dénombrer 3 ports utilisés :

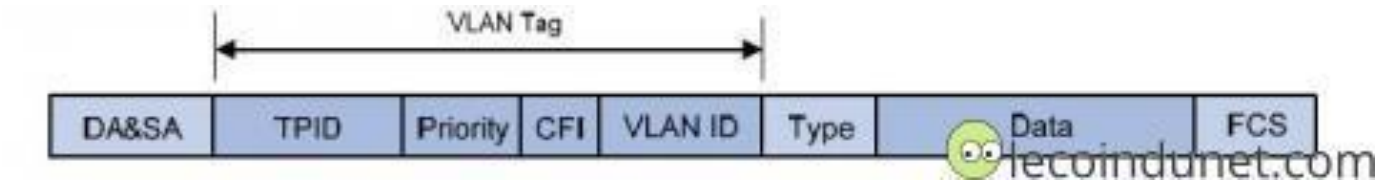
- Le port 1 : correspond au groupe d'aggrégation LACP numéroté 1 comme vu précédemment.
- Le port 1/10 : correspond à l'interface qui distribue la DATA dans l'infrastructure. Elle est connecté au Firewall Stormshield (dont on décrira plus en détails plus tard) qui elle-même est connectée à la Livebox Orange donnant l'accès internet.
- Le port 1/23 : correspond à l'interface connecté à l'IPBX qui fournit le réseau VOIX. Il permet les échanges par téléphone IP et, si évolution, les appels en extérieur.

On peut voir deux types de VLAN sur les interfaces : le type « default » ou port défaut/non taggué (encadré en rouge sur la figure) et le type « qtagged » ou port taggué (encadré en vert).

- Le port defaut/non taggué correspond à l'insertion d'un vlan défini par l'administrateur réseau en tant que vlan par défaut de l'interface. Le port est donc non taggué et si un PC est branché directement sur cette interface, il accèdera au réseau VLAN par défaut. Par exemple, pour

l'interface 1/10, c'est le réseau VLAN ADMIN qui est configuré par défaut sur l'interface. En effet l'interface étant connecté au firewall, cela permettra à l'administrateur d'accéder à la page de configuration facilement (dont on verra plus en détail la configuration dans la partie firewall). On utilisera le port défaut principalement pour le VLAN 101 pour l'utilisateur, car les ordinateurs ne sont pas en mesure d'identifier les paquets Ethernets et donc d'identifier le VLAN correspondant.

- Le port taggué ou « qtagged » signifie que la trame Ethernet échangée dans le réseau contient un numéro « taggué » pour être identifiée dans un VLAN. L'équipement destinataire (switch, borne WiFi, etc…) pourra alors reconnaître l'appartenance à son VLAN et rediriger correctement le trafic. S'il n'est pas reconnu, le trafic est supprimé.



Sur le Switch1, j'ai donc décidé de mettre le VLAN 99 par défaut et tous les autres en taggués pour l'interface 1/10 et le groupe d'agrégation 1. Cela permettait principalement de pouvoir identifier plus simplement les différents réseaux lors de la configuration du firewall que nous verrons plus tard.

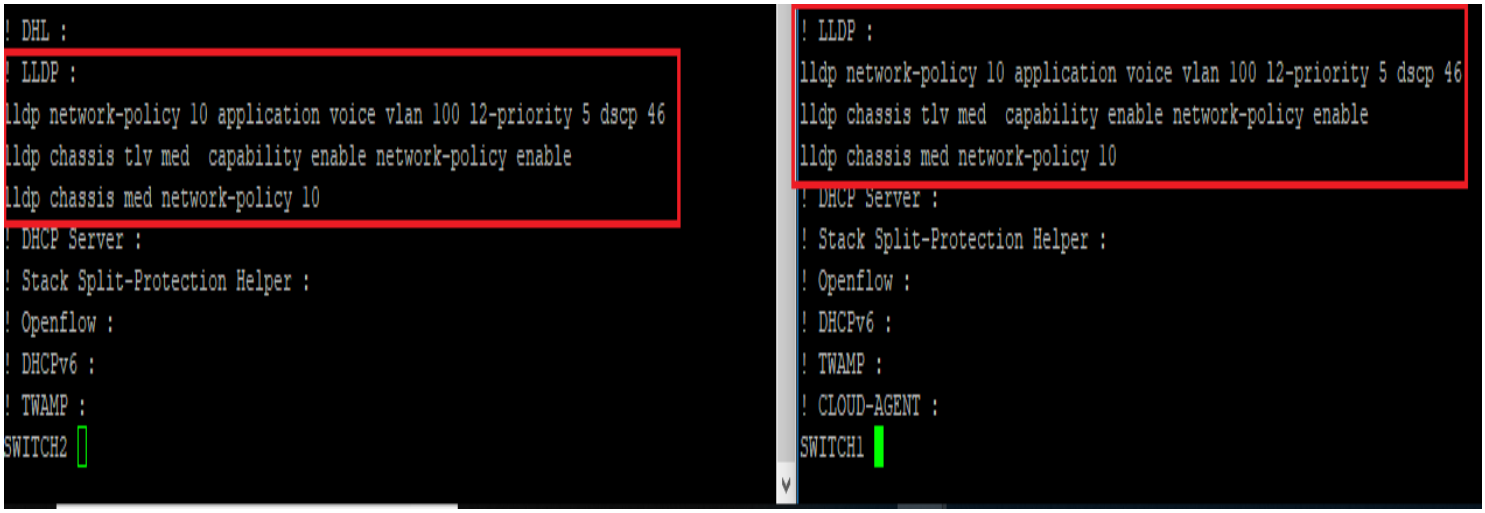
```
SWITCH2 show vlan port 1/1
  vlan      type       status
--------+---------+--------------
   100     qtagged    forwarding
   101     default    forwarding

SWITCH2 show vlan port 1/13
  vlan      type       status
--------+---------+--------------
    99     default    forwarding
   101     qtagged    forwarding
   200     qtagged    forwarding

SWITCH2 show vlan port 1
  vlan      type       status
--------+---------+--------------
    99     default    forwarding
   100     qtagged    forwarding
   101     qtagged    forwarding
   200     qtagged    forwarding

SWITCH2
```

Le Switch2 sur la maquette réseau correspond principalement à la partie accès WiFi ainsi que la connexion directe câblée Ethernet. On dénombre donc encore 3 ports configurés :

- Le port 1/1 qui est une interface sur laquelle est branché un téléphone IP lui-même connecté à un ordinateur. Cette configuration permet alors de faire marcher à la fois le téléphone IP mais aussi donner l'accès à internet pour l'ordinateur. On peut même imaginer une intercommunication entre les 2 réseaux dans l'avenir.
- Le port 1/13 correspondant à la borne WiFi sur laquelle on pourra accéder à 3 réseaux différents : ADMIN, DATA et GUEST.
- Le groupe d'agrégation LACP (port 1) faisant l'interconnexion entre les 2 switchs.
- A noter que pour les ports non utilisés ont été configuré manuellement au VLAN 50 port défaut correspondant au VLAN POUBELLE.

L'objectif de cette configuration permet alors de différencier plusieurs réseaux au sein même d'une interface du switch. C'est pour cela que le téléphone IP de bureau et l'ordinateur peuvent fonctionner correctement en étant connecté à une même interface.

Enfin pour faire fonctionner correctement le réseau VOIX de la maquette, j'ai dû configurer un protocole LLDP* et le faire fonctionner sur mon téléphone IP.



LLDP est un protocole servant à la découverte des topologies réseaux de proche en proche, mais aussi à apporter des mécanismes d'échanges d'informations entre équipements réseaux et utilisateurs finaux.
C'est un protocole qui s'est imposer comme le protocole indispensable car non propriétaires donc libre d'utilisations pour tous les constructeurs (contrairement à des protocoles propriétaires tel que Cisco CDP, Extreme EDP, etc…).

Il permet alors de meilleurs échanges entre les équipements des différents constructeurs au sein même d'une infrastructure réseau LAN*.

La configuration se passe en plusieurs étapes :

- Pour se faire, j'ai créé une « network policy » c'est-à-dire une politique réseau dans laquelle on va intégrer le VLAN 100.
- Je configure une priorité par défaut de 5. Elle n'est pas importante par rapport à la taille de notre maquette.
- J'active la network-policy manuellement et la rend par défaut dans le switch.

Maintenant, lorsqu'un téléphone IP sera branché sur une interface disponible et tagguée au VLAN 100 « VOIX », une adresse sera distribué par le DHCP du firewall Stormshield, sans même devoir configuré le téléphone.

Maintenant que la partie Switch est configurée complètement, nous devons créer un accès distant aux réseaux. Pour se faire, nous utilisons un nouvel équipement qui va baser notre 2ème partie de la maquette : la borne WiFi Alcatel-Lucent.

b. La borne Wifi Alcatel-Lucent

i. Borne Wifi Alcatel-Lucent OmniAccess AP1101

Le modèle multifonctionnel AP1101 OmniAccess® Stellar d'Alcatel-Lucent est un point d'accès (AP*) d'entrée de gamme pour les déploiements en entreprise de petite et moyenne taille.
Le point d'accès Wi-Fi intérieur AP1101 OmniAccess offre un haut débit et une expérience utilisateur fluide.

Il est idéal pour les entreprises de toute taille nécessitant une solution sans fil simple, sécurisée et évolutive. L'AP1101 OmniAccess comprend une technologie WLAN avancée avec un réglage dynamique des ondes RF, une architecture Wi-Fi à contrôle distribué et un contrôle d'admission de réseau sécurisé avec accès unifié. L'AP1101 OmniAccess fonctionne dans une architecture de clusters entièrement redondante pour fournir des déploiements simplifiés Plug-and-play.
Le Plug-and-Play signifie qu'elle s'initialise automatiquement et possède une configuration de base permettant l'accès Wifi sans même une configuration avancée (même s'il est bien sûr conseillé de configurer pour une meilleure sécurité réseau).

Le cluster de points d'accès est un système autonome comprenant un groupe de points d'accès AP1101 OmniAccess et un contrôleur virtuel, qui est le point d'accès sélectionné pour la gestion du cluster. Un cluster d'AP comprenant uniquement le modèle AP1101 peut s'étendre jusqu'à 32 points d'accès. Le cluster d'AP peut également s'étendre jusqu'à 64 points d'accès en cas de combinaison avec d'autres modèles d'AP.

La borne est composée d'un port Ethernet, d'un port de configuration console et un port prise secteur pour alimenter la borne.
Cependant, le Switch Alcatel OS6450-P24 étant effective en PoE, la borne pourra fonctionner sans alimentation mais juste avec un câble Ethernet branché.

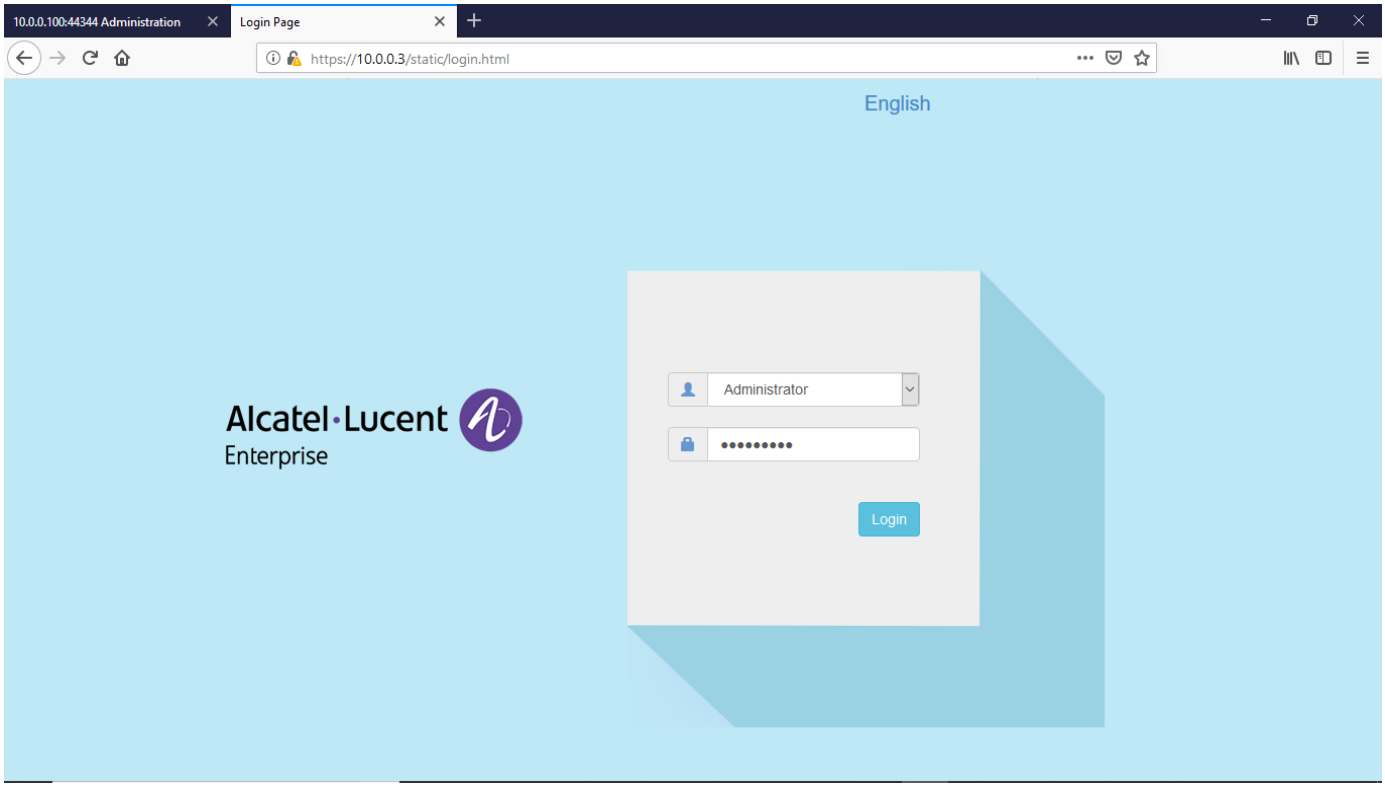
Le PoE permet de faire passer une alimentation électrique en même temps qu'un réseau internet dans les câbles. Il permet alors une alimentation de différents équipements tel que le Téléphone IP, des disques durs réseaux, des imprimantes, des caméras IP ou comme dans notre cas : une borne Wifi.

ii. Configuration

La borne Wifi à pour but dans notre maquette un accès réseau distant ouvert au public. J'ai donc distingué 3 catégories d'utilisateurs en supposant l'utilisation du Wifi dans un PME classique :

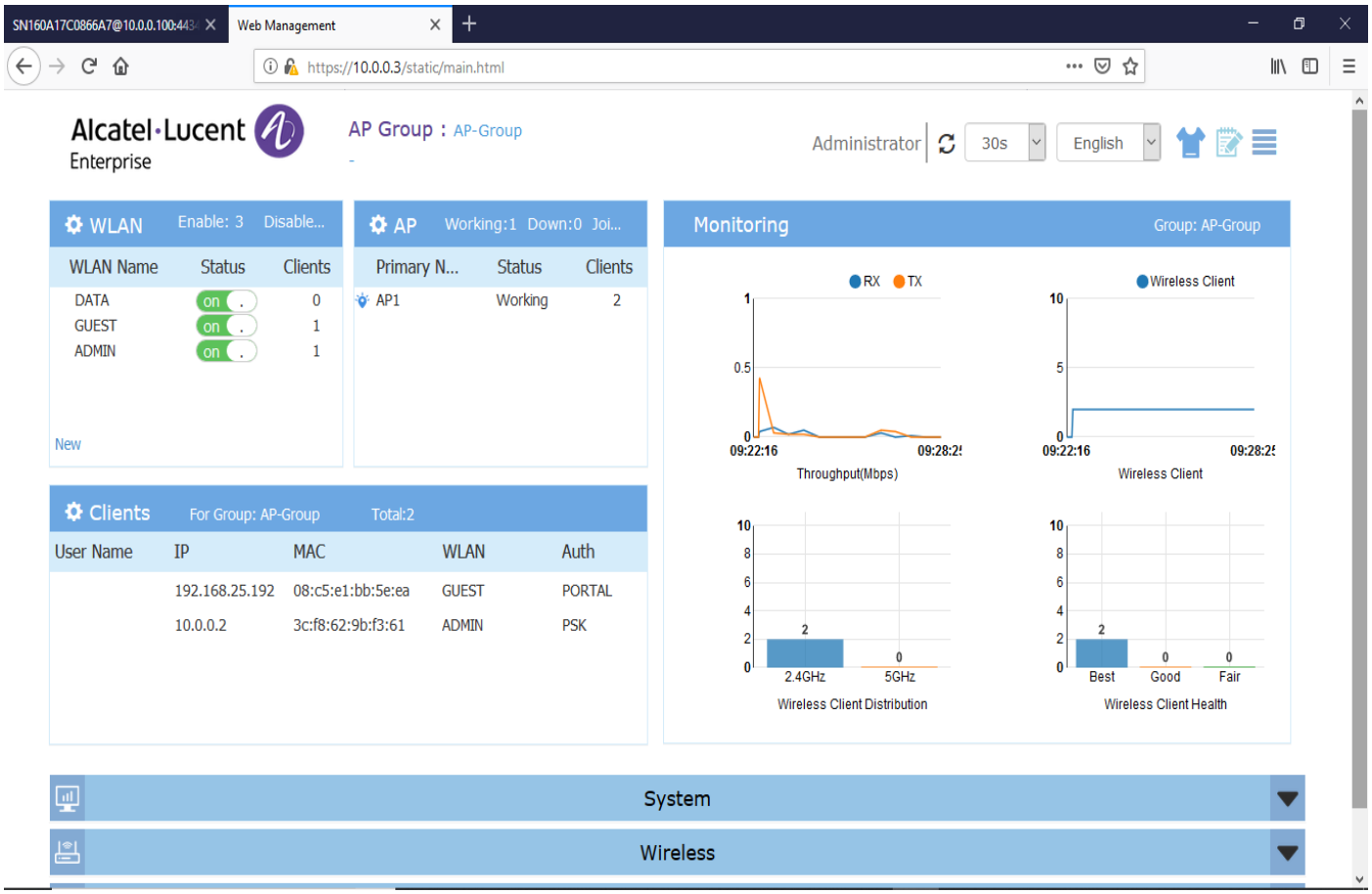
- Les employés de l'entreprise qui peuvent y accéder via un mot de passe distribué uniquement pour eux. Ils pourront alors se connecter vers internet, mais aussi vers les différents services auxquelles ils ont accès dans le réseau interne
- Les visiteurs de l'entreprise qui pourront accéder à un réseau ouvert sans mot de passe mais dans lequel ils auront des accès restreints.
- Le ou les administrateur(s) réseaux de l'entreprise qui auront accès à l'intégrale configuration du réseau interne du bâtiment. Ils pourront alors en cas de panne accéder à distance depuis n'importe où dans le bâtiment.

Mon objectif sera donc de créer plusieurs SSID* dans l'entreprise pour bien séparer les différents utilisateurs dans l'entreprise. Je commence donc la configuration par une connexion en http sur un navigateur à l'adresse https://10.0.0.3/static/login.html :



Je me connecte en tant qu'utilisateur « Administrator » puis je rentre le mot de passe que j'ai déjà configuré dans la borne.

Après cette étape, je rentre alors dans une nouvelle page de management de la borne que l'on peut voir ci-après :

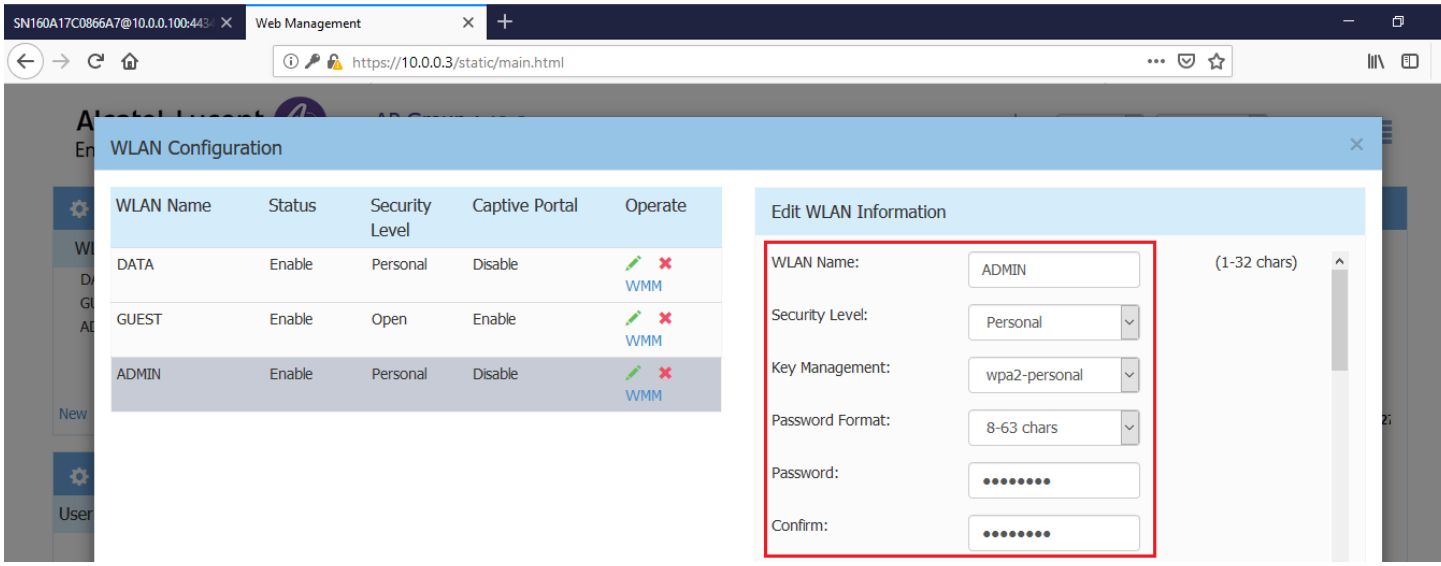


On peut distinguer alors sur la gauche de la page 3 éléments de configuration : WLAN*, AP et Clients.

L'onglet AP correspond à la configuration des paramètres réseaux et physique de la borne Wifi. C'est dans cet onglet que l'on peut alors configurer l'adresse IP statique de l'AP mais aussi créer d'autres AP ou encore renommé la borne

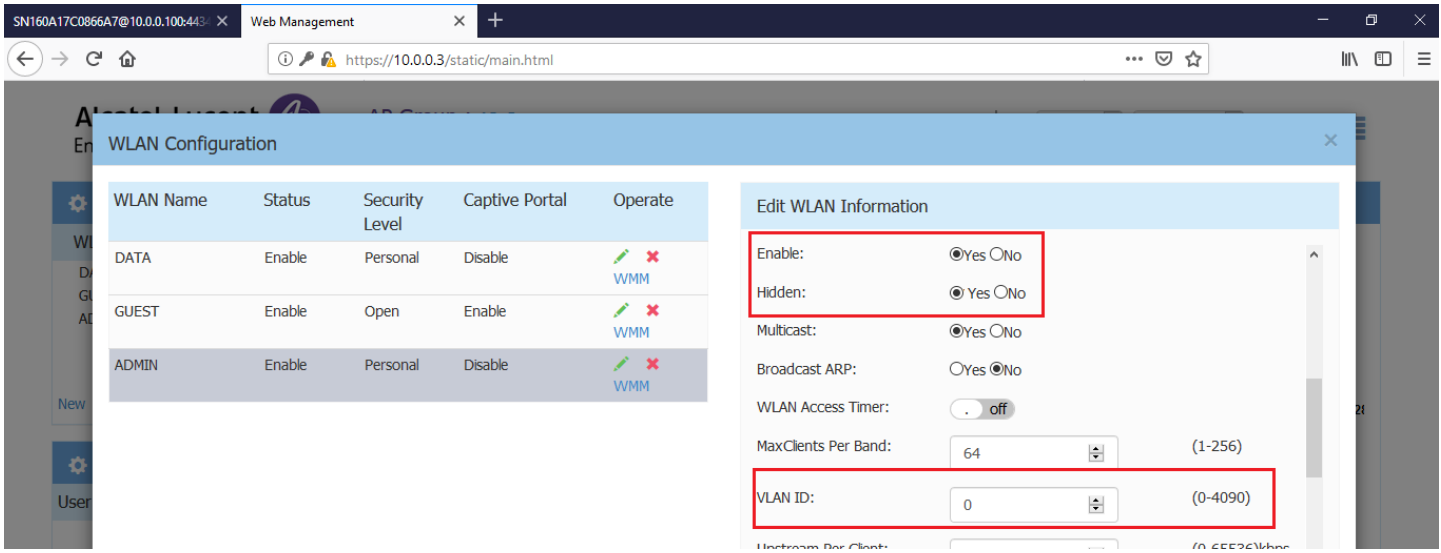
L'onglet Clients correspond à un outil de management des différents périphériques connectés à la borne. On peut distinguer l'adresse IP qui l'a obtenu par le DHCP du Firewall, son adresse MAC* (l'adresse physique et unique d'un périphérique tel qu'un smartphone, un PC ou encore une imprimante) et dans quel WLAN il est connecté.

Enfin nous avons l'onglet WLAN dans lequel nous pouvons créer différents SSID et les paramétrer différemment. Ici, j'ai décidé de créer 3 SSID nommés respectivement DATA, GUEST et ADMIN. Dans la suite, je vais donc présenter les différentes particularités que compose ses SSID.



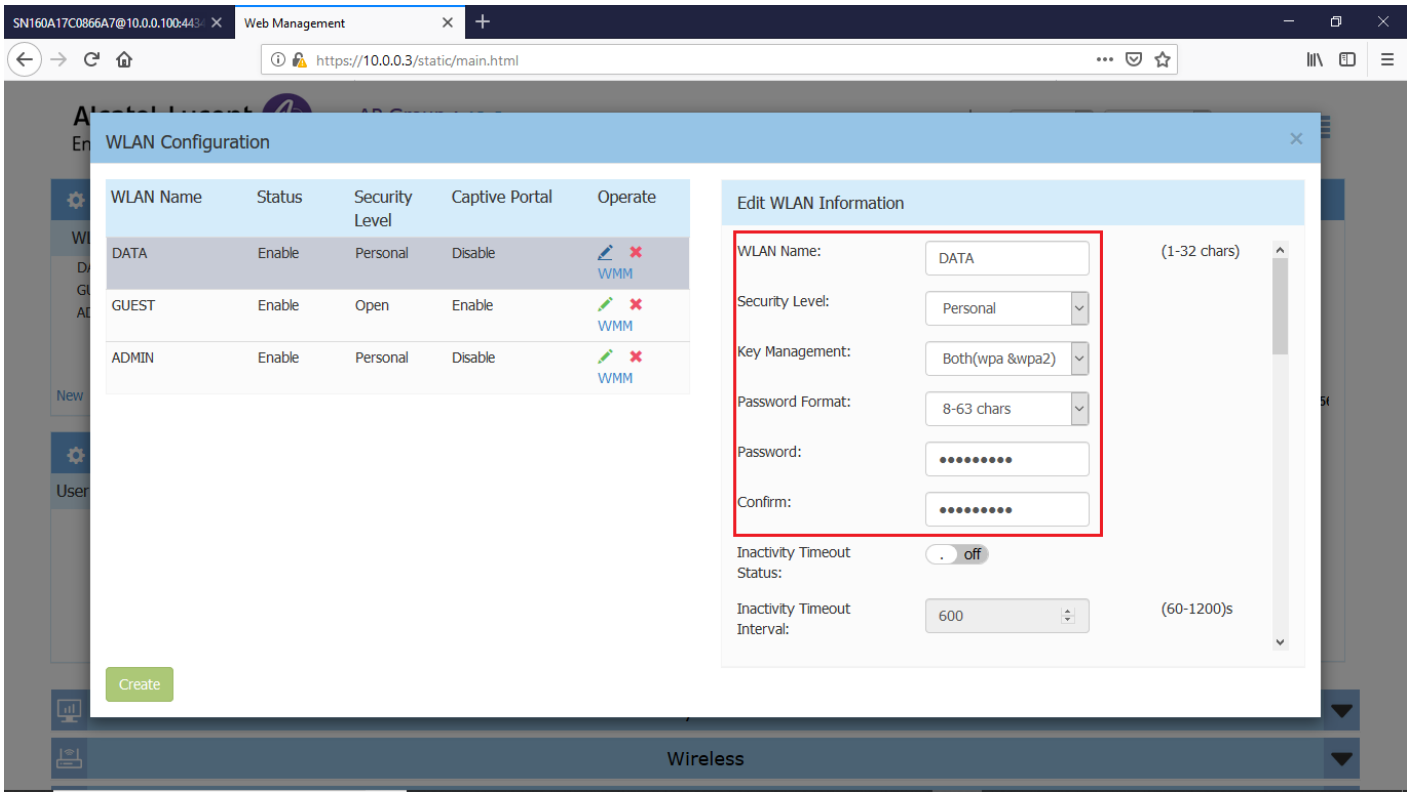
1. Le VLAN ADMIN est le plus important de la configuration de la borne. Comme nous pouvons le voir, je décide d'appeler ce SSID ADMIN. Pour renforcer la sécurité, je configure un mot de passe par clef WPA2-personal.

   La WPA2 est un mécanisme Wifi utilisé pour sécuriser les réseaux sans-fil. Il remplace le WEP qui est devenu dans les années 2000 beaucoup trop sensible aux hackers et donc moins sécurisé.

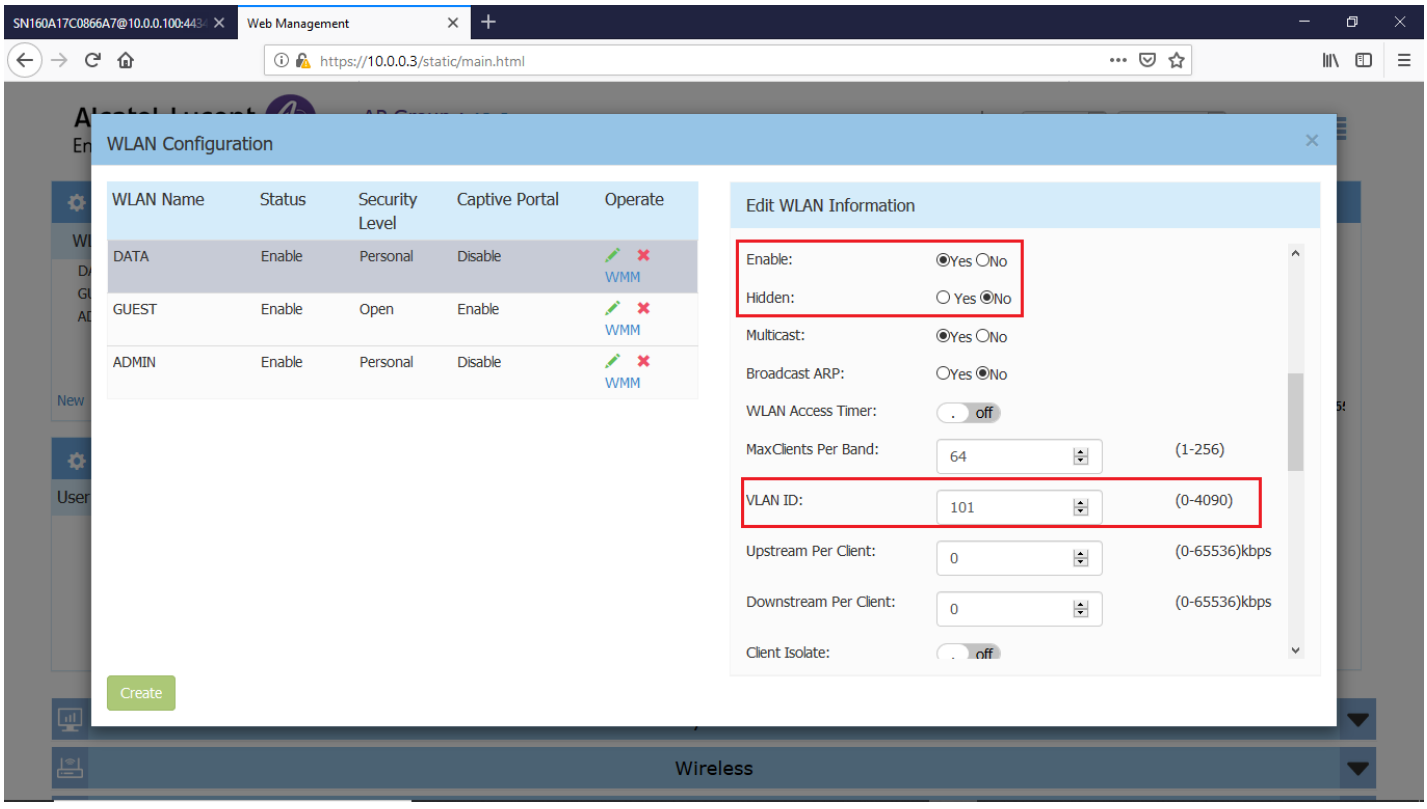


Pour renforcer l'aspect sécurité, je décide de cacher le SSID de façon que personne ne puisse le découvrir sans connaître le nom exact du SSID. Cela permet alors une nouvelle barrière de sécurité contre les « apprentis hackers » qui pourraient décider à tout moment de vouloir rentrer dans le réseau ADMIN.

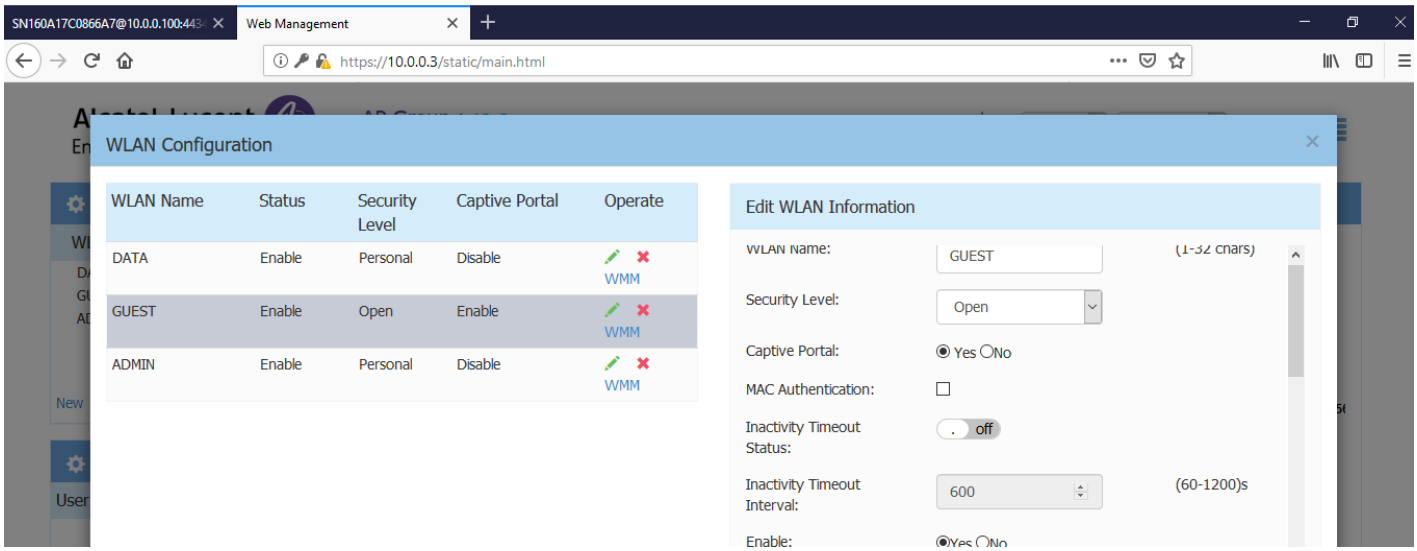
Nous pouvons remarquer que je n'ai pas configurer le numéro de VLAN au numéro 99. Cela est tout à fait normal puisque, comme nous l'avons sur la configuration du Switch2 précédemment, l'interface à laquelle est connecté la borne à pour VLAN par défaut le VLAN 99 « ADMIN ».
Etant par défaut et donc non taggué, la borne découvrira automatiquement le réseau ADMIN rattaché.



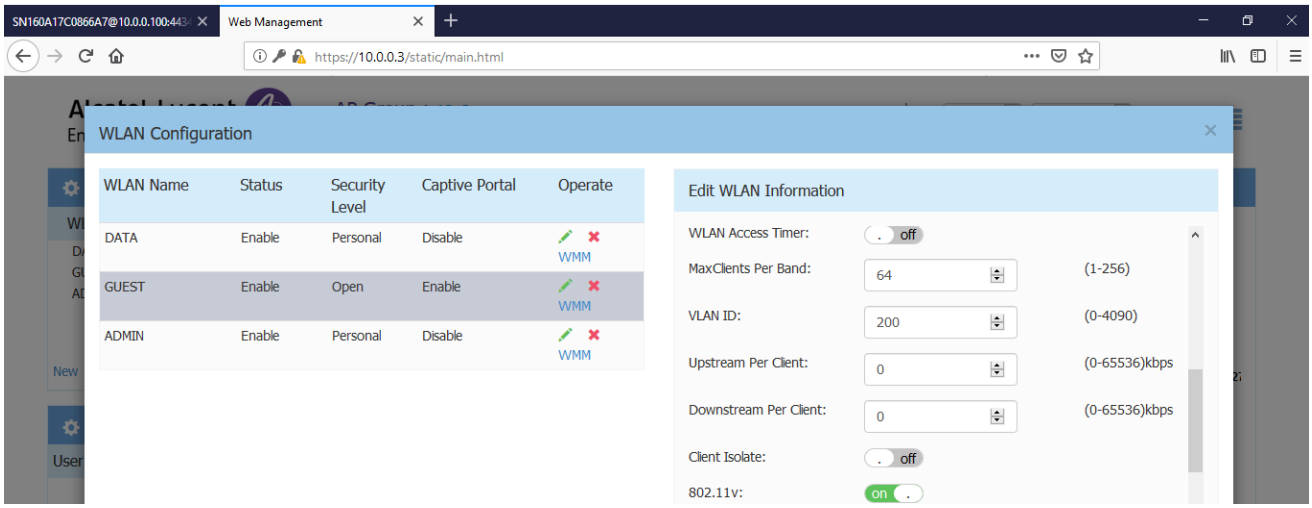
2. Pour le 2ème SSID, je le nomme DATA et je lui configure à lui aussi un mot de passe en WPA2. C'est un réseau auxquelles les visiteurs ne doivent pas avoir accès, il est donc indispensable de le sécuriser.



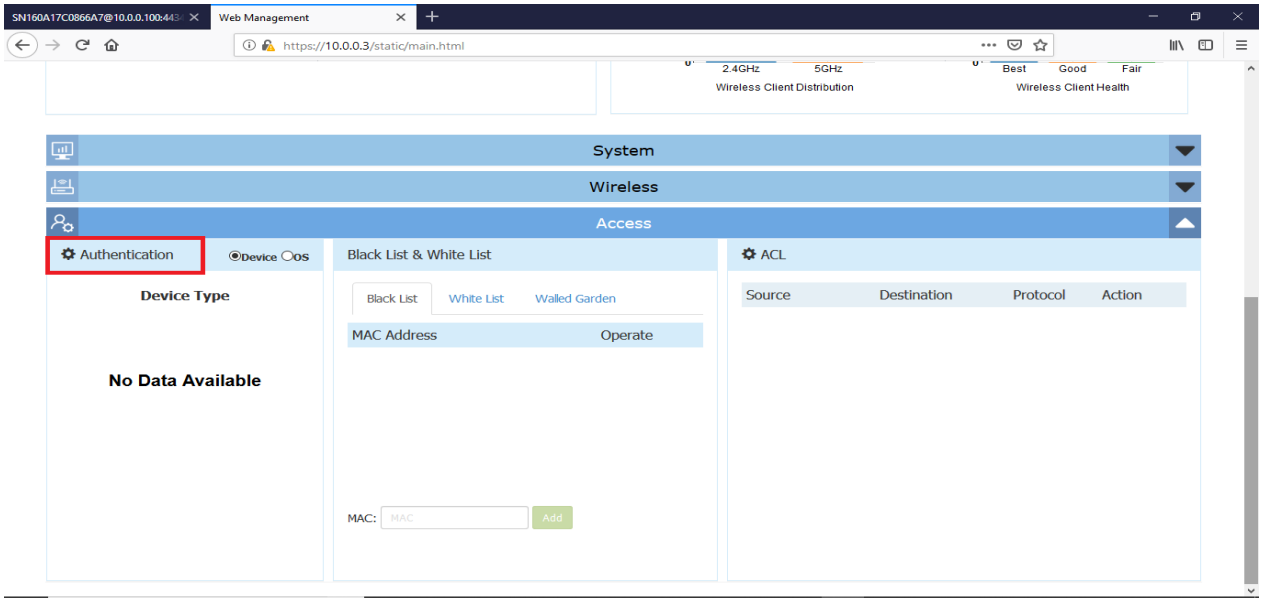
Je l'active, le rend visible pour tous les appareils et lui configure le VLAN ID 101 correspondant au VLAN DATA.



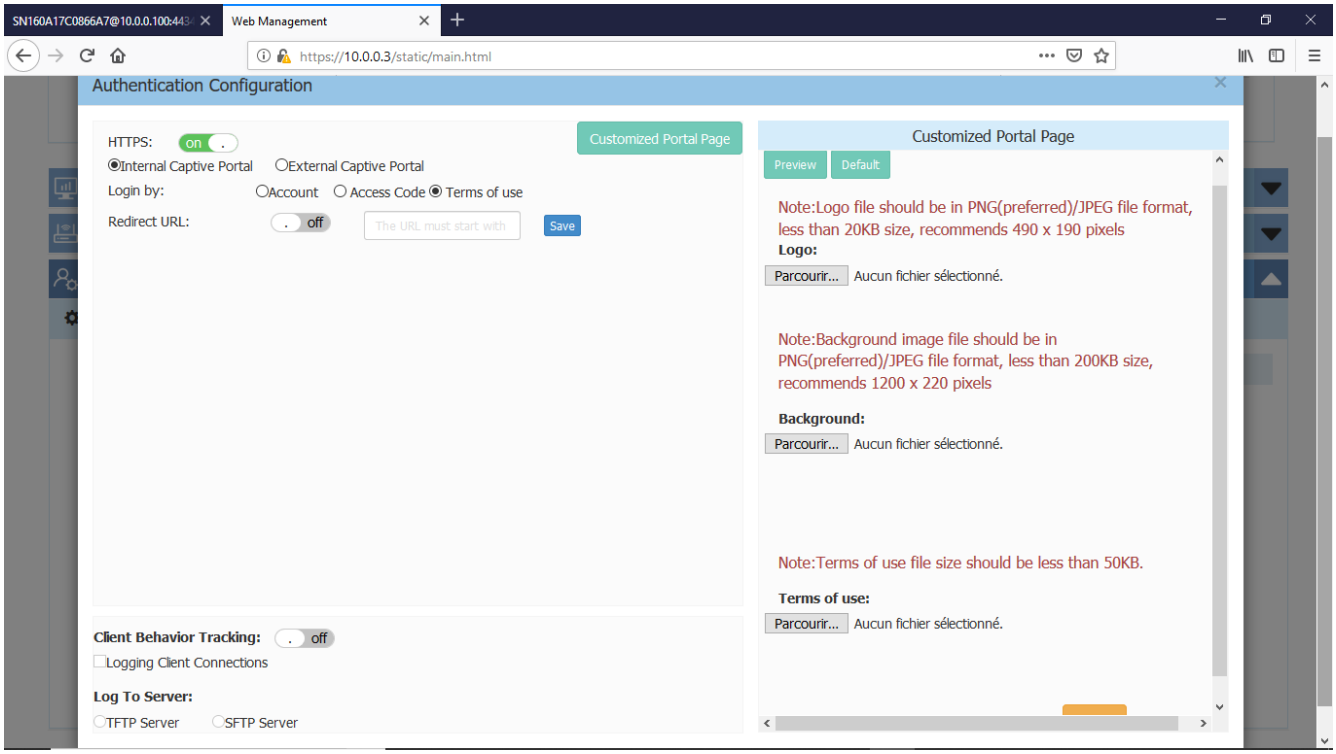
3. Pour le dernier SSID, je le nomme GUEST et je le paramètre en tant que réseau ouvert à tous et sans mot de passe. C'est à partir de cet SSID que les visiteurs dans le bâtiment de l'entreprise pourront avoir un accès à internet.



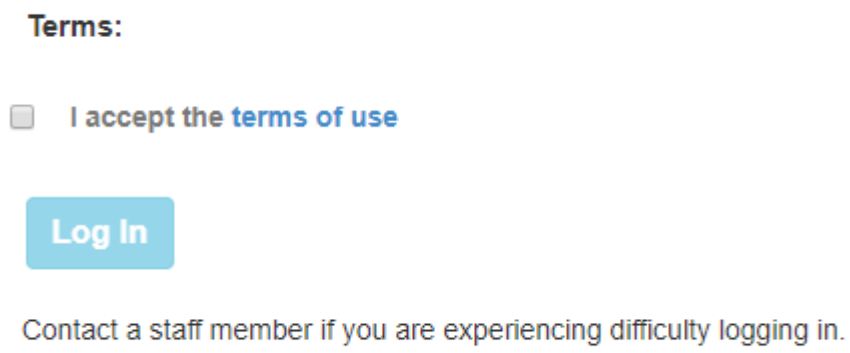
En l'activant, je l'identifie au VLAN 200 correspondant au VLAN GUEST configuré précédemment sur les Switchs. Il distribue le réseau 192.168.25.0/24.



Enfin pour finir la configuration, je crée un « captive portal » (portail captif) en accédant à l'onglet Access de la page d'accueil puis en allant sur le sous onglet Configuration.



Dans la configuration, je le paramètre pour un accès HTTPS, je lui soumets une page par défaut déjà présente dans la configuration de la borne puis je sauvegarde.
Nous pouvons alors accéder à une page d'authentification comme ci-dessous :



Après avoir lu et accepté les « Terms of use » ou termes d'utilisations en français, nous pouvons alors nous connecter et avoir accès à internet avec notre smartphone par exemple. Une page de confirmation de connexion s'affiche alors.

Nous avons pu voir durant ces 2 parties toute l'organisation de l'architecture réseau. Des VLAN en passant par la création de plusieurs SSID pour la borne Wifi, notre objectif maintenant sera de se pencher tout particulièrement sur l'aspect sécurité de la maquette.

c. La sécurité réseau : la configuration du firewall Stormshield

i. Le Firewall (Pare-feu) Stormshield SN160

Sans aucun compromis sur la sécurité, le SN160 embarque toutes les fonctions de sécurité nécessaires pour assurer une protection optimale des petites structures informatiques.

Avec les fonctionnalités VPN IPSec évoluées, les filiales et sites distants sont connectés de manière sécurisée et transparente aux ressources informatiques de votre entreprise.

Avec des assistants intuitifs, nous sommes guidés étape par étape dans l'installation et la configuration de notre nouvel équipement de sécurité.

Les solutions Stormshield Network Security reposent sur le concept de la sécurité collaborative multicouche. Cette approche globale, basée sur la collaboration active entre les moteurs de sécurité de nos différentes solutions, représente l'avenir en matière de protection des systèmes informatiques.

ii. Configuration

Le firewall se présente sous plusieurs ports :

Depuis la gauche vers la droite nous avons :

- Un port d'alimentation par prise secteur pour démarrer la machine
- Un port console dans le cas où nous ne pouvons plus accéder par interface WEB* à la page d'administration et donc configurer en affichage console
- 2 Ports USB dont l'utilité peut être lors de l'installation de fichier de mise à jour ou encore de l'installation de certificat si cela n'est pas possible via internet
- Un port WAN* ou aussi appelé OUT qui servira de lien avec la Livebox et donc de fournisseur de réseau internet. Le réseau trafiquant ici est le 192.168.23.0/24
- 4 ports LAN correspondant tous au même port IN et qui fera alors lien avec le port 1/10 du Switch1 comme vu précédemment.

Après installation, je me connecte en https au lien : https://10.0.0.254/admin/admin.html.

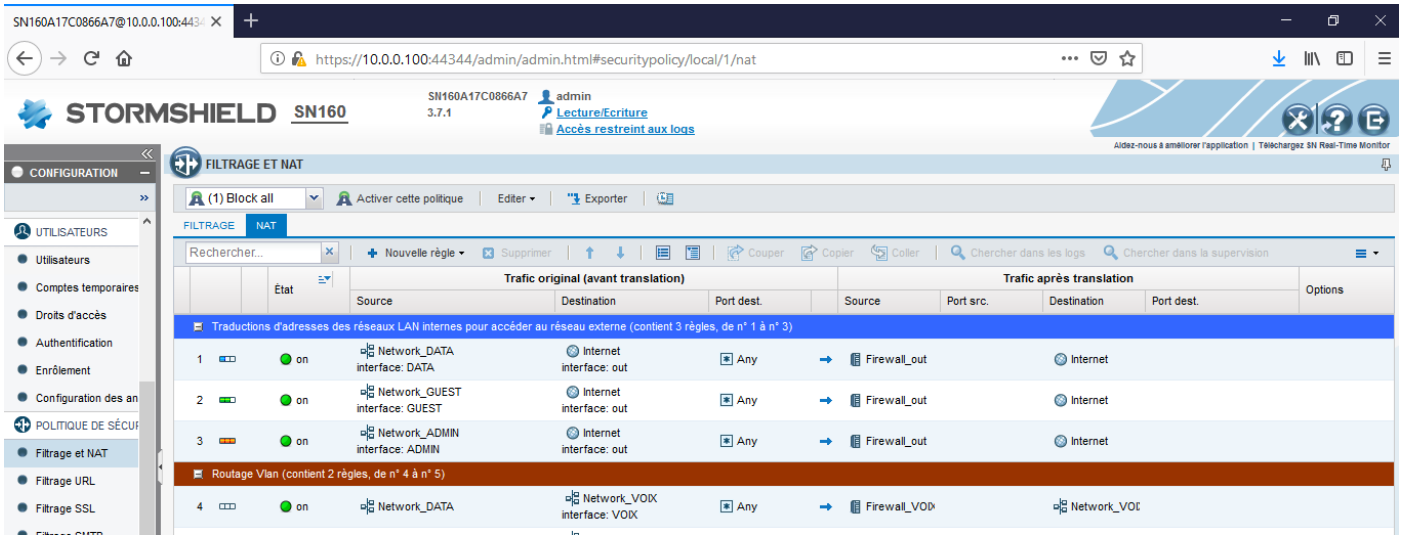
Le navigateur m'affiche alors la page ci-dessous :

On entre l'identifiant l'admin et le mot de passe. Nous pouvons alors accéder la page d'administration et de configuration du firewall.

Pour finaliser la maquette, nous devrons répondre à 2 objectifs :

- Création d'une traduction NAT* entre le réseau interne et externe
- Création de plusieurs règles de filtrages de sécurisation du réseau

En effet, pour que le réseau puisse accéder à internet, l'adresse IP réseaux interne ne doit pas accéder vers l'extérieur. De plus, la Livebox communique sur un réseau en 192.168.23.0/24 soit un réseau totalement différent de tous les réseaux internes.
Nous allons donc durant cette partie traduire tous les réseaux internes (DATA, GUEST et ADMIN) en réseaux « Firewall Out », c'est-à-dire le réseau distribuer par la Livebox en 192.168.23.0/24.



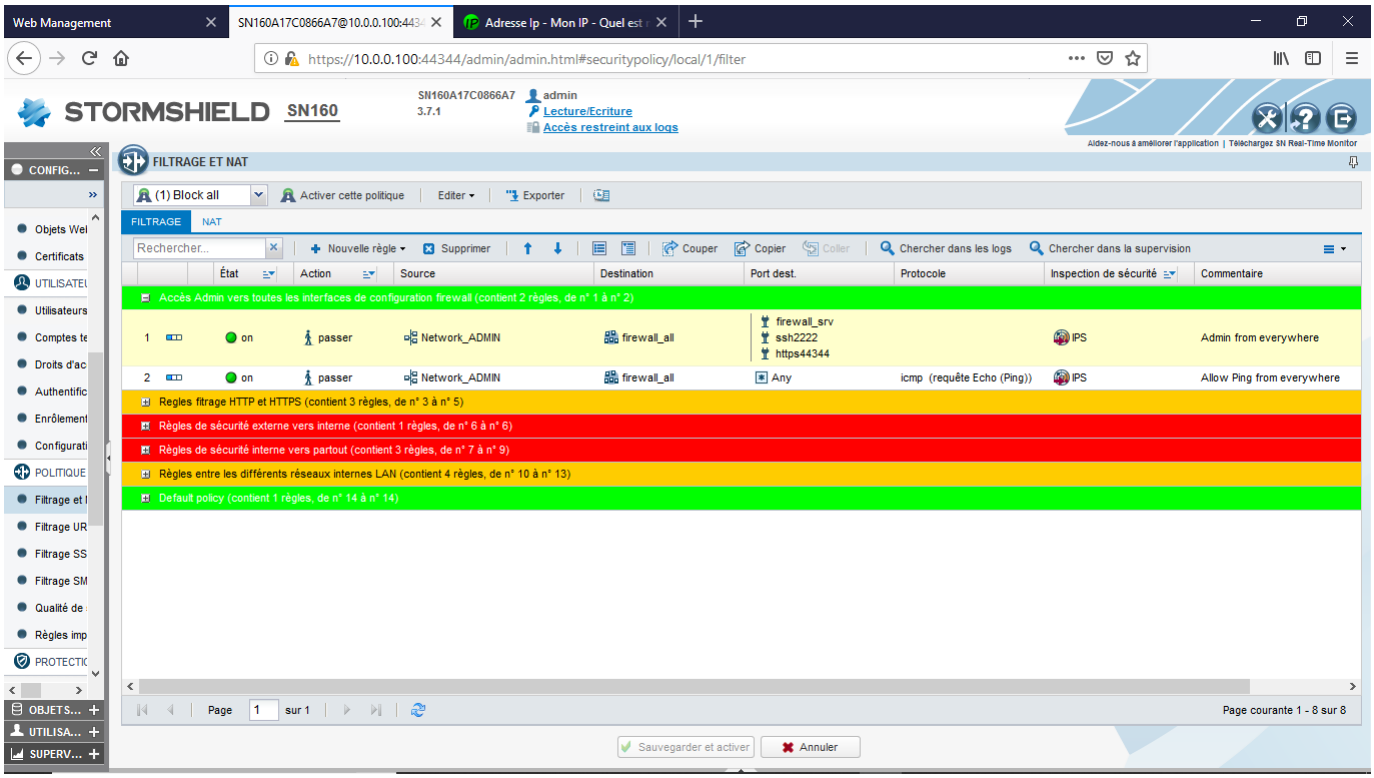
Sur l'image ci-dessus, nous pouvons voir les différentes règles de traduction configurée. On distingue la règle en 2 parties : le trafic original (avant translation) et le trafic après translation :

- Le trafic original possède comme source le réseau interne désigné que l'on veut traduire et il sera traduit que s'il est à destination d'internet.
- Le trafic après translation (après traduction) correspond donc à la traduction obtenue. Ici on peut voir que le réseau source a changé en réseau du « Firewall_Out » soit 192.168.23.0/24

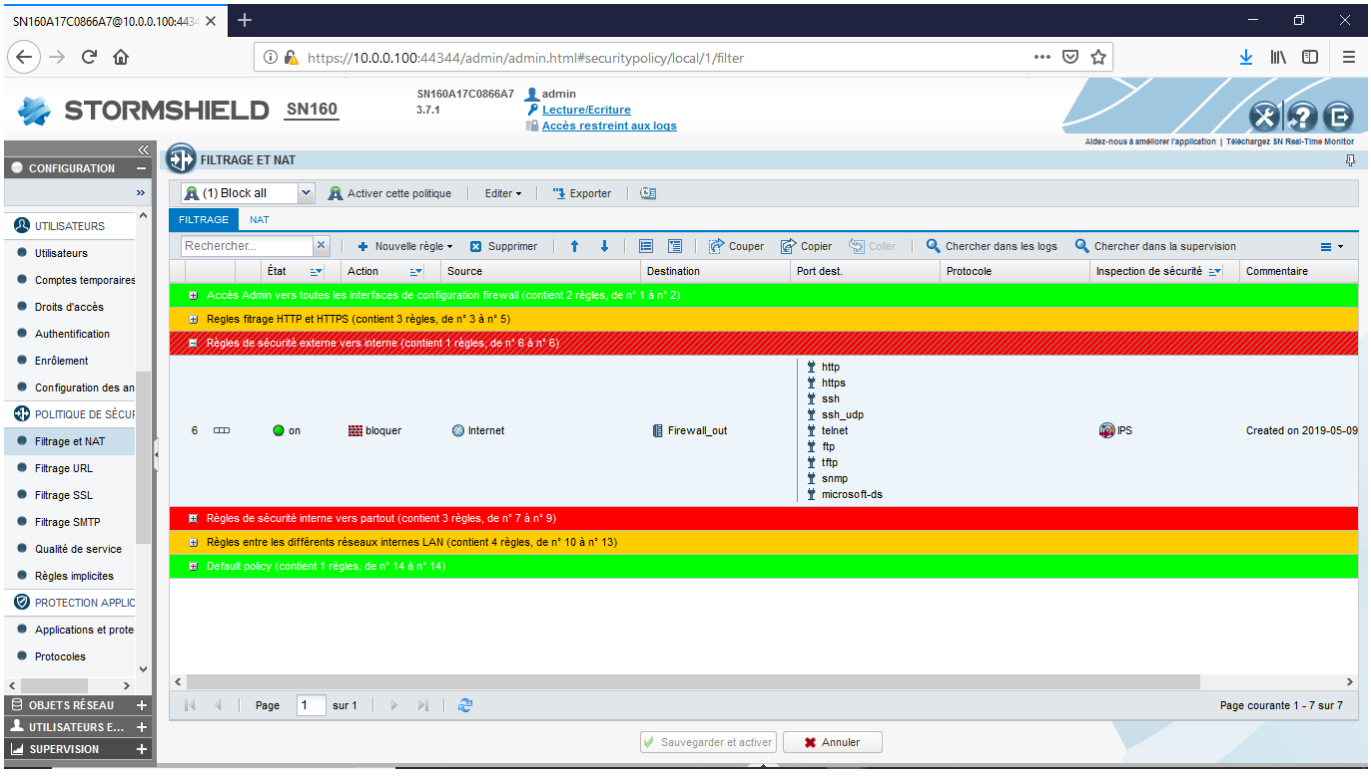
Ainsi le réseau est traduit et l'accès à internet est alors disponible via la Livebox pour laquelle aussi traduit le réseau 192.168.23.0/24 vers le réseau externe/public.

Pour qu'une architecture réseau soit complète, il faut que le débit soit constant et évite le plus de pannes possibles, mais il doit principalement être sécurisé et éviter le maximum d'infiltrations de hackeurs et autres malfaiteurs.

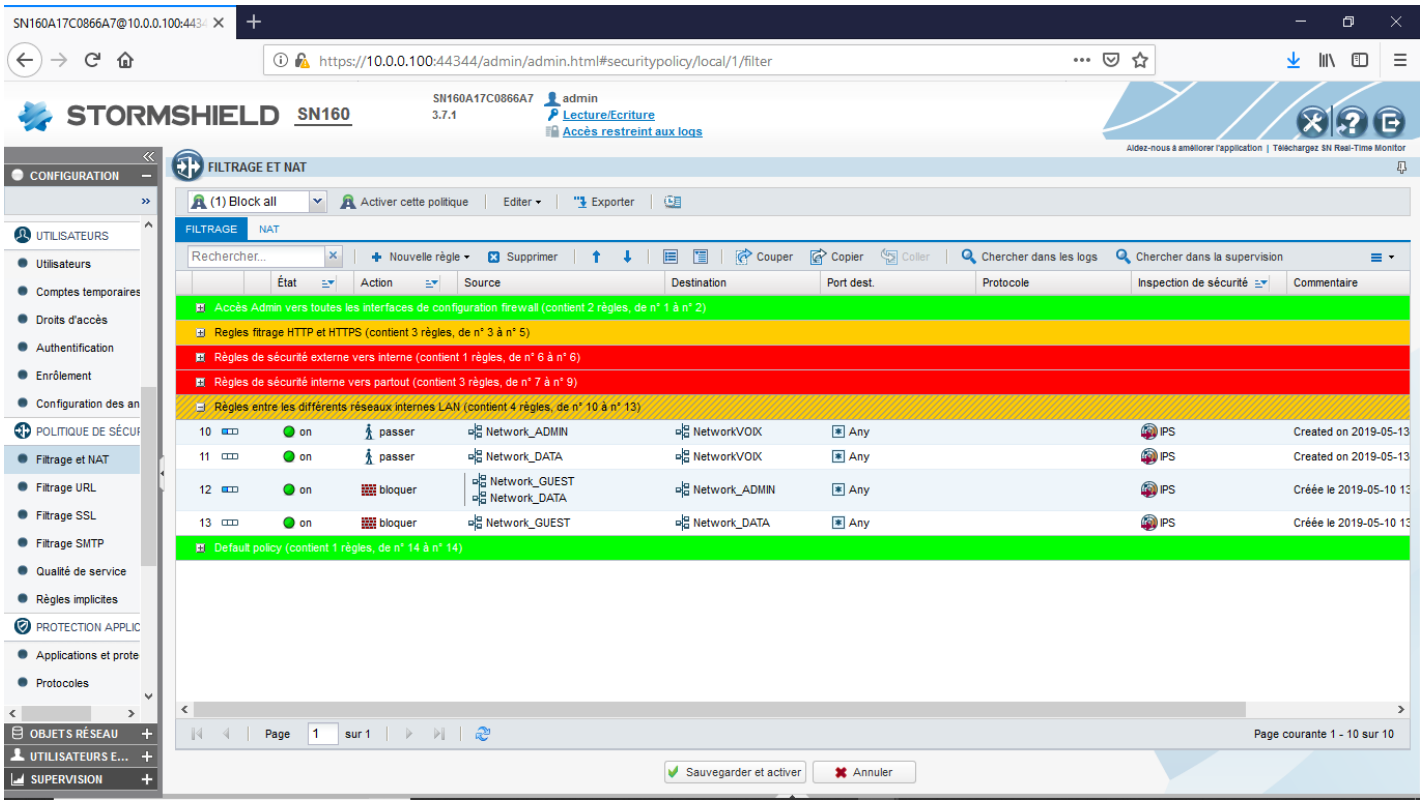
Pour cela, le firewall possède un onglet « règles de filtrage » dans lequel nous pouvons configurer les accès à différents protocoles entre les réseaux.



La 1ère règle de filtrage ci-dessus permet l'accès à l'interface WEB en https ou encore par ssh pour le réseau source ADMIN. Quant à la règle en dessous permet d'autoriser le réseau l'utilisation du protocole ICMP*.



Cette règle de blocage consiste à interdire l'accès à l'interface OUT du firewall via différents protocoles d'accès : http, https, ssh, ssh_udp, telnet, ftp, tftp, snmp ou encore microsoft-ds correspondant à un service permettant de créer des partages avec d'autre poste et peut donc être une faille pour les ordinateurs tournant sous Windows.



Sur la figure ci-dessus, nous pouvons observer la création de règle de routage inter-VLAN. Le routage inter-VLAN signifie la possibilité de faire communiquer et échanger 2 réseaux internes différents entre eux. Par exemple, la 1ère règle que j'ai pu créer permet au réseau source ADMIN de pouvoir communiquer et échanger avec le réseau interne VOIX. De même que dans la 2ème règle le réseau source interne DATA échange avec le réseau interne VOIX. Ces règles ont un intérêt applicatif pour l'entreprise puisqu'elles permettront par exemple d'appeler des téléphones IP de l'entreprise depuis son ordinateur. De plus, nous pouvons voir l'interdiction d'échange entre les réseaux interne GUEST et DATA avec le réseau ADMIN ainsi qu'entre le réseau GUEST et DATA pour renforcer l'aspect sécurité et éviter toutes infiltrations dans les réseaux internes.

5 Conclusion

Ainsi, j'ai pu effectuer mon stage de fin d'études du DUT Réseaux et Télécommunications au sein de l'entreprise Orange.

Durant ce stage de 10 semaines, j'ai pu mettre en application mes connaissances théoriques et pratiques accumulées pendant mes 2 années de formations au DUT.
Après ma très bonne intégration au sein de l'équipe technique, j'ai eu l'occasion de réaliser de nombreuses interventions qui ont constitué mes différentes missions du stage.

Chacune des tâches réalisées au sein de l'entreprise ainsi que celles pratiquées en déplacement ont été utiles au bon déroulement de l'activité de l'entreprise.
Elles se sont inscrites dans la continuité de mes études et de mon projet professionnel.

Je suis très satisfait et heureux de ces quelques semaines passées au sein de la société Orange. Elles constituent désormais pour moi une réelle expérience professionnelle valorisante et encourageante pour mon avenir ainsi que de nouvelles compétences solides, acquises grâce au travail et surtout un très bon encadrement.

Je pense que cette expérience chez Orange m'offre une bonne préparation à mon insertion professionnelle en vue de préparer mon entrée en école d'ingénieur à CPE Lyon.
Cette expérience enrichissante et complète conforte mon désir d'exercer mon futur métier d'Ingénieur dans les domaines des Réseaux et de la Cybersécurité.

Enfin, je tiens à exprimer ma satisfaction d'avoir pu travailler dans de bonnes conditions matérielles et un environnement agréable.

6 Remerciements

Je tiens à remercier tout le personnel du service PIOC 13 de l'entreprise Orange et plus particulièrement Monsieur Gey Philippe, manager du service PIOC 13 qui a eu l'amabilité de m'accueillir comme stagiaire au sein de sa société.

Je remercie bien évidemment Monsieur Fraisse Nicolas, mon tuteur de stage et responsable du service, pour sa patience et sa disponibilité pour répondre à mes nombreuses questions.

Pour finir, je tiens également à remercier sincèrement les collègues du département Aix Jas de Bouffan pour leur bienveillance et le temps accordé à me présenter chaque poste.

Chacune de ces personnes ont rendu mon stage passionnant et m'ont permis de développer mes compétences. Je leur en suis particulièrement reconnaissant puisque grâce à elles, mon avenir est des plus prometteurs.

7 Glossaire

DUT, Diplôme Universitaire de Technologie

SAV, Service Après Vente

OCWS, Orange Connectivity & Workspace Services

OCD, Orange CyberDefense

OAB, Orange Applications for Business

DOGSE, Direction Orange Grand Sud-Est

RSE, Responsabilité Sociétale des entreprises

DO, Direction d'Orange

L'UI, Unité d'Intervention

DIOCE, Direction Intégration Offres Complexes

B2B, Business-to-Business

QSE, Quality of Service Enterprise

DGC, Direction Grand Client

RPI, Responsable Production Intégration

OCB, Orange Business Services

PV, Procès-Verbal

DECT, Digital Enhanced Cordless Telephone

PME, Petites/moyennes entreprises

LAN, Local Area Network

QOS, Quality of Service

VLAN, Virtual Local Area Network ou Réseau Local Virtuel

LACP, Link Aggregation Control Protocol

SSH, Secure Shell

LLDP, Link Layer Discovery Protocol

AP, Access Point

WLAN, Wireless Local Area Network

SSID, Service Set Identifier

DHCP, Discovery Host Configuration Protocol

WAN, Wide Area Network

NAT, Network Address Translation

ICMP, Internet Control Message Protocol

8 Sitographie

Réseau intranet d'Orange Entreprise

https://www.al-enterprise.com/-/media/assets/internet/documents/omniswitch-6450-24-48-datasheet-en.pdf

https://www.al-enterprise.com/-/media/assets/internet/documents/omniswitch-6350-family-datasheet.pdf

https://www.al-enterprise.com/-/media/assets/internet/documents/omniaccess-ap1101-datasheet-fr.pdf