Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Installation et mise en réseau de salles pour le Master Réseaux & Télécommunication

Alexis Boyer

UFR Sciences

Responsable entreprise : Didier Tonneau

Responsable académique : Tin Nguyen

2021

Table des matières

1 Introduction

Dans le cadre de mon DUT (Diplôme Universitaire de Technologie), j'ai réalisé mon stage de fin d'études au sein de l'université d'AMU (Aix-Marseille Université) et plus particulièrement à l'UFR Sciences sur le site de Luminy.

Lors de ces 10 semaines de stage, j'ai réalisé diverses tâches très variées allant du tirage de câble, à l'administration des systèmes. La tâche principale a été l'architecture et administration réseau dans le but d'installer une infrastructure réseau pour les salles de TPs du master Réseaux et Télécommunications.

J'ai effectué ce stage en équipe avec M. Adrien CAILLEAU-LEPETIT, étudiant issu de la même formation que moi, et M. TCHANVOEDO et YOUNSI étudinats du Master Réseaux et Télécommunication. Nous avions une mission commune pour répondre aux besoins exprimés par le responsable des salles de TPs. Certaines tâches ont nécessairement été communes, aussi le pronom « nous » fera-t-il référence au travail effectué en équipe.

Dans ce rapport, je vais vous introduire dans un premier temps l'organisme dans lequel j'ai travaillé. Dans un second temps j'aborderai plus précisément les divers aspects techniques utilisés dans la réalisation de ce projet.

2 Présentation du contexte et de l'organisme

2.1 Le projet ECO

Ce stage s'inscrit dans le cadre du projet ECO (Education with Connected Objects) de l'Académie d'Excellence de la fondation AMIDEX. Ce projet a pour but de fournir une plateforme pour les étudiants de masters orientés vers l'informatique ou le réseau à AMU.

Cette plateforme permettrait aux enseignants de AMU ou aux start-ups de proposer des projets concernant le réseau, l'informatique ou l'IOT* (Internet of Things). Ces projets seraient ensuite réalisés par les étudiants. Les objets réalisés pourraient alors être mis aux mains des enseignants pour les aider à atteindre leurs objectifs pédagogiques.

Pour réaliser ce projet nous avons besoin de 3 éléments :

- Mise en place de salles de projets pour concevoir et réaliser les objets connectés. Ces salles doivent être équipées de switches PoE CISCO catalyst 3750, puis SG-250X
- Mise en place de la plateforme web pour proposer les sujets
- Installation d'un serveur dans le datacenter de Luminy pour les données d'objets

2.2 Présentation de l'organisme d'accueil

2.2.1 L'UFR Sciences

L'UFR Sciences est éclatée sur plusieurs sites, dont le site de Marseille-Luminy. Elle comptabilise au total environ 12 000 étudiants répartis dans de plusieurs domaines scientifiques ou Départements, en l'occurrence les Mathématiques, la Physique, la Chimie, l'Informatique et la Biologie. Elle compte au total 29 unités de recherche, 26 licences dont 13 licences professionnelles, 27 masters et 6 Ecoles Doctorales. Dans le cadre de ce stage nous avons œuvré pour un master localisé à Luminy. Nous

dépendons du Département de Physique et nous mettrons en œuvre le projet ECO pour le master Réseaux et Télécommunications spécialités IOT et Architecture et Sécurité des Réseaux.

2.2.2 Organigramme

La figure 1 donne un organigramme simplifié, permettant de visualiser d'une part la pyramide hiérarchique de ma structure d'accueil ainsi que la dépendance des personnes avec lesquelles j'ai interagi (DOSI).

Figure 1 : organigramme simplifiée de la structure d'accueil.

3 Présentation du stage : Expression du besoin

Dans le cadre de ce stage au sein de l'UFR Sciences, l'objectif global de notre mission était de concevoir et réaliser l'architecture réseau des deux salles de TPs du master Réseaux et Télécommunication de Luminy. Dans ces salles un câblage de catégorie 6 avait été installé par des anciens stagiaires. La première mission a donc été d'installer l'accès de ces salles au réseau de Luminy.

Par la suite une fois l'accès réseau mis en place, une deuxième mission a été établie : cette salle doit être en lien avec le serveur du master afin de transmettre des données capteurs ou des données vidéo. Enfin, si le temps est suffisant répliquer cette installation à Saint-Jérôme mais en partant d'une salle vide.

4 Pré-stage

4.1 Préparation et organisation

Une fois le besoin exprimé par le responsable des deux salles de TPs, nous avons dû :

- Trouver les solutions techniques
- Rédiger un cahier des charges
- Partager le travail au sein de notre équipe et concevoir un planning
- Effectuer les tâches

Une fois le travail effectué, nous devrons effectuer des tests de vérification de bon fonctionnement et de robustesse.

L'appartenance à AMU permet l'accès aux divers outils de Microsoft, parmi lesquels l'outil Planner attire notre attention. Il s'agit d'un outil permettant d'avoir une gestion de tâches et d'assigner des personnes sur ces tâches, mais également d'accéder à un SharePoint prévu uniquement pour ce projet. Il contient un drive, une messagerie dédiée liée au projet. Cet outil nous a permis de pouvoir nous partager d'éventuelles pistes ou documents pour le projet tout en étant organisé, permettant de respecter certains jalons. Enfin, nous avons dû organiser des réunions, dans un premier temps avec le tuteur de stage afin d'avoir les précisions sur ses besoins, mais également avec des intervenants externes afin de savoir ce qui avait déjà été mis en place notamment sur le serveur du Master, mais également avec la DOSI pour validation des solutions que nous avons proposées.

4.2 Documentation

Afin de réaliser notre projet de stage dans les meilleures conditions possibles et de rendre un travail de haute qualité, nous avons avons effectué une étude préliminaire des normes et préconisations de l'ANSSI* (Agence Nationale de la Sécurité des Systèmes d'Information). Cette étude nous a permis de nous renforcer dans le domaine de la Sécurité des Réseaux.

4.2.1 La politique de filtrage par firewall

Nous avons travaillé sur deux principaux aspects : la partie des firewalls et la partie des switches et 802.1X.
Pour une documentation complète vous pouvez vous référer à l'annexe n°2.

Architecture

Dans le cadre d'une entreprise ou d'un réseau personnel, nous sommes dans l'obligation de nous protéger face aux différentes menaces qui peuvent arriver. Dans le cadre de la protection des réseaux un outil, qu'il soit matériel ou logiciel, est fortement utile pour la protection : le firewall. Dans le cadre d'une protection optimale de l'entrée d'un réseau nous devons former une DMZ* (Zone démilitarisée).

Les DMZ :

La DMZ a pour but d'être une double protection par double firewall. Il faut qu'il y ait un firewall à l'arrivée de notre trafic et un autre avant l'entrée de notre réseau privé. Comme le montre le schéma figure 2.

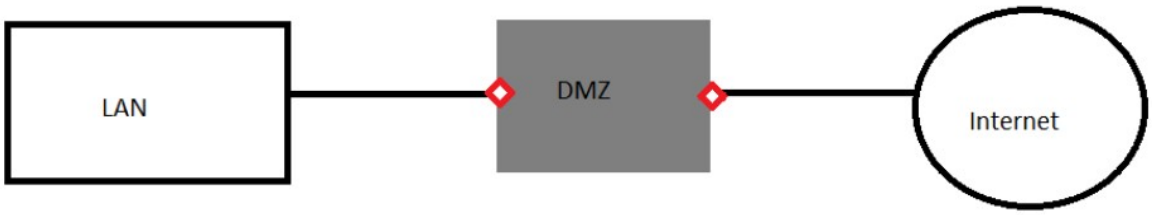

Figure 2 : Représentation schématisée d’une structure DMZ

Le filtrage et cloisonnement du réseau :

L’accès à internet est fourni par un FAI* (Fournisseur d’Accès Internet). Ce dernier fournit également une mini-solution de firewall. Cette solution est certes convenable pour un particulier, mais pour une entreprise il faut une entité de protection forte dès l’entrée du réseau. Il nous faut donc installer un firewall incontournable qui fait du filtrage IP ou du filtrage de protocoles. En plus de ce firewall fort il faut penser aux différentes failles de sécurité qui peuvent parvenir d’un opérateur particulier. Il est donc recommandé d’utiliser différentes gammes de firewalls, mais également de se référer aux conseils de l’ANSSI sur des firewalls qui sont recommandés en fonction des dernières failles qui peuvent être trouvées sur certains modèles.
Dans un but de protection de notre réseau l’idéal est d’avoir des services de relai qui permettent d’éviter l’interruption de l’accès en cas d’attaque. Mais également si on suit scrupuleusement les recommandations il serait important de protéger chaque service critique par un firewall. Afin d’en assurer la protection la plus optimale, le seul gros problème de cette solution reste les coûts qu’elle engendre.

Politique de filtrage des pares-feux

Dans cette partie nous allons mieux cerner comment appliquer des règles de filtrage plus précises pour nos firewalls. Un des fondamentaux dans la mise en place de ses règles est de bien documenter afin d'avoir un suivi au fil du temps et une possibilité d'évolutivité si une personne tierce prend l'installation en main.

Les flux en destination du pare-feu :

Dans le cadre des flux qui sont à destination de notre pare-feu, c'est-à-dire ceux concernant la gestion de notre pare-feu, nous allons uniquement garder les flux permettant sa supervision (Ex : SSH, SNMP-Get..)

Les flux émis du pare-feu :

Dans le cadre d'un trafic émis par le pare-feu, nous allons laisser les flux de gestion réseau : syslog, snmp-trap et le SSH par exemple

La protection du pare-feu :

Dans le cadre d'une protection optimale, tout service non utilisé sera systématiquement rejeté, ceci afin de rejeter le trafic sans donner de réponse de retour.

L 'autorisation des flux métiers :

Les flux métiers, permettent d'établir au cas par cas les besoins d’une personne pour la réalisation de son travail, par exemple autoriser l'accès à un serveur web ou à un serveur de fichiers.

Les règles antiparasites :

Les règles antiparasites permettent d'alléger le système de log. Cela permet, en cas d'attaque ou de problèmes, de pouvoir lire plus facilement les logs. Un exemple de flux filtré concerne les nombreux ‘broadcasts’ qui ne sont pas nécessairement pas utiles à journaliser.

Règles de nettoyage des politiques de pare-feu

Un firewall est une installation évolutive au cours du temps. Il faut donc prévoir de pouvoir ajouter ou retirer des politiques de sécurité pouvant être obsolètes. Dans cette partie nous allons voir comment les nettoyer.

Le nettoyage des doublons :

Les politiques de sécurité peuvent cibler une adresse particulière. Ceci équivaut au fil du temps à retrouver une liste non exhaustive de règles liées à une même adresse, dans un but de performance et de simplicité de suivi. Il convient alors de compacter cette règle à une seule règle regroupant l'ensemble.

Les règles inutilisées :

Les règles inutiles c'est à dire des règles n'étant plus d'actualité doivent être enlevées afin d'alléger la liste de filtrage mais également d'éviter des potentielles confusions.

Les règles redondantes :

Des règles peuvent être également redondantes lorsqu’elles autorisent le même flux. Cela peut donc compromettre l'intégrité du réseau lorsqu’elles ne sont pas appliquées avec la même rigueur de filtrage.

La suppression des règles :

La suppression des règles pouvant être redondantes ou inutiles devra se faire en suivant une méthode précise. En effet, nous ne devons pas affaiblir notre réseau le temps de ces changements ni supprimer des règles importantes par mégarde.

La suppression des règles inutilisées :

Pour la suppression des règles, nous devons les identifier précisément avec une date de coupure, un intervalle avant la suppression afin de savoir si cette règle n'influe pas sur le réseau, sur des questions de performance ou d'intégrité. Mais il est important de segmenter ces suppressions afin de pouvoir cibler les différents problèmes pouvant suivre à ces suppressions.

La suppression des règles redondantes :

Pour les règles redondantes, deux cas sont à envisager. Si elles sont exactement identiques, nous en supprimons une des deux. Si une des règles ne diffère de l’autre que légèrement, nous allons devoir affiner et potentiellement les compacter en une seule règle commune regroupant les aspects des deux politiques appliquées.

4.2.2 Sécurité des réseaux locaux

Pour protéger nos réseaux locaux plus orientés sur les commutateurs, nous devons considérer deux aspects : la protection du commutateur en lui-même et la protection de l'accès au réseau via la norme 802.1X.

Protection des commutateurs

Pour protéger notre commutateur nous avons d'abord besoin de savoir quelles interfaces nous allons configurer. Ces interfaces doivent être uniquement accessibles par l'administrateur. Nous allons utiliser le port console qui est la moins faillible pour la configuration.

Un cloisonnement en VLANs* (Virtual LAN), permet de sécuriser le réseau. Un aspect important est de couper les ports de commutation non utilisés.

Également, un réseau peut être faillible sur des aspects d'accès exemple le DHCP* (Dynamic Host Configuration Protocol), ARP. Il faut donc bien penser à protéger ces différents protocoles qui permettent à notre réseau de fonctionner de façon automatique.

Authentification 802.1X

En plus de la protection via les VLANs et les coupures de ports, nous pouvons utiliser 802.1X pour vérifier les appareils qui se connectent à notre réseau. Cela se passe grâce à une authentification.
Il convient d'utiliser les protocoles les plus sécurisés.
Cela permettra de lutter en général contre la connexion illégitime, ce qui est la faille la plus importante d'un réseau

5 Réalisation au sein de l'organisme

5.1 Cahier des charges

Après avoir pris le temps d'étudier différentes normes liées à la sécurité des réseaux informatiques et des systèmes d'informations, nous avons pu commencer à travailler plus précisément sur notre projet. Seul le câblage réseau de la salle était fait. Donc pour pouvoir nous lancer dans le projet sans éviter d'erreurs de compréhension nous avons établi le cahier des charges.

Le premier cahier des charges avait pour but d'établir les premières étapes de notre projet afin de le soumettre aux avis de la DOSI* (Direction Opérationnelle des Systèmes d'Information) pour ensuite réaliser l'ensemble des salles. La première version du cahier des charges est disponible en annexe n°3.

Dans un premier temps, il faut se pencher sur nos besoins. Voici la listes des besoins qui sont adressés par le cahier des charges :

- La connexion des équipements :

Il faut connecter les prises murales que nous allons utiliser à un switch PoE. Nous devons alors définir quels appareils y seront reliés afin d'établir au mieux les sécurités à appliquer en fonction du besoin en réseau.

- L'accès vers l'extérieur :

Tous les appareils seront reliés soit au datacenter, soit au réseau de Luminy pour internet.

- Sécurité de notre réseau :

Si nous établissons un lien avec internet il faut être sûr que nous avons un appareil légitime mais également que les appareils capteurs ne polluent pas le réseau de Luminy.

Pour tous ces besoins des solutions techniques découlent de chaque demande il faut donc établir un plan logique et réfléchir aux différentes techniques. Dans ce cadre nous allons voir pour chaque point cité précédemment les solutions techniques.

a) Pour la connexion des équipements :

Dans le cadre de la mise en réseau et de la connexion des équipements nous devons établir un ordre logique de connexion. Nous avons donc choisi de prendre les prises paires pour les ordinateurs et les prises impaires pour les capteurs et les caméras. De plus il nous faut un pool d'adresses IP pour nos appareils. Pour cela une question subsiste : soit nous avons accès au pool DHCP de la DOSI soit la DOSI nous fournit un pool d'adresses que nous pouvons utiliser dans notre propre pool autogéré. Il faut également établir une politique de sécurité sur les postes qui se connectent à notre réseau. Nous avons décidé de filtrer les adresses MAC dans un premier temps. Nous allons également mettre en place une authentification des appareils via (802.1X) pour des appareils fixes.

Également nous allons isoler les différents VLAN (Virtual LAN) en fonction des flux qui transitent. Nous allons donc utiliser 3 Vlans : un VLAN pour nos ordinateurs correspondant au VLAN de l'université, un VLAN pour les capteurs mais également un VLAN pour les flux Vidéos émanant de TPs avec une sécurité renforcée.

b) Pour l'accès vers l'extérieur :

Dans le cadre de l'accès vers l'extérieur pour les ordinateurs fixes, le trafic transitera simplement par le VLAN de l'université. Ceci nous permet un accès simple vers le réseau de l'université et internet. Concernant le serveur du master et de l'accès au datacenter une solution choisie est la mise en place d'un tunnel VPN IP-Sec (Virtual Private Network – figure 3) permettant un accès direct au serveur du master tout en permettant une protection de ces données grâce à un chiffrement. L'avantage d'un VPN, permettant le lien entre 2 points bien définis, est la certitude que les données envoyées arriveront à destination.

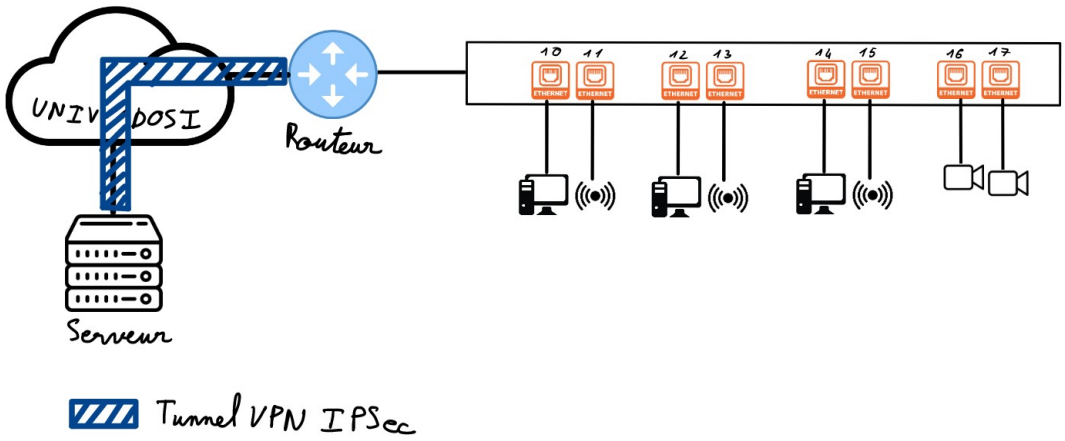

Figure 3 : Représentation schématisée de la première infrastructure

c) Pour la sécurité de notre réseau :

Dans le cadre de la protection de nos réseaux une solution maintenue dans la première version de notre cahier des charges est l'installation d'un firewall. Celui-ci permet une protection contre les flux internes et externes c'est à dire qu'il permet de mieux isoler notre réseaux contre les menaces externes mais également d'éviter d'inonder le réseau avec les flux des capteurs si un problème survient. Également pour la protection des ordinateurs nous passeront par le VLAN de l'université dans un cadre de gestion et de suivi de la DOSI qui nous permet d'avoir une gestion simplifiée des problèmes. Concernant la sécurité des objets capteurs et caméras, nous avons pensé à l'utilisation d'un Pvlan

(Private VLAN). Cette solution permet, en plus du chiffrement, d'isoler du réseau le vlan concerné dans le but d'augmenter la sécurité. Un PVlan est un "sous-vlan privé". Nous utilisons les propriétés d'un Vlan privé unique, car nous ne pouvons avoir qu'un PVlan isolé par Vlan. De la nous découle l'utilité de 2 Vlans pour les données capteurs et caméra ce qui permet d'avoir 2 vlans privés.

5.1.1 La première rencontre avec la DOSI

A la fin de l'écriture du premier cahier des charges nous avons dû nous entretenir avec la DOSI (M. Pascal MOURET) afin de vérifier que nos propositions étaient compatibles avec les politiques d'installation sur Luminy. Cette réunion a eu lieu sur place ou les salles doivent être mises en place, afin de mieux lui montrer ce qui doit être installé. Nous avons eu également la chance de pouvoir aller voir la baie de répartition de notre bâtiment afin de pouvoir nous rendre compte de l'installation réseau dans laquelle nous devons insérer notre réseau. Nous avons également pu nous rendre compte du fonctionnement plus détaillé du réseau informatique de Luminy.
Par la suite de ce premier cahier des charges et un premier entretien avec la DOSI de Luminy, nous avons eu des propositions alternatives aux nôtres mais également des axes d'amélioration de notre propre cahier des charges. Nous avons donc établi un deuxième cahier des charges qui se rapproche de l'infrastructure finale qui sera installée dans les salles. Ce cahier des charges est également disponible en annexe n°3. Nous allons ci-dessous explorer les changements et argumenter les différentes modifications dans le but de comprendre pourquoi nous devons nous orienter vers d'autres techniques.

5.1.2 L'évolution de l'installation en lien avec la DOSI

Pour le choix des switchs, nous nous sommes penchés sur les besoins des salles. Nous avons besoin d'un switch PoE* (Power Over Ethernet), mais également un switch supportant dans un premier temps le trafic des ordinateurs, des flux capteurs et caméra. Le master disposait d'un switch CISCO PoE de 48 ports à 10 Mbits. Pour des raisons d'homogénéité, le responsable de la salle a décidé d'acheter deux switchs neufs de manière à s'assurer d'une bonne longévité de l'installation. Pour cela nous sommes partis sur un switch de la gamme Cisco, partenaire privilégié de la formation de Master Réseaux et Télécommunication. Nous avons donc choisi le switch le SG-250X de 48 ports pour laisser une marge d'évolution des besoins dans les cinq ans. Ce switch possède 4 ports 10 giga et 48 ports 1 giga, ce qui permet d'avoir un très bon accès de desserte. Si les besoins du projet n'ont pas changé depuis le premier cahier des charges, les solutions techniques quant à elles ont évolué avec le nouveau matériel mais également en tenant compte des propositions d'installation faites par la DOSI.

Pour la connexion des équipements nous avons eu des réflexions sur l'aspect évolutivité dans le temps mais également sur la maintenance. Nous avons alors convenu d'une solution d'Etherchannel, permettant de faire un gros lien virtuel de desserte assemblé partir de plusieurs liens physiques. Nous installerons cette solution entre chaque switch et le local de desserte de la DOSI (figure 4), mais également entre nos deux switches (figure 4) afin de maintenir une forme de redondance. Cette structure triangulaire permet l'accès au réseau ou au serveur, même en cas de rupture d'un des liens de desserte tout en évitant une période de down time trop longue.

Dans un second temps nous avons testé les prises d'accès aux salles. Nous avons remarqué que l'installation étant vieille, elle n'était pas de même norme que les équipements que nous installons dans la salle. En effet, le bâtiment était équipé de câble de catégorie 3 permettant de faire passer un débit de 100 Mégabits/s maximum. Nous serions énormément bridés sur des ports 10 Go dont nous disposons sur les switches. La solution a donc été de tirer des câbles jusqu'au switch de répartition de la DOSI. Ceci a été réalisé avec des câbles de catégorie 7, seuls câbles permettant d'atteindre le 10 Gbit/s autorisé par les switchs.

Dans un troisième temps pour la partie de la connexion des équipements, en accord avec la DOSI, nous devons mettre en place notre propre service DHCP sur le serveur du master qui est situé dans le datacenter de Luminy. Un serveur Radius sera également mis en place pour le service

d'authentification 802.1X. Ces services seront hébergés sur une machine virtuelle que nous installerons sur le serveur.

Du côté de l'accès vers l'extérieur et du serveur, un des gros changements est le fait de remplacer notre idée initiale de tunnel VPN par une encapsulation QinQ. L'encapsulation QinQ correspond à une double encapsulation. De façon très simplifiée, cela revient à ajouter quelque chose permettant de délivrer le courrier à la bonne destination. Dans le cas de notre réseau nous faisons entrer notre VLAN dans un autre VLAN. Cette installation permet, contrairement au tunnel VPN IP Sec, de pouvoir faire du temps réel. En effet, le chiffrement et le déchiffrement des données empêchent cette notion de temps réel nécessaire notamment pour des flux vidéo.

Après l'établissement du deuxième cahier des charges, nous sommes rentrés une dernière fois en contact avec Pascal Mouret afin d'établir des derniers détails sur notre architecture. Nous avons principalement orienté la discussion autour de l'Etherchannel et trouvé un accord entre leur matériel et le nôtre. En effet, nous possédons du matériel Cisco alors que la répartition ne contient que des switches HP. Nous n'avons donc pas pu utiliser des outils propriétaire Cisco autour d'Etherchannel tels PAgP* (Port Aggregation Protocol). Nous nous sommes alors orientés vers LACP* (Link Aggregation Control Protocol). Sachant que notre infrastructure forme un triangle entre nos deux switches et le switch de répartition, il faut établir un système permettant d'éviter les boucles de couche 2. La DOSI voulant se réserver le contrôle sur leur spanning-tree, le protocole permettant d'éviter les boucles de couche 2, la solution proposée est d'utiliser par exemple un autre système qui est le fail-over. Le fail-over permet d'éviter les boucles en coupant les liens redondants entre des switches. Le switch réactivera automatiquement un des liens si le lien opposé n'est plus relié au réseau.

Pour la partie protection de notre réseau, nous avons décidé avec la DOSI que ce service s'occuperait de la gestion du firewall, d'autant qu'AMU vient de changer sa politique 'Firewall' et va sous peu être dotée de nouveaux équipements. La DOSI maintiendra l'installation pour la rendre compatible avec les différentes normes de sécurité. Cette tâche ne peut être confiée qu'à un administrateur réseau.

Le schéma final de l'installation que nous voulons mettre en place est donné figure 4.

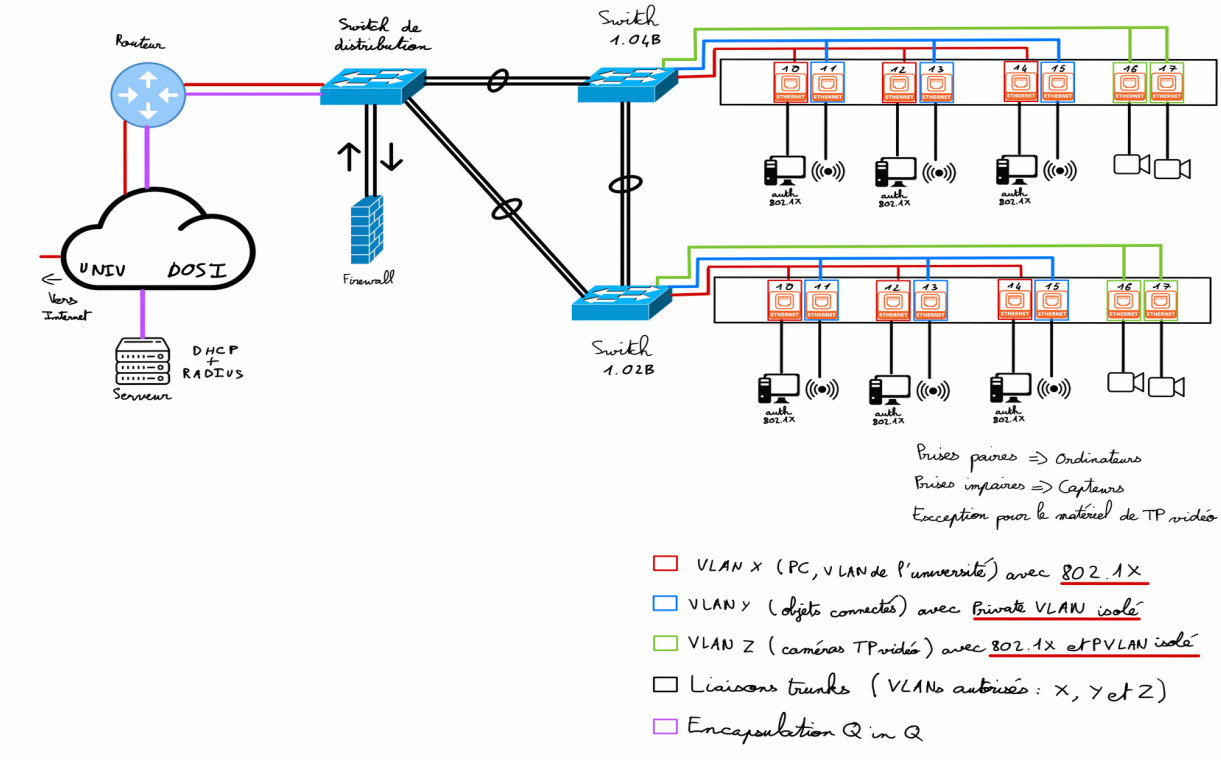

Figure 4 : Infrastructure globale à la fin du cahier des charges

5.2 Le maquettage et la modélisation

Dans ce projet, nous avons décidé d'utiliser GNS3 pour les simulations. Il s'agit d'un outil de création de maquettes réseau open-source. Il se décompose en deux grands axes d'utilisation :

- une partie cliente qui est graphique permettant de travailler sur notre maquette,
- une partie serveur qui héberge le service GNS3 mais également nos plans et les appareils que nous utilisons au cours de notre projet.

5.2.1 Installation de GNS3

Pourquoi GNS3 ?

Nous avons décidé d'utiliser GNS3, pour des raisons pratiques. Il s'agit d'un logiciel très rependu dans l'ingénierie réseau. Il nous permet de créer des maquettes proches du réel, contrairement à un autre outil qui est packet tracer, qui reste plus proche d'un cadre de simulation. GNS3 nous permettra donc d'évoluer plus sereinement dans le projet que nous voulons développer.

Mise en place d'un réseau temporaire

Pour accéder au serveur GNS3, nous avons dû créer un réseau local temporaire. Pour cela nous avons utilisé un switch 3750 sur lequel nous avons configuré un port security. Nous avons configuré les interfaces non utilisées en shutdown. Un DHCP nous fournit des adresses dynamiquement.

Figure 4 : Switch Catalyst 3750 utilisé pour le réseau temporaire

Tout cela sera agrémenté de VLAN pour augmenter la sécurité. Toute cette installation est dans un but optimal d'un réseau qui serait raccordé à internet, ici nous avons voulu nous entraîner pour mieux nous adapter au réseau futur.

Configuration et mise en place de GNS3 Server

Pour installer notre serveur GNS3, nous avons d'abord installé docker, qui nous a servi à gérer nos VM. Par la suite nous avons installé le serveur GNS3 mais également le système d'exploitation de GNS3. Par la suite nous avons ajouté les images des switches et routeurs que nous avons utilisés. Nous avons également activé les licences des switchs pour pouvoir les démarrer. Dans un but de pratique, nous avons fait un script Bash (Bourne-Again Shell) permettant de lancer le serveur sur l'adresse IP connue mais également de le lancer sur un port choisi.

5.2.2 Maquette du réseau

Après avoir conçu le cahier des charges et avoir convenu des technologies que nous allions utiliser pour mettre en place notre réseau, nous sommes passés à l'étape plus technique de réalisation d'une maquette fidèle. Grâce à GNS3, nous avons pu concevoir la maquette donnée figure 5.

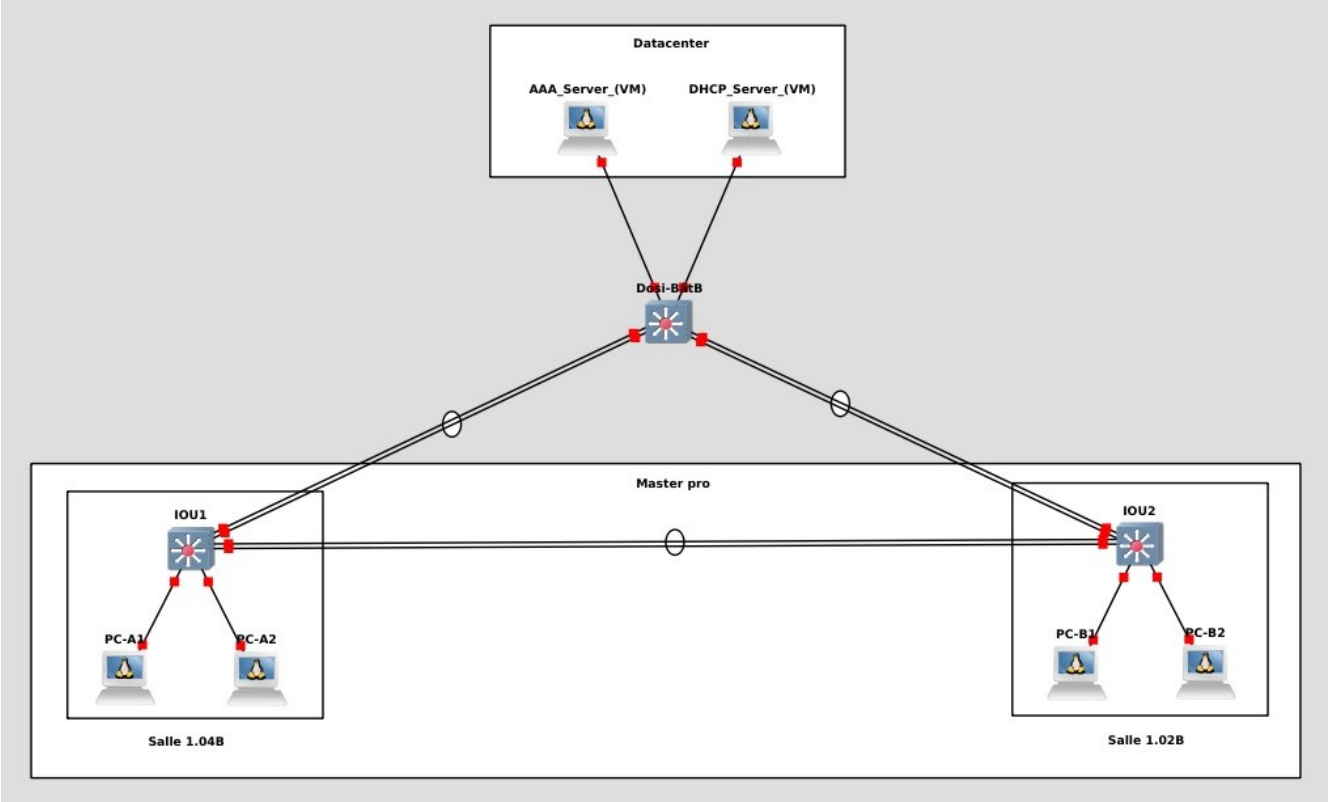

Figure 5 : Représentation de la maquette GNS3

Nous avons effectué la répartition en fonction des zones maîtrisées par le master RT ou celles gérées par la DOSI. Our rappel, les switches de nos salles de TPs sont des switches Cisco SG250X (figure 6).

Figure 6: Switch SG250-X 48P

Dans cette maquette nous avons simplifié les accès extérieurs à la salle. En effet, ne connaissant pas les configurations mise en place par la DOSI, nous n'avons pu faire qu'une installation approximative. Cependant, nous avons essayé de prendre en compte les compatibilités technologiques entre nos switches et ceux de la DOSI. Cette maquette malgré les informations dont nous disposions ne peut être complète car les postes changent d'adresse MAC à chaque redémarrage. De plus, l'accès à internet n'est pas possible pour les postes à l'intérieur de la maquette. Nous manquons de connaissance sur GNS3 pour mettre cela en place

5.3 Installation physique du réseau

5.3.1 Câblage

L'avantage de nos switches c'est que nous disposons de ports 10 Gpbs. Cependant l'installation réseau de Luminy étant vieille, elle n'est pas aux normes pour nos switches. Il nous a donc fallu tirer des câbles. Il fallait que nos deux switches soient reliés dans un premier temps à la baie de brassage et dans un second temps qu'ils soient reliés entre eux. Pour cela nous avons pu établir les distances pour nos câbles. Il fallait 2 câbles d'environ 40 mètres pour relier la salle 1.04B au local technique, et 2 câbles d'environ 60 mètres pour la relier à la salle 1.02B. Comme le réfère le plan donné figure 7.

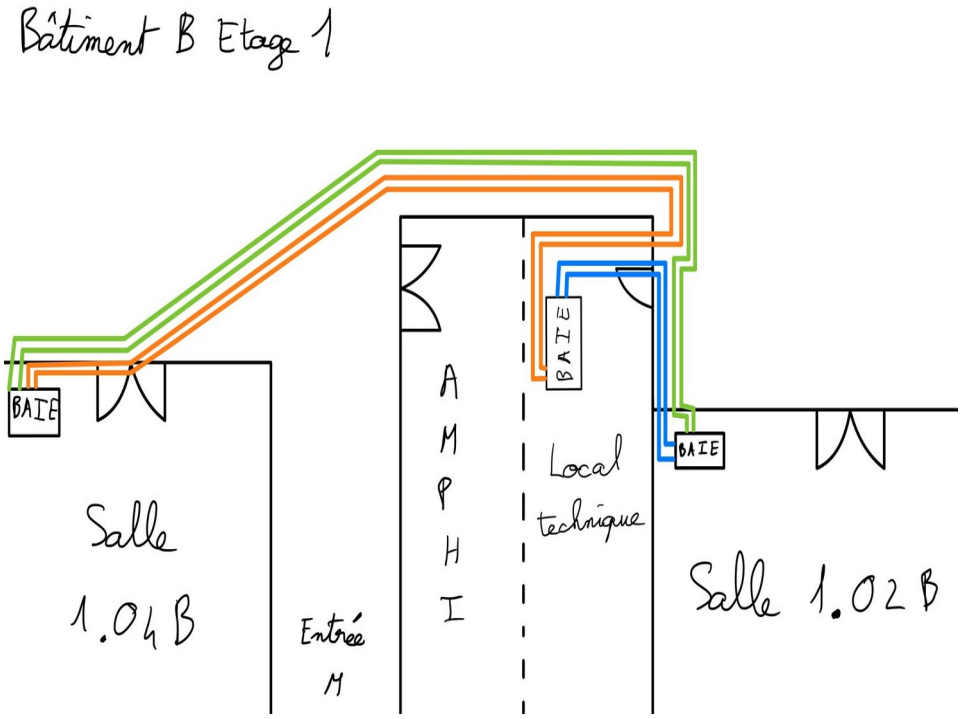

Figure 7 : Schématisation de la mise en place des câbles CAT. 7

Pour accéder à ce local technique nous devons tirer les câbles par les faux plafonds pour éviter qu'ils soient visibles et accessibles tout en évitant les traversées de poutres de béton. Les câbles sont passés et nous attendons la disponibilité de la DOSI pour le branchement à la baie de brassage du bâtiment.

5.3.2 Interconnexion des commutateurs

Dans le cadre de l'interconnexion de nos commutateurs, nous avons voulu garder une haute valeur de maintien de service. Pour cela, une notion importante est la redondance. La redondance consiste à avoir un deuxième appareil qui peut prendre le relai si le premier ne peut plus maintenir le service. Également ayant des ports 10 Gbits, nous allons profiter de cette puissance pour lier plusieurs liens entre eux afin d'avoir un effet de sécurité. Ainsi, si un des liens physiques venait à tomber, le deuxième lien pourra toujours prendre le relai. Pour cela nous allons utiliser une agrégation de lien, grâce au protocole LACP qui nous permettra d'obtenir la fusion de ces deux liens. Cependant, si on met en place cette agrégation entre nos deux switches et la salle de répartition, nous obtiendrons une architecture en triangle, ce qui mène à avoir des boucles au niveau de la couche 2. Il faut donc impérativement pouvoir verrouiller un des liens afin de pouvoir éviter ce phénomène de boucle. Pour cela, nous allons utiliser fail-over qui sera mis en place sur le switch de la DOSI. Celui-ci permettra de couper un des liens et si les deux liens du switch qui est actif tombe, fail-over changera automatiquement le chemin en laissant le trafic passer par le deuxième switch.

5.3.3 Liaison avec le serveur distant

L'accès au serveur se distinguera par deux façons différentes. L'accès via les postes informatiques et l'accès par les capteurs ou les caméras pour la transmission de leurs données. Pour cela nous allons utiliser la puissance des VLANs. Nous allons utiliser QinQ, ce qui équivaut à une double encapsulation. La première encapsulation aura lieu au niveau de notre switch. Et la deuxième encapsulation aura lieu au niveau du switch de desserte de la DOSI. Par la suite le flux sera désencapsulé par le dernier switch du datacenter en amont du serveur afin que le flux soit transmis au serveur. Le serveur possédant un firewall logiciel PFSense, il traitera les données en fonction des VLANs. Il traitera les données variables envoyées par les capteurs ou les caméras.

5.3.4 Configuration d’usine des switches et première configuration

Dès lors que nous avons reçu nos nouveaux switches, il a fallu apprendre à les utiliser et savoir comment les configurer. Ces switches ne possédant pas d’interface par port console, il a fallu passer par une interface WEB pour la configuration. Par défaut Cisco à mis en place un système d’adressage fixe et le switch possèdera l’adresse 192.168.1.254. Ainsi, si nous ne raccordons pas le switch à un service DHCP, nous devrons mettre dans le réseau 192.168.1.0/24 pour pouvoir configurer ce switch. Une fois l’accès au switch mis en place, il a fallu créer un compte administrateur, mais également choisir une méthode de configuration plus sécurisée, par exemple l’utilisation de SSH qui permet d’avoir le chiffrement de bout en bout. Après avoir configuré tout ces accès il était temps de configurer nos premières interfaces. Cependant un problème est survenu : à peine une adresse ou une modification sur une interface était faite le switch était bloqué. Après quelques recherches, une solution est apparue. En effet, Cisco met en place un VLAN temporaire sur toutes les interfaces. Si un changement est fait sur une interface, le VLAN temporaire n'est plus actif. Après avoir surmonté ce souci, nous sommes donc passés à la configuration des VLANs, d’un DHCP temporaire et à la mise en place des interfaces de notre switch. La configuration doit encore être améliorée notamment avec l’ajout des agrégations de liens par exemple.

6 Conclusion

A travers ce stage, j'ai pu acquérir de nombreuses nouvelles compétences dans les réseaux et de son administration. A travers cette mission j'ai pu me conforter dans mon autonomie de travail mais également dans mes compétences que j'ai pu acquérir lors de mes études à l'IUT. J'ai également pu travailler en équipe avec différents stagiaires ce qui renforce l'aspect de communication.

Durant cette mission j'ai pu apprendre ce que représentait de mener un projet réseau de bout en bout, depuis le besoin client jusqu'à l'installation. Cela m'a appris les démarches d'entreprise mais également les diverses contraintes qu'on peut rencontrer entre les délais pour différentes demandes qui peuvent survenir lors du projet. Ce stage me conforte également dans mon projet personnel et professionnel qui serait de travailler dans l'ingénierie réseau et de poursuivre mes études dans les réseaux en intégrant la Licence pro ASUR de Luminy.

7 Remerciements

Dans un premier temps, je tiens à remercier Didier Tonneau de m'avoir accueilli en tant que stagiaire et de m'avoir fait confiance pour pouvoir mener ce projet en autonomie avec d'autres stagiaires. Également je tiens à remercier Adrien Cailleau-Lepetit avec qui j'ai pu travailler et échanger sur plusieurs sujets. Mais également, Brandon Courtois, Anis Younsi et Marcel Tchanvoedo pour les échanges et la collaboration pour certaines parties du projet ou nous avons pu collaborer.

Je tiens également à remercier le service opérationnel du campus de Luminy, spécifiquement la DOSI et principalement Pascal Mouret, qui ont pu nous aider à la mise en place de certains aspects techniques mais également m'apprendre un grand nombre de technologies réseau que je n'ai pas pu étudier lors de mes études à l'IUT.

Je souhaite également remercier MM. Tin NGUYEN et Roland DEPEYRE de m'avoir guidé et aidé durant le projet que nous devions mener avec beaucoup d'autonomie. Et je tiens à remercier également l'équipe enseignante de l'IUT Réseaux & Télécommunications de nous avoir donné une formation de qualité.

8 Glossaire

DUT, Diplôme Universitaire de Technologie

AMU, Aix-Marseille Université

UFR, Unité de Formation et de Recherche : Structure universitaire associant des départements de formation, des laboratoires et des centres de recherche.

IOT, Internet of Things = Internet des Objets. Désigne les objets connectés destinés à être reliés à d'autres terminaux via Internet.

ANSSI, Agence Nationale de la Sécurité des Systèmes d'Information

DMZ, Demilitarized Zone. Notion dans la sécurité des réseaux, c'est l'action de protéger son système d'information via une protection double firewall

Pare-feu/Firewall, Dispositif qui protège un système informatique des tentatives d'intrusion externes.

SI, Système d'Information : Ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information, en général grâce à un réseau d'ordinateurs.

FAI, Fournisseur d'Accès Internet

DHCP, Dynamic Host Configuration Protocol. Protocole réseau chargé de la configuration automatique des adresses IP d'un réseau informatique.

VLAN, Virtual LAN réseau local virtuel servant à cloisonner logiquement les appareils au sein du même réseau physique.

QinQ, QinQ permet d'insérer plusieurs tags de VLAN dans la même trame Ethernet.

Encapsulation : Procédé consistant à inclure les données d'un protocole dans un autre protocole.

DOSI , Direction opérationnelle des systèmes d'information. Elle gère les infrastructures informatiques de l'ensemble des composantes universitaires

PoE, Power Over Ethernet

VPN, Virtual Private Network. Type de réseau informatique qui permet la création de liens directs sécurisés entre des ordinateurs distants.

IPSec, Internet Protocol Security : Regroupe un ensemble de protocoles, qui utilisent des algorithmes destinés à transporter des données sur un réseau IP de façon sécurisée.

PAgP, Port Aggregation Protocol

LACP, Link Aggregation Control Protocol

Adresse IP, Numéro d'identification de chaque appareil connecté à un réseau utilisant le protocole Internet.

ARP, Address Resolution Protocol. Protocole utilisé pour traduire une adresse de protocole de couche réseau (typiquement une adresse IPv4) en une adresse de protocole de couche de liaison (typiquement une adresse MAC).

Authentification, Processus par lequel un système informatique s'assure de l'identité d'un utilisateur.

Baie de brassage, Armoire technique qui centralise des éléments de réseaux informatiques.

Commutateur/switch, Equipement qui fonctionne comme un pont multiport et qui permet de relier plusieurs segments d'un réseau informatique entre eux.

Datacenter, Centre de données, Infrastructure composée d'un réseau d'ordinateurs et d'espaces de stockage.

Docker, Logiciel libre permettant de lancer des applications dans des conteneurs logiciels qui profitent mieux des composants natifs de l'ordinateur.

Machine virtuelle ou VM, Environnement entièrement virtualisé qui fonctionne sur une machine physique. Elle exécute son propre système d'exploitation (OS) et contrairement aux conteneurs, ils vont principalement virtualiser les composants informatiques pour des raisons de compatibilité.

Gbps, Gigabit per second

Fail-over, Capacité d'un équipement à basculer automatiquement vers un réseau ou un système alternatif ou en veille.

Journalisation/logging, Action de relever dans un journal (log) tous les évènements qui se produisent dans un système.

Panneau de brassage, Support d'interconnexions qui se place en général dans une baie de brassage. On y connecte des cordons de brassage afin de relier les différents périphériques entre eux.

Réseaux locaux/LAN, Local Area Network, Réseau informatique local de petite taille.

SNMP, Simple Network Management Protocol. Protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.

SSH, Secure Shell. Protocole de communication sécurisé avec des clés de chiffrement.

STP, Spanning Tree Protocol. Protocole réseau de niveau 2 permettant de déterminer une topologie réseau sans boucle dans les LAN avec ponts

MAC, Media Access Control. Identifiant physique stocké dans une carte réseau ou une interface réseau similaire.

9 Bibliographie

AMIDEX, (05/2021). *Des projets pédagogiques innovants*
https://www.univ-amu.fr/system/files/2021-05/Catalogue_formations_AMidex_2021_05_03.pdf

GNS3, (2021). *Getting Started with GNS3*
https://docs.gns3.com/docs/

L'ANSSI, (19/06/2020). *Recommandations relatives à l'interconnexion d'un système d'information à internet*
https://www.ssi.gouv.fr/uploads/2020/06/anssi-guide-passerelle_internet_securisee-v3.pdf

L'ANSSI, (30/03/2013). *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*
https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_Politique_pare_feu_NoteTech.pdf

L'ANSSI, (04/08/2016). *Recommandations et méthodologie pour le nettoyage d'une politique de filtrage réseau d'un pare-feu*
https://www.ssi.gouv.fr/uploads/2016/08/np_nettoyage-politique-pare-feu.pdf

L'ANSSI, (07/08/2018). *Recommandations de déploiement du protocole 802.1X pour le contrôle d'accès à des réseaux locaux*
https://www.ssi.gouv.fr/uploads/2018/08/guide_802.1x_anssi_pa_043_v1.pdf

L'ANSSI, (24/06/2016). *Recommandations pour la sécurisation d'un commutateur de desserte*
https://www.ssi.gouv.fr/uploads/2016/07/nt_commutateurs.pdf