Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Conception d'une architecture réseaux

Dany LAU

LE CINAM

Responsable entreprise : Didier Tonneau

Responsable académique : Roland Depeyre

2019

Table des matières

1 Introduction

Le Master de Réseaux et Télécommunications (R&T) souhaite préparer les étudiants aux métiers de demain dans le domaine du Numérique. Pour cela un parcours de master a été dédié à l'Internet des objets (IoT pour Internet of Things). L'internet des objets désigne un système où les objets physiques sont connectés à Internet. Il s'agit également de systèmes capables de créer et transmettre des données afin de créer de la valeur pour ses utilisateurs à travers divers services (agrégation, analytique…).

L'UIT (Union Internationale des Télécommunications) définit l'Internet des Objets comme « *une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution* ».

Figure 1 : Campus de Luminy

L'IoT est déjà, un grand enjeu dans le monde et dans tous les domaines, que ce soit pour les grandes entreprises, mais aussi pour de simples utilisateurs dans leur vie quotidienne. Pour répondre à la demande grandissante de personnes compétentes dans l'IOT, l'Equipe Pédagogique du master R&T du Parc de Luminy a décidé de lancer le projet ECO. Mon stage s'effectue dans le cadre de ce projet.

2 Contexte

2.1 Le projet ECO

L'idée sous-jacente du projet ECO est le couplage entre l'Enseignement, le Service Opérationnel informatique d'AMU (DOSI*), les enseignants chercheurs et l'industrie.
Le but du projet ECO est de doter AMU* d'une Plateforme de Service IoT, ouverte aux étudiants, considérés comme Ingénieur Support ou Technique, et aux Enseignants-Chercheurs d'AMU et l'industrie, les clients. L'idée est qu'au travers de la plateforme, un client puisse poster un projet dans le domaine du Numérique et de l'IoT. Après validation du projet par l'Equipe Pédagogique du master, le projet sera affiché en ligne et les étudiants d'AMU pourront postuler pour intégrer une équipe qui mènera à bien la réalisation du projet.
Les Enseignants Chercheurs d'AMU pourront également demander aux étudiants de développer des outils connectés pédagogiques. Le projet ECO associera donc les étudiants à la transition numérique dans la pédagogie au sein de notre université. Cela permettra d'user librement de leurs aptitudes à utiliser l'environnement pour imaginer des fonctions, et nous aider à franchir les barrières naturelles que la génération des enseignants se fixe.
Pour mener à bien ce projet, nous étions quatre stagiaires répartis sur trois missions:

1. La première concerne la conception et l'installation d'une architecture réseaux dans les salles de travaux pratiques dédiés aux objets connectés. Cette tâche a été réalisée par moi-même et un autre étudiant de l'IUT Réseaux et Télécoms.

2. La deuxième implique la réalisation de la plateforme web, réalisée par un étudiant en L3 Informatique.

3. La troisième concerne l'installation et la configuration d'un serveur WEB dans la Data Center du bâtiment TPR1 pour héberger le site et stocker les données venant des capteurs des deux salles. Cette tâche est réalisée par un étudiant du M1 Réseaux et Télécommunications.

La mission principale de mon stage était de concevoir une architecture réseaux dédiée à l'IoT pour deux salles de travaux pratique du Bâtiments B sur le campus de Luminy, qui permettrait aux étudiants de connecter différents capteurs sur un réseau privé et sécurisé, et ensuite l'installer dans les deux salles de travaux pratiques.

2.2 Organisme d'accueil : AMU

L'université d'Aix-Marseille est née de la fusion des universités de Provence, Méditerranée et Paul-Cézanne en 2012. Avec plus de 75000 étudiants et 8000 employés, elle fait partie des plus grandes universités de France, et une des premières universités françaises au classement de Shanghai. Avec un budget de 720 millions d'euros par an, AMU a pu se doter de 120 structures de recherches comme par exemple le CINAM*. C'est au sein de ce laboratoire que j'ai pu effectuer mon stage de fin d'études. Situé sur le campus de Luminy à Marseille, le CINAM est spécialisé dans les Nanosciences. Mon responsable de stage Didier Tonneau est enseignant-chercheur au CINAM, et également le responsable du Master Réseaux et Télécommunications.

2.3 Le financement du projet: AMidex

L'initiative d'excellence d'Aix-Marseille a été définitivement créée en avril 2016, son objectif est de valoriser et développer le potentiel du site d'Aix-Marseille, cet objectif est traduit par deux vecteurs: à savoir les appels à projets, ou appels à candidatures et par la mise en place d'actions structurantes. Le projet ECO a été financé par l'Académie d'Excellence de AMIDEX.

3 Conception de l'Architecture réseaux

3.1 L'Architecture des salles

La mission principale de ce stage était de concevoir et d'installer une nouvelle architecture réseaux, pour créer un LAN* dédié aux travaux pratiques sur l'IoT. Les deux salles, qui seront aménagées sont situées dans le Bâtiment B du Campus de Luminy (figure 2).

Figure 2 : Le Bâtiment B de Luminy

La première salle, est une ancienne salle de TP du Master Réseaux et Télécommunications, et mesure environ 73 m² (figure 3).

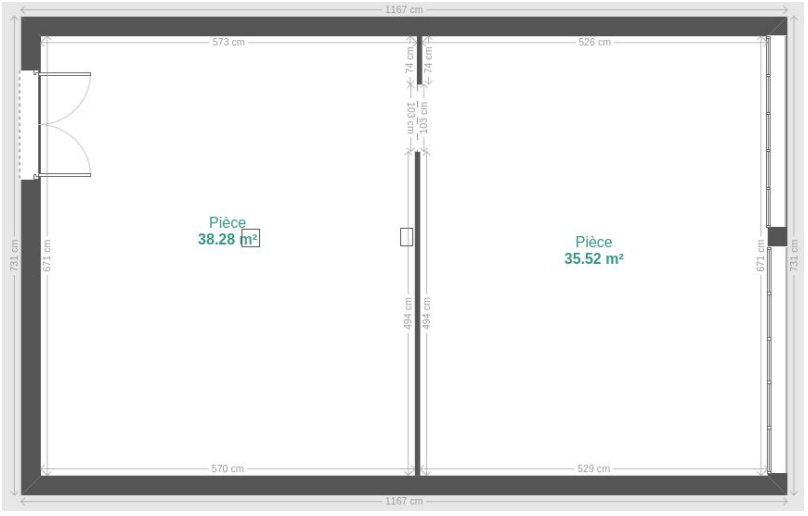

Figure 3 : Salle de TP 1 du Bâtiment B

La deuxième, est une ancienne salle de TP optique qui sera réaménagée pour l'IoT. Elle mesure 65.5m² (figure 4).

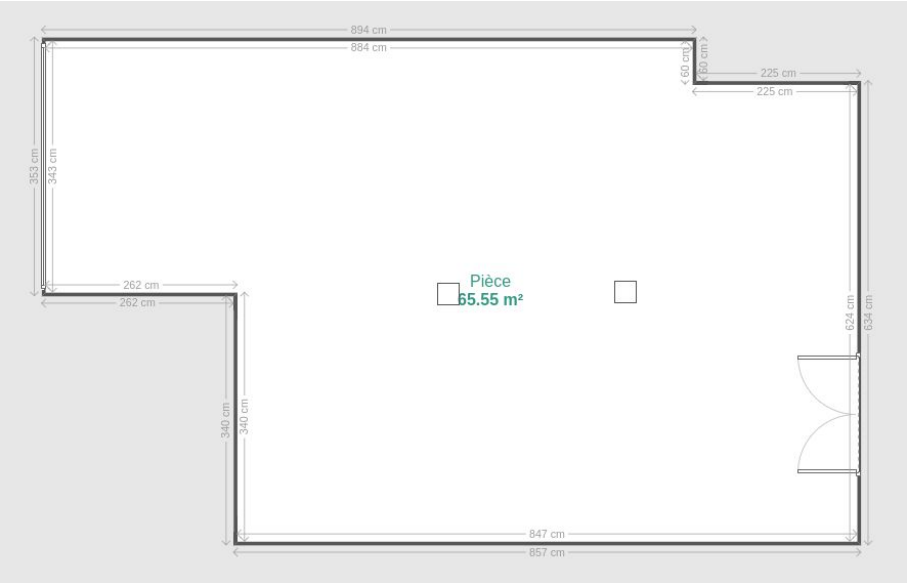

Figure 4 : Salle de TP 2 du Bâtiment B

Dans ces salles, trois installations majeures seront mises en places pour permettre des TPs sur l'IoT:

- L'Installation de ports RJ45 catégorie 6 femelle permettant le branchement de capteurs, sur le réseau dédié à l'IoT.

- L'installation d'un système d'éclairage Intelligent et Interactive sera mise en place, et remplacera le système actuelle. Ce système aura un but pédagogique, en permettant aux étudiants d'interagir directement sur les luminaires à l'aide de capteurs et de différents outils. L'étude de ce système a fait partie de mon travail, mais son câblage est prévu l'année prochaine.

- Un système de caméras de surveillance sera installé pour des projets futurs sur l'IoT,

Les deux salles n'étant pas neuves, elles possèdent déjà une installation réseaux et électrique dont il a fallu prendre compte. Pour des raisons pratiques l'installation des ports RJ45, sera superposée à l'installation déjà existante.

3.2 La Passerelle d'interconnexion

Ma seconde mission était de mettre en place une passerelle d'interconnexion sécurisée, en suivant les recommandations de l'ANSSI*(voir Annexe page 2). Une architecture passerelle d'interconnexions, permet d'interconnecter un réseau à un autre, dans notre cas un réseau privé (LAN*) à un réseau externe (WAN*) comme internet. Une passerelle d'interconnexion est dite sécurisée, quand des mesures sont mises en places pour empêcher ou au moins minimiser les attaques provenant du WAN (voir Annexe page 5). Pour définir les sécurités à mettre en place, il faut définir les besoin de l'entreprise, les activités qu'elle souhaite développer et son budget. Il n'existe pas une passerelle d'interconnexion sécurisée universelle, chaque passerelle est conçue au cas par cas. Dans notre cas on souhaite ouvrir un site web, où les utilisateurs pourront consulter et déposer des projets.

Aucune donnée sensible ne sera stockée ou ne transitera par le site, ce n'est donc un point majeur de la sécurité. Le point le plus important, est qu'en aucun cas les utilisateurs venant du WAN ne puisse accéder au LAN et à ses données. La sécurité à mettre en place au vue des besoins cités précédemment, des ressources disponibles et des recommandations de L'ANSSI, nous ont décidés à adopter une architecture passerelle d'interconnexion basée sur deux pare-feux* avec une DMZ* (figure 5).

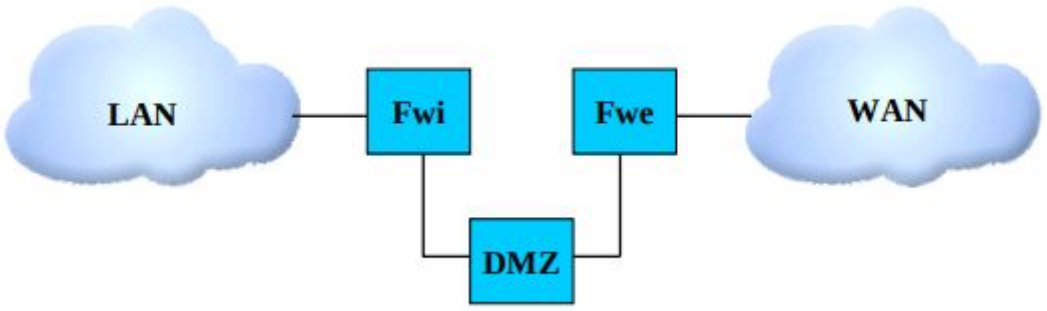

Figure 5: Architecture basée sur deux pare-feux avec coupure physique.

- Un pare-feu externe (FWe) entre le WAN et la DMZ, pour filtrer les données qui transitent et qui seront autorisées par notre politique de sécurité.
- Une DMZ qui contiendra le serveur LAMP*, où sera hébergé le site mais aussi certaines données du LAN.
- Un pare-feu externe (FWi) entre le LAN et la DMZ, même principe que le pare-feu externe mais qui servira aussi de rempart de secours entre le LAN et le WAN, au cas où le pare-feu externe soit compris.

La Politique de sécurité :

Le pare-feu externe doit accepter les paquets de données* suivants :

- Autoriser les paquets HTTP*/HTTPS* provenant du WAN vers le serveur Web.
- Autoriser les paquets HTTP/HTTPS provenant du serveur Web vers le WAN.
- Refuser tout le reste.

Le pare-feu interne les paquets de données suivants :

- Autoriser les paquets HTTP/RTSP* provenant des caméras à destination du serveur Web.
- Autoriser les paquets SNMP*/SYSLOG*/HTTP/SSH* provenant de l'ordinateur de supervision vers le Serveur Web,le pare-feu externe et interne.
- Autoriser les paquets UDP*/TCP* provenant des capteurs vers le serveur Web.
- Refuser tout le reste.

Toute cette infrastructure sera stockée dans le data-center* sécurisé de la DOSI, qui possède et gère un pare-feu général.

Pour tester notre politique de sécurité, nous avons utilisé le logiciel Packet Tracer. Packet Tracer est un logiciel simulation de matériel réseau Cisco. Ce logiciel est très utile car il permet de faire des simulations d'architectures réseaux et de configuration réseaux. Packet tracer n'utilisant que des équipements de la marque Cisco, la politique de sécurité sera mise en place sur des pare-feux ZBF*.

```
class-map type inspect match-any FORINTERVLAN
 match protocol snmp
 match protocol ssh
 match protocol syslog
 match protocol rtp
 match access-group 101
class-map type inspect match-any FORLAN
 match protocol syslog
 match protocol snmp
 match protocol tcp
 match protocol udp
 match protocol ssh
 match protocol rtp
 match protocol http
 match protocol https
class-map type inspect match-any FORINTERLAN
!
policy-map type inspect LAN-TO-INTERVLAN
 class type inspect FORLAN
  inspect
!
policy-map type inspect INTERVLAN-TO-LAN
 class type inspect FORINTERVLAN
  inspect
!
!
!
zone security LAN
zone security INTERLAN
```

```
zone-pair security ZP-LAN-TO-INTERVLAN source LAN destination INTERLAN
 service-policy type inspect LAN-TO-INTERVLAN
zone-pair security ZP-INTERLAN-TO-LAN source INTERLAN destination LAN
 service-policy type inspect INTERVLAN-TO-LAN
!
!
interface GigabitEthernet0/0
 ip address 10.10.10.4 255.255.255.0
 zone-member security LAN
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 10.10.12.1 255.255.255.0
 zone-member security INTERLAN
 duplex auto
 speed auto
!
```

Figure 6 : Configuration du pare-feu interne

La figure 6, représente la configuration du pare-feu entre le LAN et la DMZ selon les critères cités précédemment. Avec cette configuration seuls les protocoles indiqués seront autorisés à traverser le pare-feu. Ci-dessous vous pouvez trouver la configuration du pare-feu entre le WAN et la DMZ (figure 7)

```
class-map type inspect match-any from-wan-class
 match protocol http
 match protocol https
 match protocol dns
class-map type inspect match-all server-to-wan-class
 match protocol http
 match protocol https
 match protocol dns
!
policy-map type inspect from-wan-policy
 class type inspect from-wan-class
  inspect
!
policy-map type inspect server-to-wan-policy
 class type inspect server-to-wan-class
  inspect
!
!
!
zone security WAN
zone security SERVER
```

```
zone security WAN
zone security SERVER
zone-pair security ZP-FROM-WAN source WAN destination SERVER
 service-policy type inspect from-wan-policy
zone-pair security ZP-SERVER-TO-WAN source SERVER destination WAN
 service-policy type inspect server-to-wan-policy
!
!
interface GigabitEthernet0/0
 ip address 192.168.12.1 255.255.255.0
 zone-member security SERVER
 duplex auto
 speed auto
!
```

Figure 7 : Configuration du pare-feu externe

3.3 Plan d'adressage et Conception des VLANs

Le parc informatique de Luminy est géré par la DOSI, dans ce contexte ce Service nous a attribué un VLAN* avec une plage d'adresses défini (figure 8).

Figure 8 : Plage d'adresse fourni par la DOSI

Pour des raisons de sécurité et pour faciliter la gestion du réseau, nous divisons notre réseau en plusieurs VLANs.

Un VLAN est un réseau virtuel, il permet de découper au niveau logique et non physique un réseau. Sans VLAN un switch* considère toutes ses interfaces comme faisant partie du même réseau (figure 9)

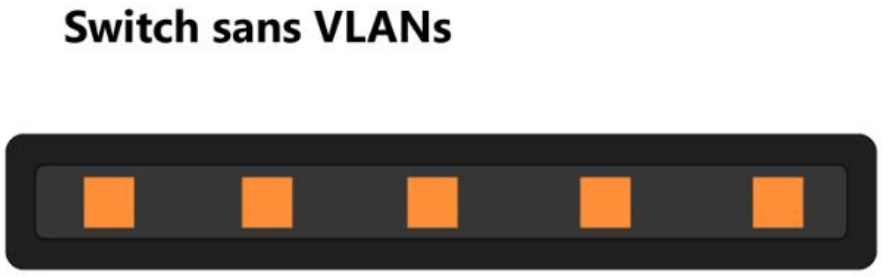

Figure 9 : Switch sans VLANs

Dans ce cas les risques majeurs sont :

- Si un appareil du réseau est compromis par un attaquant, il est lui est très facile d'avoir accès aux autres appareils du réseau, et ainsi compromettre tout le réseau.
- Si le nombre d'appareils connectés sur le réseau est conséquent, alors le domaine de diffusion sera grand. Un domaine de diffusion est l'ensemble des appareils qui peuvent communiquer entre eux sans sortir du réseau. Plus il est grand, plus les appareils du réseau recevront des messages de diffusion, et seront donc plus lents à répondre.
- Ce problème concerne aussi le domaine de collision. Un domaine de collision est un ensemble d'appareils qui partagent le même média de communication. Plus le nombre d'appareils est grand, plus la chance de collision entre les paquets de données sont grand, donc la chance que les données n'arrive pas à destination.

Avec des VLANs (figure 10), ces problèmes peuvent être résolus.

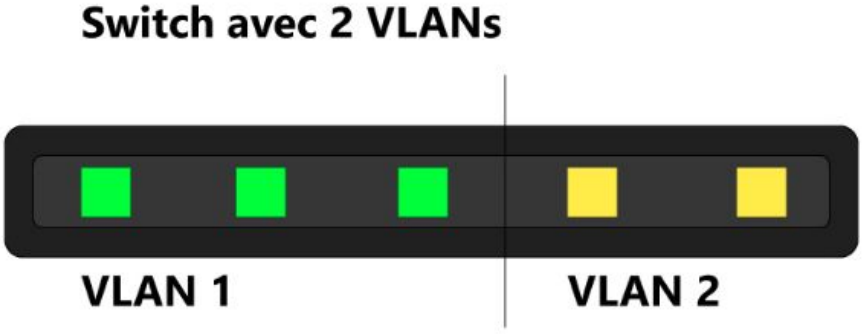

Figure 10 : Switch avec deux VLANS

- En découpant le réseau en plusieurs sous-réseaux, les VLANs permettent d'isoler au niveau logique les appareils qui ne sont pas du même réseau. Ainsi si un appareil du VLAN 1 est compromis par un attaquant, il aura plus de difficultés à attaquer un appareil du VLAN 2.
- Les VLANs permettent de réduire le problème d'un trop grand domaine de diffusion ou de collision. En découpant le réseau en plusieurs sous-réseaux, ils réduisent ainsi dans le même temps les domaines de collision et de diffusion.
- Autre avantage des VLANs, ils permettent une meilleure gestion du réseau . Pour prendre un exemple simple, il est plus compliqué de gérer une classe de 60 élèves que trois classe de 20 élèves. Il est donc plus simple de gérer trois VLANs avec 20 appareils, que 60 appareils dans le même réseau.

Nous allons découper notre réseau en six VLANs:

- Un VLAN pour le système d'éclairage intelligent.
- Un VLAN pour le système de caméra surveillance.
- Un VLAN pour les capteurs.
- Un VLAN un d'administration
- Un VLAN pour la connexion entre le pare-feu interne et le Serveur Web.
- Un VLAN pour la connexion entre le WAN et le Serveur Web.

Figure 11 : Plan d'adressage des VLANs

Nous avons simulé sur Packet Tracer, la configuration des VLANs sur un switch pour savoir si elle été opérationnel et avons nommés les VLANs comme suit (figure 12):

```
10   LUMINAIRES                      active
20   CAMERAS                         active
30   CAPTEURS                        active
40   Administrations                 active
50   LAN-DMZ                         active
60   WAN-Serveur                     active
```

Figure 12 : Configuration des noms des VLANs

3.4 Le Routage

Le routage désigne le procédé par lequel les différents réseaux communiquent entre eux. Il existe deux types de routage : le routage statique* et le routage dynamique* . Notre réseau étant de petite taille, nous pouvons nous permettre d'utiliser un routage statique. Ses avantages sont multiples :

- Il permet un meilleur contrôle du trafic qui transite entre les réseaux. Et par conséquent une sécurité renforcée.

- Une baisse de la consommation des ressources.

On utilise uniquement le routage dynamique si cela est nécessaire, par exemple si les réseaux sont volumineux en terme de terminaux (figure 13).

	Routage statique	Routage dynamique
Mis en œuvre dans des	Petits réseaux	Grands réseaux
Configuration	Manuel	Automatique
Les Routes	Défini par l'utilisateur	Les itinéraires sont mis à jour en fonction du changement de topologie.
La construction de la table de routage	Les routes sont remplis à la main	Les routes sont remplis dynamiquement dans la table.
Algorithmes de routage	N'utilise pas d'algorithmes de routage complexes.	Utilise des algorithmes de routage complexes pour effectuer des opérations de routage.
Sécurité	Fournit une haute sécurité.	Moins sécurisé en raison de l'envoi de diffusions et de multidiffusions.
Échec du lien	L'échec de liaison bloque le routage.	L'échec de liaison n'affecte pas le routage.

Figure 13 : Tableau comparatif entre le routage dynamique et statique

En ce qui concerne le routage inter-VLAN, nous utiliserons une architecture dites Router-On-a-Stick (figure).

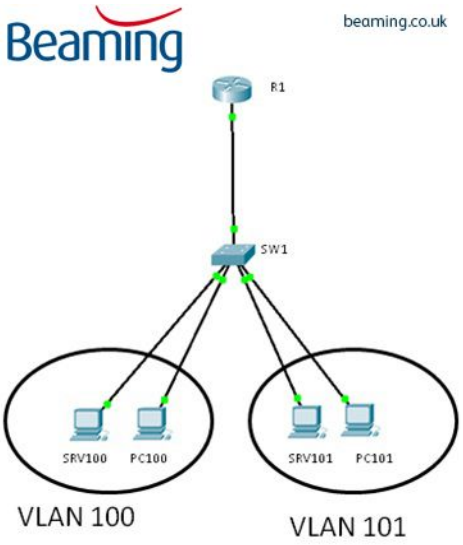

Figure 14 : Exemple d'architecture Router-On-a-Stick

Une architecture Router-On-a-Stick revient à diviser l'interface réseau du routeur relié à un switch possédant plusieurs VLANs, en sous-interfaces de nombre égal au nombre de VLANs, qui serviront de passerelle par défaut aux équipement des VLANs(figure 15).

```
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 10.10.10.1 255.255.255.0
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 10.10.11.1 255.255.255.0
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 10.10.12.1 255.255.255.0
!
interface GigabitEthernet0/0.40
 encapsulation dot1Q 40
 no ip address
!
interface GigabitEthernet0/0.50
 encapsulation dot1Q 50
 ip address 10.10.14.1 255.255.255.0
!
interface GigabitEthernet0/0.60
 encapsulation dot1Q 60
 ip address 10.10.15.1 255.255.255.0
!
```

Figure 15 : Configuration des sous-interfaces

4 La Proposition d'offre

4.1 Définition du besoin

Après la conception théorique de l'architecture, nous avons pu passer à la définition du besoin en terme de matériel et d'équipement. Cette conception et installation étant faite pour permettre des travaux pratiques, il était important de connaître les TPs qui seront effectués et les projets que souhaitent mettre place les enseignants.
Une discussion avec le responsable du projet ECO, nous a permis de définir les besoins suivants:

- Des ports RJ45 catégorie 6 (figure 16) pour permettre le branchement de différents capteurs. Si possible deux ports RJ45 par poste de travail, pour permettre à deux étudiants de travailler sur le même poste. Il y a au total pour les deux salles trente postes de travail, donc il nous faudra soixante port RJ45

Figure 16 : Port RJ45

- Un système d'éclairage intelligent et interactif, qui sera programmable par les étudiants
- Un système de surveillance, qui servira pour de futurs projets actuellement en phase de conception
- Des ports RJ45 supplémentaires, pour des projets encore non définis mais à venir, comme un système de volets connectés

4.2 Choix du matériel

Avec les besoins définis, nous avons pu commencer à choisir les différents matériels et solutions à mettre en place. C'est ainsi que nous avons créé une proposition d'offre, contenant des comparatifs et des explications sur les choix finaux des matériels (Proposition d'offre disponible dans l'Annexe).

Le systèmes d'éclairage intelligent:

L'installation d'un nouveau système d'éclairage intelligent à plusieurs objectifs. Tout d'abord un but écologique et économique, avec un éclairage intelligent qui s'adapte en fonction de plusieurs paramètres et ainsi permettre un gain d'énergie et, d'une réduction de la pollution. Mais ce système a pour but principal la pédagogie notamment pour les TPs d'IoT.

Il doit donc répondre à des critères bien précis:

- Être interactif, c'est-à-dire qu'il doit pouvoir adapter sa luminosité selon différents paramètres
- Il devra permettre aux étudiants un contrôle total sur les luminaires. Ainsi ils pourront programmer le système d'éclairage, et y incorporer différents capteurs.

L'unique entreprise qui puisse fournir actuellement un système d'éclairage répondant à nos exigences est Philips Lighting (aujourd'hui Signify), avec son éclairage fonctionnant à l'aide de la technologie PoE* (voir Annexe choix du système d'éclairage page 24).
Le nouveau système remplacera l'ancien, donc il est nécessaire d'acheter le même nombre de luminaires (figure 17) (voir Annexe plan d'éclairage), ce qui nous fait un total de 19 luminaires pour les deux salles.

Figure 17 : Luminaire Philips lighting

Si l'installation de ce système se passe correctement et que les résultats sont satisfaisants, le dispositif pourrait à l'avenir, être étendu sur tout le bâtiment B de Luminy.

Le système de vidéosurveillance:

Le système de vidéosurveillance sera couplé aux systèmes d'éclairage. Les étudiants pourront se servir des caméras pour développer des projets, comme la détection d'émotion et ainsi diminuer/augmenter la luminosité si un étudiant s'endort.
Comme pour le système d'éclairage, celui de surveillance doit correspondre à certaines exigences:

- Les caméras doivent être compatibles avec la technologie PoE, pour faciliter leur utilisation et installation.
- Les caméras devront être installées en hauteur et avoir une grande résistance, pour résister au vandalisme.
- Si possible posséder un système de détection de mouvement.
- Une résolution haute définition, minimum de 1920x1080.
- Le système de surveillance devra avoir un visuel sur l'ensemble des pièces, sans laisser d'angle mort. Pour cela nous avons développé un plan d'installations des caméras (figure 18 et 19), et ainsi nous avons pu nous rendre compte, de la nécessité de commander au total huit caméras.

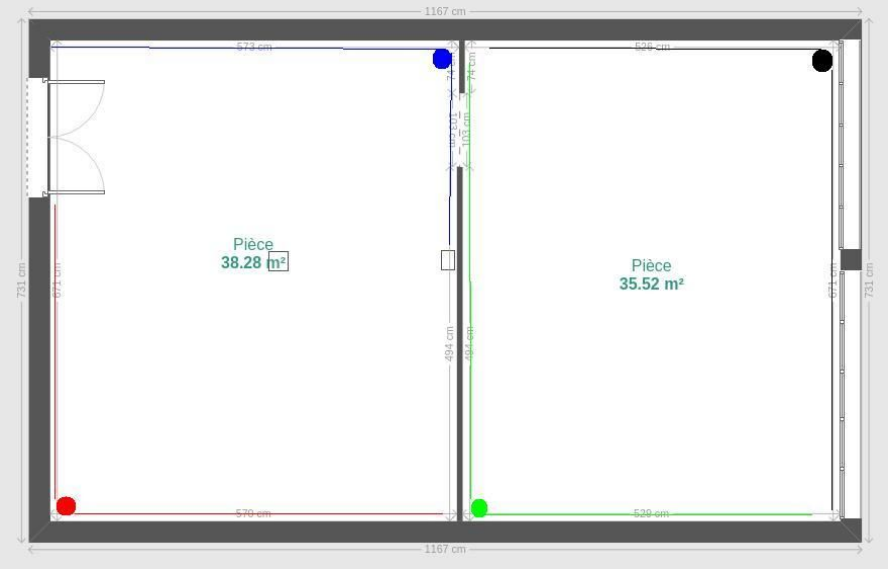

Figure 18 : Position des caméras(les points de couleurs) de la salle de TP1

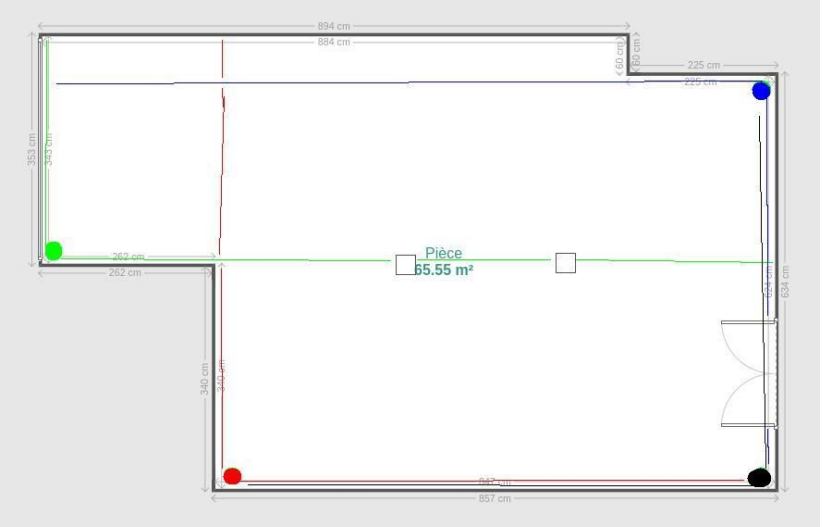

Figure 19 : Position des caméras(les points de couleurs) de la salle de TP2

Après comparaison des différents modèles (voir Annexe page 20), nous avons choisi la caméra DCS-4602EV de D-LINK(figure 20) car elle correspondait à nos exigences et possédait le meilleur rapport qualité prix.

Figure 20 : Caméra D-LINK DCS-4602EV

Les Switchs:

Les switchs sont une partie primordiale de notre architecture réseaux, il est donc important de bien les choisir. La caractéristique la plus importante et indispensable dans la sélection du Switch, est la disponibilité de la technologie PoE. Nos systèmes de vidéosurveillance et d'éclairage fonctionnent grâce à l'aide de la technologie PoE, il est donc impératif de posséder un switch PoE pour alimenter ces appareils. Il faut aussi prendre en compte le nombre de port RJ45, qui doit être supérieur aux nombre de ports nécessaires pour permettre une évolutivité du réseau. En comptant les soixante ports RJ45 pour les postes de TPs, les dix-neuf luminaires PoE, et les huit caméras PoE, nous avons besoin au minimum 86 port RJ45. Nous avons choisi des switchs Cisco Catalyst Series PoE-48 (figure 21) avec 48 port RJ45 chacun, pour un total de 96 ports disponibles.

Figure 21 :Switch Cisco Catalyst Series PoE-48

Les Pare-Feux:

Nous avons choisi précédemment une architecture passerelle d'interconnexion sécurisée à deux pare-feux de marques différentes, suivant en cela les préconisations de l'ANSSI. (Voir Annexe p10). Ces pare-feux ont pour principale mission d'assurer une protection du LAN des attaques provenant du WAN. Mais ils ont aussi une mission secondaire à but pédagogique, car la maintenance de ces pare-feux sera assurée par les étudiants du master réseaux et télécommunications. Les étudiants pourront ainsi s'exercer sur de vrais pare-feux dans un cas de fonctionnement réel. En prenant compte ces objectifs et que le master possède déjà des pare-feux Cisco, nous avons choisi des pare-feux de la marque Stormshield pour diversifier les TPs de master.
Le modèle qui a été retenu est le Stormshield SN3100 (figure 22), qui est agrée par l'ANSSI.

Figure 22 : Pare-feu Stormshield SN3100

Le Serveur Web:

Le Serveur Web sera hébergé dans le data-center de Luminy(figure 23). Le data-center de luminy est une salle hautement sécurisée avec un accès très réglementé par la DOSI, qui nous a conseillé de prendre un serveur Dell possédant la technologie IDRAC (Integrated Dell Remote Access Controller). Cette technologie permet une gestion totale du serveur à distance.

Figure 23 : Data-Center de Luminy

Le Serveur devra donc être obligatoirement de la marque Dell, possesseur du Marché d'Aix-Marseille Université, et répondre aux besoins suivants:

- Un grand niveau de stockage, pour stocker les données des capteurs et des caméras.
- Des ressources conséquente, pour faire fonctionner les différents services comme le service Web.

Le Serveur qui a été retenu est le Serveur Dell PowerEdge R740, qui répond à tous nos critères et qui permettra une évolution dans le futur (voir Annexe p).

Matériels Annexe:

Les matériels figurant dans cette partie, sont du matériel obligatoire pour l'installation de l'architecture réseaux mais ne requièrent aucune exigence particulière.

Les câbles réseaux: Il a été calculé que 150 mètres de câbles réseaux seraient suffisants pour les deux salles de travaux pratiques. Vu la différence de prix qui est minime nous avons décidé de prendre des câbles de type S/STP* catégorie 6 (figure 24), qui est le câble de meilleur qualité actuellement.

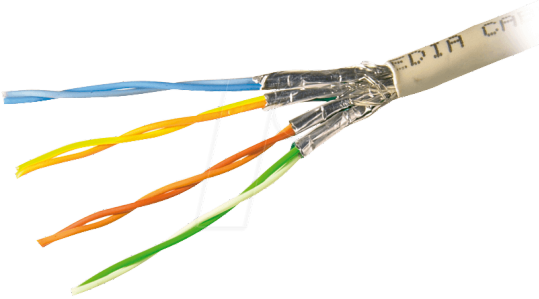

Figure 24 : Câbles S/STP cat6

Les goulottes de câbles: Pour faire passer les câbles nous avons besoin de goulottes (figure 25). Pour l'ensemble des salles, nous avons calculé que 30 mètres de goulottes seraient suffisants, avec une largeur de 60 mm et hauteur de 100 mm.

Figure 25 : Goulottes de câbles

La baie de brassage: Une baie de brassage permet de stocker nos équipements réseaux comme des routeurs ou des switchs. Il a été demandé que chaque salle soit équipé d'un switch, pour les stocker nous aurons besoin donc de deux baies de brassage. Une baie de brassage de petite taille est largement suffisante pour stocker un switch. L'échelle de mesure des baies de brassage se mesure en Unités (symbole U). Le modèle de plus petite taille mesure 4 U (figure 26).

Figure 26 : Baie de brassage de 4U

4.3 Mise en place des commandes

Le choix du matériel étant défini et validé par le responsable du projet, l'étape suivante était de trouver les fournisseurs adéquates et de les contacter, pour les équipements suivants :

- Le système d'éclairage
- Les caméras de surveillance
- Le Serveur Dell
- Les pare-feux
- Les bobines de câbles
- Les goulottes de câbles
- Les baies de brassages

Le projet ECO est financé par l'initiative AMIdex qui impose une liste de fournisseurs. L'avantage est que cette liste nous a permis de repérer et contacter facilement les différents fournisseurs. Le désavantage était qu'après vérification, nous devions passer par un fournisseur différent pour chaque équipement, alors que si nous n'avions pas de fournisseurs imposés, nous aurions pu passer par un seul fournisseur où une grande partie des équipements souhaités était disponible (Amazon par exemple).

Les devis concernant le système d'éclairage (Philips Lighting), la goulotte (Cabus&Raulot, Marseille), les caméras (LDLC.pro), le câble (UGAP) sont donnés en annexe liste des devis page 33.

4.4 Installation du matériels

L'installation du matériel, débutera lors du mois de juillet lorsque tous les équipements seront livrés. L'installation commencera par la mise des goulottes de câbles et des prises RJ45, qui seront superposés au réseau existant.

Figure 27 : Installation actuelle des goulottes de câbles

Le câblage terminé, nous mettrons en place la baie de brassage avec les switch dans chaque salle. Un câble reliera nos switchs à la baie de brassage de la DOSI, pour pouvoir un accès à internet et au serveur stocké dans le data-center.

En ce qui concerne la mise en place des pare-feux et du serveur, ils seront configurés et testés localement avant d'être implémentés dans le data-center de la DOSI.

Cette installation prendra normalement une semaine pour être achevée (figure 28).

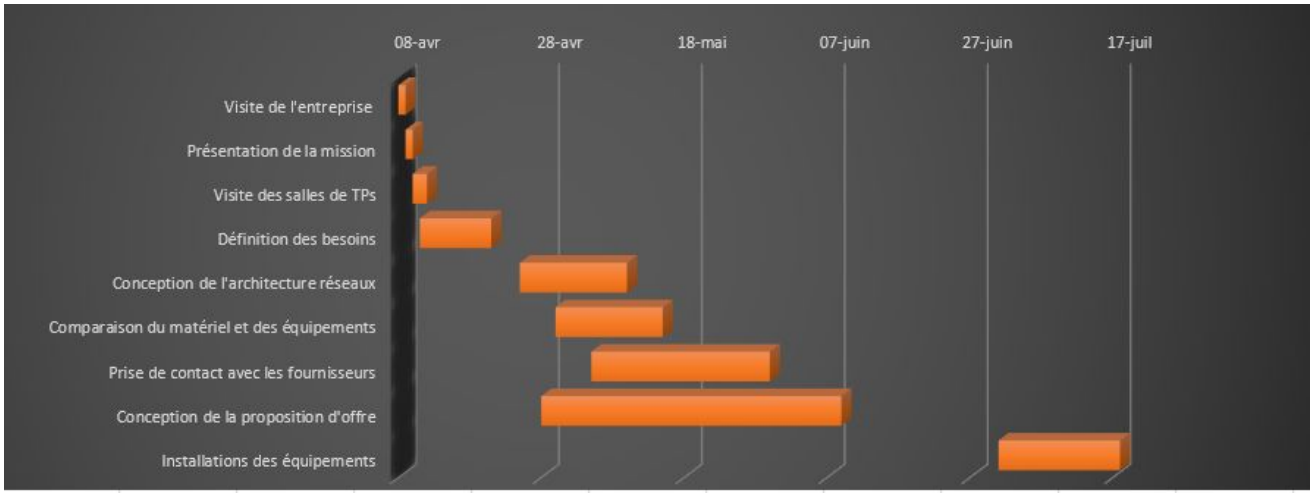

Figure 28 : Diagramme de GANTT de mon stage

4.5 Missions Annexe

Une mission annexe que j'ai effectuée lors de mon stage et qui a duré une journée, était le référencement des câbles réseaux du bâtiment de Grand Luminy (figure 29). L'Association Grand Luminy assure trois missions principales autour de l'animation et la promotion du Parc et de la création et du développement des entreprises sur le territoire. Elle aide à la création et l'incubation d'entreprise en mutualisant les ressources.

Figure 29 : Bâtiment principal de Grand Luminy

Dans le bâtiment principal, je devais mettre à jour la documentation sur le branchement des câbles. La première étape était de vérifier que les entrées et sortie correspondent à la documentation, et si ce n'était pas le cas la mettre à jour en modifiant les entrées et les sorties.

5 Conclusion

Pour conclure, ce stage de fin d'étude a été très enrichissant sur plusieurs plans.
Sur le plan technique, j'ai pu améliorer mes compétences et connaissances dans le domaine des réseaux grâce au recherche que j'ai dû effectuer pour la réalisation de ce projet ambitieux. Les documentations de l'ANSSI m'ont permis d'acquérir une connaissances et une méthodologie sur la sécurité des réseaux et la mise en place d'une politique de sécurité qui me seront très utiles pour mes futurs projets .
En ce qui concerne le savoir être, ce stage m'a donné l'occasion d'améliorer mon relationnel et mon aptitude à travailler en équipe. En effet lors de mon stage nous étions une équipe de quatre stagiaires travaillant dans le même bureau et sur le même projet, chacun d'entre nous travaillant sur des tâches différentes. Nous nous sommes néanmoins entraidés lorsque l'un d'entre nous été bloqué dans sa mission, et avons ainsi appris les uns des autres.
Sur le plan professionnel, les missions que j'ai accomplies étaient très enrichissantes et passionnantes. Actuellement à la recherche d'une alternance pour une école d'ingénieur, cette expérience professionnelle m'a permis de définir quel type de poste je souhaitais occuper en l'occurrence ingénieur avant-vente*. En plus de m'avoir permis de définir quel type de poste je souhaitais occuper, ce stage est un gros plus sur mon CV*, et les missions que j'ai réalisées durant ce stage ont impressionné beaucoup d'entreprises comme Orange et ENGIE, qui ont souhaité me proposer des postes à la suite d'entretiens.

Aujourd'hui le projet ECO n'est pas encore terminé, il prendra normalement fin en juillet (figure 30).
Ce projet m'aura marqué, et permis de progresser d'un point vu scolaire, professionnel et humaines qui me survivront dans mes futurs projets professionnel, mais aussi personnel.

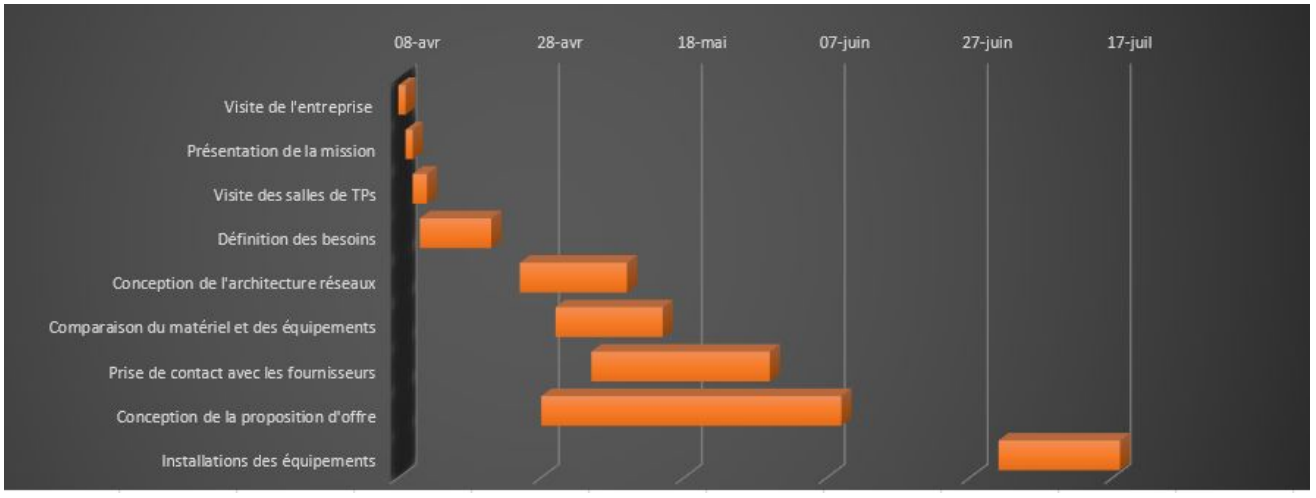

Figure 30 : Diagramme de GANTT de mon stage

Remerciements

Je tiens tout particulièrement à remercier mon responsable de stage Didier TONNEAU et toute l'équipe du CINAM pour leur accueil, pour m'avoir accepté en tant que stagiaire, et de m'avoir fait partager leur expérience professionnelle et personnelle. La confiance que m'a accordée M. Tonneau lors de mon stage, m'a permis de réaliser des missions à responsabilités, qui m'ont enrichi tant sur le plan professionnel que personnel.

Je tiens aussi à remercier Pascal Mestre et Julien Cazaubon, pour leur accueil chaleureux lors de nos interventions sur le Campus de Saint-Jérôme.

Je remercie grandement mes maîtres de stages, Roland Depeyre et Tin Nguyen qui m'ont recommandé pour ce stage. Leurs conseils et leurs écoutes m'ont permis, de trouver ce stage qui était en totale adéquation avec mes attentes, et mon projet professionnel.

Je tiens à remercier en général toutes les personnes avec qui j'ai pu travailler lors de mon stage.

Glossaire

IoT, Internet of Things

DOSI, Direction Opérationnelle des Systèmes d'Information

CNRS, Centre Nationale de la Recherche Scientifique

INSERM, Institut National de la Santé et de la Recherche Médicale

IRD, Institut de la Recherche pour le Développement

CINAM, Centre Interdisciplinaire des Nanoscience de Marseille

TP, Travaux Pratiques

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

LAN, Local Area Network

Un réseau local, est un groupe d'ordinateurs et de périphériques associés qui partagent des liaisons de communication filaires ou sans fil.

WAN, Wide Area Network

Un réseau étendu, correspond à un LAN mais qui couvre une zone géographique très vaste comme la superficie d'un ou de plusieurs pays réunis, voire la planète toute entière.

Pare-feu ou FireWall, Un pare-feu est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il surveille et contrôle les applications et les flux de données (paquets).

DMZ, Demilitarized Zone

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

Paquets de Données,Le paquet est l'unité de données qui est acheminée entre une origine et une destination sur un réseau.

LAMP, Linux Apache MariaDb Php

LAMP est un acronyme désignant un ensemble de logiciels libres permettant de construire des serveurs de sites web.

HTTP, HyperText Transfer Protocol est un protocole de communication client-serveur développé pour le World Wide Web.

HTTPS, HyperText Transfer Protocol Secure est la version sécurisé de HTTP.

RTSP, Real Time Streaming Protocol

Le protocole de streaming temps-réel, est un protocole de communication de niveau applicatif destiné aux systèmes de streaming média.

SNMP, Simple Network Management Protocol

Le protocole simple de gestion de réseau est un 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.

SYSLOG, est un protocole définissant un service de journaux d'événements d'un système informatique. C'est aussi le nom du format qui permet ces échanges.

SSH, Secure SHell est à la fois un programme informatique et un protocole de communication sécurisé.

UDP, User Datagram Protocol, est un des principaux protocoles de télécommunication utilisés par Internet. Il fait partie de la couche transport du modèle OSI, comme TCP.

TCP, Transmission Control Protocol, est un protocole de transport fiable, à l'opposé d'UDP.

Data-Center, Un centre de traitement des données (data-center) est un lieu où sont installées les infrastructures centrales du système d'information : serveurs, baies de stockage, équipements réseau… Comme son nom l'indique, le data-center sert à héberger les applications qui gèrent les données et qui fournissent des services.

ZBF, Zone Base Firewall

Technique la plus moderne et la plus évoluée des Firewalls Stateful.

VLAN, Virtual Local Area Network

Un VLAN est un réseau local virtuel. Le concept de VLAN est utilisé afin d'avoir plusieurs réseaux indépendants sur le même équipement réseau physique.

SWITCH, Un commutateur réseau, est un équipement qui relie plusieurs segments, dans un réseau informatique et de télécommunication et qui permet de créer des circuits virtuels.

Routage statique, Avec le routage statique, les administrateurs vont configurer les routeurs un à un au sein du réseau afin d'y saisir les routes à emprunter pour aller sur tel ou tel réseau. Concrètement, un routeur sera un pont entre deux réseaux et le routeur d'après sera un autre pont entre deux autres réseaux

Routage dynamique, Le routage dynamique permet quant à lui de se mettre à jour de façon automatique, sans intervention manuelle de l'administrateur du réseau contrairement au routage statique.

S/STP, Super Shielded Twisted Pair, Le S/STP est type de câble, dans lequel chacune des paires du câble est blindée par un écran en aluminium, et en plus la gaine extérieure est blindée par une tresse en cuivre étamé.

Ingénieur Avant-Vente, Un ingénieur avant-vente est chargé de fournir une assistance technique aux ingénieurs commerciaux dans le but de les aider lors de la négociation de contrats.

CV, Curriculum vitæ

6 Bibliographie

L'ANSSI. *Définition d'une architecture de passerelle d'interconnexion sécurisée (https://www.ssi.gouv.fr/entreprise/guide/definition-dune-architecture-de-passerelle-dinterconnexion-securisee/)*

L'ANSSI. *Définition d'une politique de pare-feu (https://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-definition-dune-politique-de-filtrage-reseau-dun-pare-feu/)*