**Institut Universitaire de Technologie,**
**Aix-Marseille Université**

**RAPPORT DE STAGE**
**Diplôme Universitaire de Technologie**
**Spécialité Réseaux et Télécommunications**

# Conception et installation d'un réseau local

Mounir

BENLHAJ

Responsable entreprise : Didier Tonneau

Responsable académique : Roland DEPEYRE

**2019**

## Table des matières

# 1 Présentation de l'organisme d'accueil

**Université d'Aix-Marseille :**

L'Université d'Aix-Marseille (AMU), est une université française pluridisciplinaire créée le 1er janvier 2012 par la fusion des trois universités d'Aix-Marseille existant précédemment, l'université de Provence, l'université de la Méditerranée et l'université Paul-Cézanne.

Avec plus de 75 000 étudiants pour un budget de 720 millions d'euros, elle est l'une des plus grandes universités de France. Ses campus sont situés principalement dans les villes d'Aix-en-Provence et de Marseille, et son siège est localisé à Marseille, au Pharo.

Labellisée en 2012 par un jury international au titre de l'Initiative d'excellence (IDEX), Aix Marseille Université voit ce financement confirmé en 2016.

**Fondation universitaire A*MIDEX :**

L'initiative d'excellence d'Aix-Marseille a été créée en avril 2016, son objectif est de valoriser et développer le potentiel du site d'Aix-Marseille.

Cet organisme gère les fonds alloués au titre du projet A*MIDEX, soit près de 26 millions d'euros par an. Ils permettent de mettre en œuvre les projets de Laboratoires d'Excellence (« LABEX ») portés par l'université d'Aix-Marseille et sélectionnés dans le cadre des Investissements d'Avenir et financer des projets de recherche et d'enseignement supérieur (émergents, interdisciplinaires et innovants) de très haut niveau international dans un périmètre d'excellence évolutif, tout en participant à la promotion de l'académie.

# 2 Contexte du stage

## 2.1 Projet ECO

Le but du projet ECO (Education with connected Object) financé par l'Académie d'Excellence d'AMIDEX est de doter AMU d'une plateforme IOT* (Internet of Things) pour l'enseignement ouvert aux étudiants, considérés comme techniciens et ingénieurs, aux enseignants-chercheurs de AMU ou aux industriels, considérés comme 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 au Smart Grid et dans les bureaux du Département Génie Electrique du site de Saint Jérôme. 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 de L3 Informatique.

3. La troisième concerne l'installation et la configuration d'un serveur WEB dans la Data Center du Site de Saint Jérôme, pour stocker les données venant des capteurs des salles. Cette tâche est réalisée par un étudiant du M1 Réseaux et Télécommunications. La configuration sera la même que pour les salles de TPs du site de Luminy (voir rapport de M. Dany LAU).

## 2.2 Problématique

La mission principale de ce stage était de concevoir et d'installer une nouvelle architecture réseau pour le Département Génie Electrique du site de Saint-Jérôme, pour créer un LAN dédié aux travaux pratiques sur le Smart Grid.
Le Département comprend une grande salle de TP, un couloir principal séparant deux rangées de salles (bureaux d'un côté du couloir et salles de TPs de l'autre côté). La grande salle de TP mesure au total 343 m² (figure 3) et comprend une grande salle d'environ 300 m² et 2 salles de stockage d'environ 22 m² chacune. Cette salle principale de TP comporte plusieurs piliers au centre de la pièce, sur lesquels sont fixées des gaines amenant la puissance électrique aux postes de travail. L'autre partie consiste en 2 salles de projet de 63 m² chacune, 2 bureaux de 18 m², un bureau de 36 m² ainsi que la salle de Smart Grid qui fait également 36m².

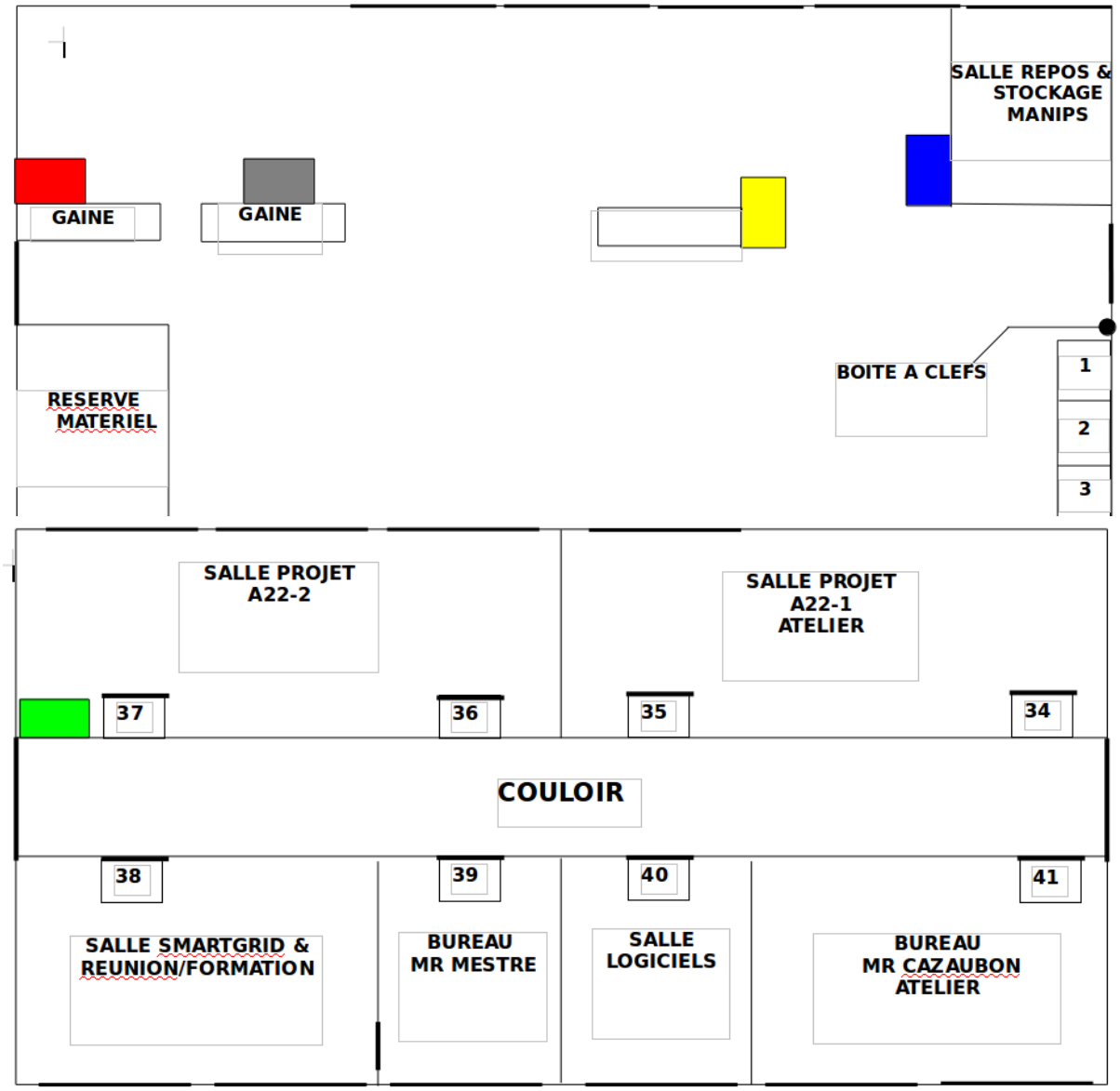



*Figure 0 : Plan du Master Génie et Electrique*

Dans ces salles, trois installations/modification majeures seront mises en places pour permettre des TP sur le Smart Grid:

- L'installation d'un système d'éclairage Intelligent et Interactif. Ce système remplacera le système actuel .Ce système aura un but pédagogique, en permettant aux étudiants d'interagir directement sur les luminaires en utilisant les données de capteurs et de différents protocoles.

- L'Installation de prises/ports RJ45 femelle (voir annexe) permettant le branchement de capteurs, sur le réseau dédié à l'intelligence du système

- Un système de caméras de surveillance, qui sera installé pour des projets futurs, en relation avec les projets IoT développés sur le site de Luminy.

Les deux salles n'étant pas neuves, elles possèdent déjà une installation réseaux numérique et Électrique dont il faut tenir compte. Pour des raisons pratiques l'installation des ports RJ45, sera superposée à l'installation déjà existante/présente.

# 3 Présentation du travail réalisé

## 3.1 Installation d'un réseau local sur le site de Saint-Jérôme

### 1 Choix et présentation du matériel :

La première étape à réaliser était de choisir le matériel répondant aux exigences. Il a fallu faire un travail de recherche et échanger avec les professionnels de la vente pour trouver le bon modèle, puis rédiger une proposition d'offre (voir annexe) détaillant mes choix.

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 en récupérant les données des luminaires grâce à la GTB (Gestion du batiment).
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
- Les étudiants pourront avoir un contrôle sur les luminaires. Ils pourront ainsi 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*.



*Figure 1: Luminaire Philips lighting*

Ils existent 2 technologies pour faire fonctionner ses luminaires qui sont le POE*, ZigBee*. Le Master Génie et Electrique souhaitent combiner les deux solutions pour pouvoir offrir un large panel de connaissance a ses étudiants.

Switch* Cisco ws-c2960-48pst-l:

*Figure 2: Switch Cisco ws-c2960-48pst-l*

Ces switchs permettent l'utilisation de la PoE (Power of Ethernet)*. Ces switchs permettent d'alimenter des appareils en réseau avec via le câble Ethernet utilisé. Pour cela une paire torsadée est utilisée pour l'alimentation.

Caméra  Caméra D-Link DCS-4602EV


*Figure 3 : Caméra D-Link DCS-4602EV*

Il m'a été demandé de ne prévoir que l'achat des caméras, l'installation devant être réalisée par des étudiants de master, dans un but pédagogique. Les caméras devaient répondre à plusieurs critères:

-  - Elles devaient être IP
-  - Supporter la technologie PoE (Power over Ethernet)
-  - Avoir un prix raisonnable

J'ai opté pour une caméra de la marque D-Link répondant à tous les critères :
J'ai choisis d'acheter 14 caméras pour couvrir les 360m² du Département Génie Electrique sur le site de Saint-Jérôme.

Câbles et goulotte :

Le choix du câble est très important dans une architecture réseaux. Le câblage est normalement une opération coûteuse et doit donc être pensé sur le long terme. Dans notre cas les câbles de courant faible et courant fort seront brassés ensemble, il est donc impératif de choisir des câbles blindés pour éviter les perturbations engendrées par le réseau d'alimentation électrique. J'ai donc choisis des câbles catégorie 6 de type S/STP* parmi les 5 types existant (voire proposition d'offre dans l'annexe). Nous avons acheté 300 m de câbles pour les deux sites.

Ensuite j'ai dû déterminer le métrage de goulotte ainsi que le nombre de ports réseaux, en accord avec l'Equipe Pédagogique. J'ai pris 40 mètres de goulotte ainsi que 40 ports RJ45 pour le site de Saint-Jérôme.

## 2 Conception et configuration du réseau

Introduction au réseau local et au VLAN :

Le LAN (Local Area Network ou en français réseau local), est un réseau informatique local qui relie au sein d'un organisme un ensemble de matériels informatiques. Le plus souvent par une connexion Ethernet.


*Figure 4 : Exemple de LAN*

Un VLAN (Virtual Local Area Network) est un réseau virtuel qui permet de découper au niveau logique un réseau en plusieurs sous-réseau.
Sans VLAN un switch* considère toutes ses interfaces comme faisant partie du même réseau :

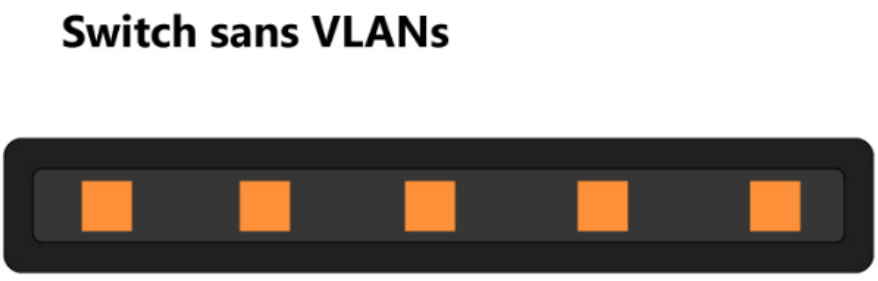



*Figure 5 : Switch sans VLANs*

Dans ce cas les risques majeurs sont :

- Si un appareil du réseau est compromis par un attaquant, il lui sera très facile d'avoir accès aux autres équipements du réseau.

- Plus il y aura d'appareils connectés sur un réseau, plus le domaine de diffusion* sera grand et donc les appareils connectés lents à répondre.

- Ce problème concerne aussi le domaine de collision*. Plus le nombre d'appareils est grand, plus les chances de collisions (donc pertes de données) entre les paquets de données sont grandes.

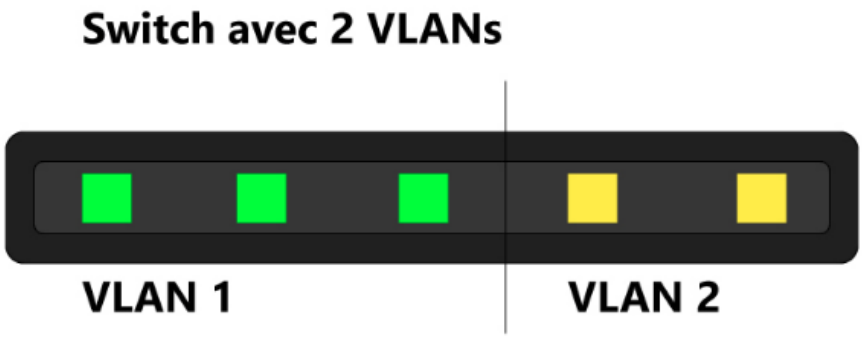



*Figure 6 : Switch avec deux VLANS*

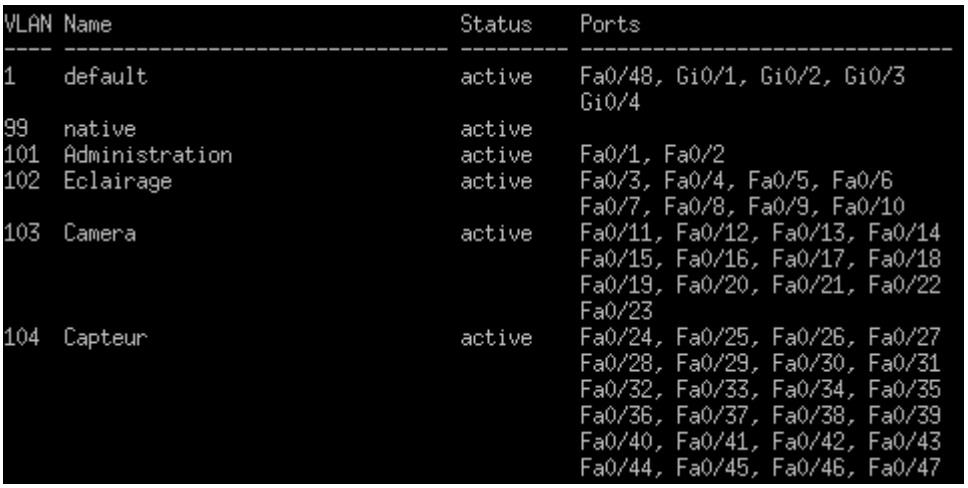
Le découpage du réseau en plusieurs sous-réseaux, ou VLANs, permet d'isoler au niveau logique les appareils qui ne sont pas du même réseau. Ainsi si un appareil du VLAN 1 est compromis par un attaquant, le pirate aura plus de difficultés à attaquer un appareil du VLAN 2.

Les VLANs permettent de réduire le problème d'un trop grand domaine de diffusion ou de collisions. En découpant le réseau en plusieurs sous-réseaux, ils réduisent ainsi dans le même temps les domaines de collisions 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 3 classe de 20 élèves. Il est donc plus simple de gérer trois VLANs avec 20 appareils, que 60 appareils dans le même réseau.

Pour nous le LAN sera composé d'un système de luminaires connectés, de capteurs, de caméras, et d'un PC permettant la supervision du réseau. Une adresse IP nous sera communiquée ultérieurement par la DOSI* pour notre LAN. Cependant, dans le but d'effectuer les tests, j'ai utilisé des adresses réseaux quelconques.

Nous allons découper notre réseau en 4 VLANs :

- Un VLAN pour l'administration
- Un VLAN pour le système d'éclairage intelligent.
- Un VLAN pour le système de caméras surveillance.
- Un VLAN pour les capteurs.



| VLAN | Name | Status | Ports |
|---|---|---|---|
| 1 | default | active | Fa0/48, Gi0/1, Gi0/2, Gi0/3<br>Gi0/4 |
| 99 | native | active | |
| 101 | Administration | active | Fa0/1, Fa0/2 |
| 102 | Eclairage | active | Fa0/3, Fa0/4, Fa0/5, Fa0/6<br>Fa0/7, Fa0/8, Fa0/9, Fa0/10 |
| 103 | Camera | active | Fa0/11, Fa0/12, Fa0/13, Fa0/14<br>Fa0/15, Fa0/16, Fa0/17, Fa0/18<br>Fa0/19, Fa0/20, Fa0/21, Fa0/22<br>Fa0/23 |
| 104 | Capteur | active | Fa0/24, Fa0/25, Fa0/26, Fa0/27<br>Fa0/28, Fa0/29, Fa0/30, Fa0/31<br>Fa0/32, Fa0/33, Fa0/34, Fa0/35<br>Fa0/36, Fa0/37, Fa0/38, Fa0/39<br>Fa0/40, Fa0/41, Fa0/42, Fa0/43<br>Fa0/44, Fa0/45, Fa0/46, Fa0/47 |

*Figure 7 : Configuration des Vlans*

J'ai affecté les deux premières interfaces au Vlan d'administration puis six interfaces pour les luminaires POE ainsi que les passerelles d'interconnexion pour les luminaires

Introduction au 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. Il permet un meilleur contrôle du trafic qui transite entre les réseaux et donc une sécurité renforcée ainsi qu'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 termes de terminaux.

| | 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 8 : Différence entre routage statique et Dynamique*

Configuration de VTP :

Le protocole VTP (Vlan Trunk Protocol) permet de réduire la gestion dans un réseau commuté. Quand vous configurez un nouveau VLAN sur un serveur VTP, le VLAN est distribué par tous les commutateurs dans le domaine. Ceci réduit la nécessité de configurer le même VLAN partout.

Dans mon cas l'utilisation de VTP permet de redistribuer les VLANs de notre switch principal vers le switch de distribution.

Configuration du serveur :

```
Sw1-Lan-MasterGE(config)#vtp version 2
Sw1-Lan-MasterGE(config)#vtp domain MasterGE
Changing VTP domain name from cisco to MasterGE
Sw1-Lan-MasterGE(config)#
*Mar  1 05:04:04.617: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to MasterGE.
Sw1-Lan-MasterGE(config)#vtp password MasterGE
Setting device VTP password to MasterGE
Sw1-Lan-MasterGE(config)#vtp mode server
Setting device to VTP Server mode for VLANS.
```

*Figure 9 : Configuration VTP du serveur*

Configuration du client :

```
Sw2-Lan-MasterGE(config)#vtp version 2
Sw2-Lan-MasterGE(config)#vtp domain MasterGE
Changing VTP domain name from cisco to MasterGE
Sw2-Lan-MasterGE(config)#
*Mar  1 04:30:12.402: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to MasterGE.
Sw2-Lan-MasterGE(config)#vtp password MasterGE
Setting device VTP password to MasterGE
Sw2-Lan-MasterGE(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
```

*Figure 10 : Configuration VTP du client*

<u>Configuration du routage Inter-Vlan :</u>

Les switch que nous utilisons sont de niveau 2 et ne permettent pas de faire routage. Pour remédier à ce problème, il existe 2 solutions : utiliser un switch de niveau 3* ou utiliser un routeur et la technologie router-on-a-stick.

J'ai d'abord simulé notre réseau LAN sur packettracer* puis configuré notre switch dans le cas où ce réseau serait connecté à un routeur de la DOSI.

La configuration router-on-a-stick consiste à diviser une interface réseau (connectée directement au switch) en sous-interfaces qui serviront de passerelles par défaut aux équipements de chaque Vlan.

Configuration du routeur :

```
interface GigabitEthernet0/0.10
 encapsulation dot1Q 101
 ip address 10.101.101.2 255.255.255.0
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 102
 ip address 10.102.102.2 255.255.255.0
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 103
 ip address 10.103.103.2 255.255.255.0
!
interface GigabitEthernet0/0.40
 encapsulation dot1Q 104
 ip address 10.104.104.2 255.255.255.0
```

*Figure 11 : Configuration des sous-interfaces réseau*

Ici j'ai divisé l'interface g0/0 en 4 sous-interfaces, chaque interface étant associée à une adresse réseau du Vlan dont elle va s'occuper.

Configuration du switch :

```
interface GigabitEthernet0/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 99,101-104
 switchport mode trunk
```

*Figure 12 : Configuration du lien trunk entre le switch et le routeur*

Du côté du switch, j'ai placé l'interface G0/1 (connecté au routeur) en mode trunk* et autorisé le passage de nos VLANs.

## Installation du matériel :

L'installation du matériel aura lieu durant le mois de juillet lorsque tous les équipements seront livrés. Elle commencera par la mise en place des goulottes et des prises RJ45 qui seront installées en parallèle du réseau existant. Une fois cela terminé, je mettrai en place les switchs configurés et puis nous tirerons les câbles pour relier tous les appareils aux switchs.

## 3.2 Conception et Installation d'une configuration double pare-feu ZBF

Il faut mettre en place une passerelle d'interconnexion sécurisée dans le but de protéger le serveur à la fois du LAN et du WAN.

### Introduction aux passerelles d'interconnexion sécurisée :

Aujourd'hui quelle que soit l'entreprise et son domaine d'activité, l'entreprise aura besoin d'avoir un accès à Internet (WAN) et donc d'une passerelle d'interconnexion entre son LAN et le WAN. Malheureusement, quand on se connecte à un réseau dont on n'a pas le contrôle, une simple passerelle d'interconnexion ne permet pas de se protéger des différentes menaces et attaques provenant de l'extérieur. Or avec l'apparition et l'expansion d'internet, de nouvelles menaces ont vu le jour.

Les principales menaces qui pourraient impacter, une entreprise sont les suivantes :

- La fuite de données sensibles pour l'entreprise, sur internet ;
- Les dénis de services, qui empêcheraient l'accès à internet depuis l'entreprise, et inversement ;
- Modification du serveur web sans autorisation par l'entreprise. Un attaquant peut en effet chercher à modifier le contenu du serveur web à des fins de désinformation, d'atteinte à l'image de marque de l'entreprise ou de revendication ;

Pour lutter contre ces menaces, il faut mettre en place une passerelle d'interconnexion dites sécurisée. 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 pas un point majeur de la politique de sécurité. Le point le plus important, est que dans aucun cas les utilisateurs venant du WAN ne puissent accéder au LAN 'capteurs' et à ses données. Pour avoir une sécurité conforme aux préconisations de l'ANSSI, nous avons décidé d'adopter une architecture passerelle d'interconnexion basée sur deux pare-feu* de marques différentes et d'une DMZ*. Le système se compose :

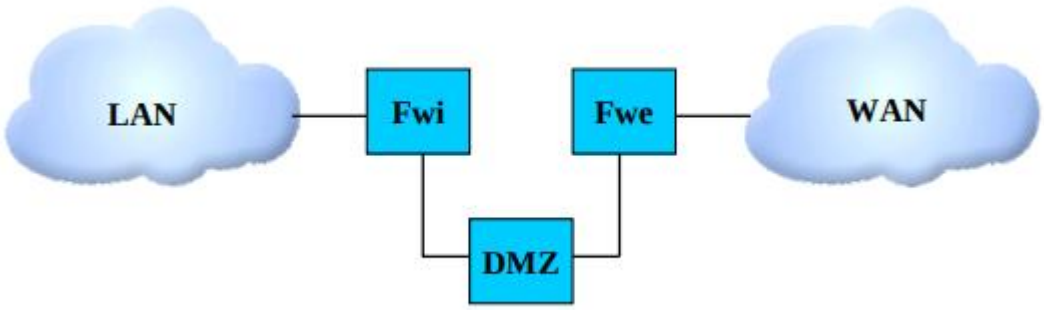



*Figure 13 : Architecture basée sur deux pare-feux avec coupure physique.*

- D'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 interne (FWi) entre le LAN et la DMZ. De 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.

<u>La Politique de sécurité :</u>

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/HTTPS/RTSP* provenant des caméras à destination du serveur Web.

- Autoriser les paquets SNMP*/SYSLOG*/HTTP/HTTPS/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.

J'ai utilisé packetracer pour pouvoir tester notre politique de sécurité :

```
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 14 : Configuration ZBF du pare-feu interne*

```
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 15 : Configuration ZBF du pare-feu externe*

## 3.3 Mission annexe

Une mission annexe que j'ai effectué lors de mon stage et qui a duré une journée, était le référencement des câbles réseaux du bâtiment de Grand Luminy . 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 16 : 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.

# 4 Conclusion

Ce stage était très enrichissant sur plusieurs plans.
D'abord la conception complète d'un réseau local était un projet ambitieux qui m'a permis de revoir et consolider une grosse partie de mes connaissances.

La configuration de la passerelle d'interconnexion ainsi que les guides de l'ANSSI m'ont permis d'acquérir des compétences et une compréhension beaucoup plus globale de la sécurité réseau.

Sur le plan humain, ce stage m'a permis d'améliorer mon travail d'équipe car nous étions 4 stagiaires sur le projet ECO avec des taches et des compétences différentes, et c'était intéressant de pouvoir échanger ensemble pour pouvoir se compléter les uns les autres.
Pour ce stage j'ai aussi dû échanger avec des professionnels pour l'achat du matériel et cela m'aura permis d'améliorer mon relationnel.

Sur le plan professionnel, ce stage s'inscrit complément dans mon projet professionnel, il m'a permis de découvrir à quoi ressembler la conception d'un réseau informatique en partant de rien. Les missions que j'ai accomplis comme la configuration des pares-feux sont un atout considérable dans la recherche d'une future expérience professionnel.

Le projet ECO n'est pas terminé, il reste un moi pour finaliser la configuration ainsi que l'installation des équipements. Actuellement le réseau à était complétement simulé sur packet tracer, il reste donc à configurer les switchs pour Saint-Jérôme et les pares-feux pour Luminy.

## 5 Remerciements

Tout d'abord, j'adresse tous mes remerciements à **M. Nguyen** et **M. Depeyre** qui m'ont recommandé et accompagné pour ce stage. Je les remercie aussi pour leurs conseils ainsi que pour le le temps qu'ils ont accepté de me consacrer.

Je tiens à remercier toute l'équipe du CINaM pour leur accueil et tout particulièrement mon maître de stage, **Didier Tonneau** pour son accueil, le temps passé ainsi que la confiance qu'il m'a accordée, pour le stage intéressant ainsi que pour l'expérience acquise au cours de ce travail.

Je remercie aussi **M. Pascal Mestre** et **Julien Cazaubon** pour leur accueil enthousiaste sur le campus de Saint-Jérôme.

Je remercie aussi toutes les personnes avec qui j'ai pu travailler durant ses deux mois.

# 6 Glossaire

**Switch,** Un switch ou commutateur réseau en français, est un équipement qui fonctionne comme un pont multiports et qui permet de relier plusieurs segments d'un réseau informatique entre eux.

**POE,** Le PoE permet d'alimenter des appareils en réseau avec des câbles **Ethernet** via la connexion de données existante.

**Zigbee,** ZigBee est un protocole de haut niveau permettant la communication d'équipements personnels ou domestiques équipés de petits émetteurs radios à faible consommation

**Câble S/STP,** Chacune des paires est blindée par un écran en aluminium, et en plus la gaine extérieure est blindée par une tresse en cuivre étamé. Protection optimale, pour les zones à très hautes perturbations.

**Domaine de diffusion,** Un domaine de diffusion est une aire logique d'un réseau informatique où n'importe quel ordinateur connecté au réseau peut directement transmettre à tous les autres ordinateurs du même domaine, sans devoir passer par un routeur.

**Domaine de collision,** Un domaine de collision est une zone logique d'un réseau informatique où les paquets de données peuvent entrer en collision entre eux, en particulier avec le protocole de communication Ethernet.

**Packet Tracer,** Packet Tracer est un logiciel simulation de matériel réseau Cisco.

**Port Trunk,** Un port trunk est une liaison ayant pour but de véhiculer le trafic de plusieurs vlans.

**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 tout 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.

# 7 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/)*