RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

MediaSchool

IRIS

BTS SIO - ETUDE DE CAS
CAS EXPERTY

le 14 février 2025

Amir Tajik
Soulaiman RAYANE
Yann-isaac KOUZETOUKA
Jeremie-cephas SEGBEAME
Ferdinand NKONE

SOMMAIRE

Table des matières

1. Contexte et objectifs

1.1 Contexte

L'entreprise **EXPERTY** est un cabinet d'expertise comptable fondé en **2012** par M. Bernard SIMON. Depuis sa création, l'entreprise a connu une forte croissance, renforçant ainsi sa position sur le marché. Aujourd'hui, elle compte **80** employés répartis en 13 secteurs comptables ainsi que dans divers services généraux. Cette expansion a entraîné une augmentation des besoins en ressources et en infrastructures, nécessitant une adaptation constante pour garantir un environnement de travail optimal.

Dans cette dynamique de développement, la direction a pris la décision stratégique de construire un nouveau bâtiment situé dans la banlieue ouest de Strasbourg. Ce nouvel espace vise à accompagner la croissance de l'entreprise en offrant des locaux modernes et adaptés aux exigences des activités comptables. Cependant, ce bâtiment est actuellement vide et ne dispose d'aucune infrastructure informatique ni de câblage réseau.

Afin d'assurer le bon fonctionnement des services et de répondre aux exigences de performance et de sécurité, nous allons concevoir et déployer un réseau informatique robuste. Ce réseau devra être capable de supporter la charge de travail des employés, d'assurer une connectivité fluide entre les différents services et de garantir la sécurité des données sensibles traitées par le cabinet. Ce projet constitue donc une étape clé dans l'évolution d'EXPERTY et vise à doter l'entreprise d'une infrastructure fiable et évolutive pour accompagner sa croissance future.

1.2 Objectifs

Le projet a pour objectifs principaux :

- **Renouveler tout le parc informatique** : Les équipements réseaux et les postes clients doivent être entièrement remplacés.
- **Permettre le télétravail** : Tous les collaborateurs doivent pouvoir travailler à distance, ce qui nécessite des PC portables et une connectivité sans fil performante.
- **Installer les derniers logiciels** : Tous les postes clients doivent être équipés de **Windows 11** et de la suite bureautique **Microsoft Office 365**.
- **Mettre en place un câblage structuré** : Installation de prises **RJ45** et de **fibre optique** dans tout le bâtiment.
- **Sécuriser le réseau** : Mise en place de **VLAN**, de caméras de surveillance, d'un lecteur de badge, et d'une climatisation pour la salle serveur.
- **Déployer un réseau Wi-Fi** : Installation de bornes Wi-Fi pour une couverture totale du bâtiment.

2. Analyse des besoins et contraintes

2.1 Besoins

Afin d'assurer un environnement de travail optimal et conforme aux standards actuels, plusieurs aspects doivent être pris en compte. Il s'agit notamment de l'installation du câblage et des équipements réseau, de la mise en place d'une solution adaptée au télétravail, du déploiement de logiciels essentiels, de la sécurisation des infrastructures et de l'optimisation de la connectivité Wi-Fi. Chacun de ces points sera développé en détail afin d'assurer une mise en œuvre efficace et adaptée aux exigences d'EXPERTY :

- **Câblage** : Le câblage est un élément fondamental pour garantir la connectivité des équipements informatiques dans tout le bâtiment. Il est prévu d'installer des prises RJ45 dans chaque bureau et espace de travail afin d'assurer une connexion filaire stable et rapide. En complément, une infrastructure en fibre optique sera mise en place pour relier les différents étages et garantir une transmission optimale des données, notamment entre la salle serveur et les postes utilisateurs.
- **Équipements** : Afin d'assurer un fonctionnement optimal du réseau et des postes de travail, le projet prévoit le remplacement et l'installation de plusieurs équipements. Cela inclut des switchs performants pour gérer le trafic réseau, des routeurs adaptés aux besoins de l'entreprise, une baie de brassage bien organisée pour centraliser les connexions, ainsi que de nouveaux PC portables pour les employés. L'objectif est d'assurer une infrastructure fiable, évolutive et adaptée aux exigences de performance de l'entreprise.
- **Télétravail** : Avec l'essor du travail à distance, il est essentiel que les nouveaux PC portables soient configurés pour permettre le télétravail dans les meilleures conditions. Cela implique l'installation de solutions de connexion sécurisée, comme un VPN, ainsi que la mise en place d'outils collaboratifs permettant aux employés de travailler efficacement depuis n'importe quel endroit. Une attention particulière sera portée à la compatibilité des équipements avec les solutions cloud et les systèmes d'authentification sécurisée.
- **Logiciels** : Chaque poste de travail devra être équipé des logiciels nécessaires aux activités comptables et administratives de l'entreprise. Il est prévu d'installer **Windows 11** comme système d'exploitation, ainsi que la suite **Microsoft Office 365** pour la bureautique et la collaboration en ligne. Ces logiciels offriront aux employés un environnement de travail moderne, sécurisé et conforme aux standards actuels.
- **Sécurité** : La sécurité étant une priorité, plusieurs dispositifs seront mis en place afin de protéger les données et les infrastructures. Cela inclut la segmentation du réseau via des **VLAN** pour limiter les risques de cyberattaques, l'installation de caméras de surveillance pour surveiller les accès, et la mise en place d'un lecteur de badge pour restreindre l'entrée aux locaux sensibles. De plus, des mesures techniques telles que la climatisation de la salle serveur, une mise à la

terre efficace et l'installation d'un parafoudre permettront de garantir la pérennité des équipements.

- **Wi-Fi** : Un réseau Wi-Fi performant et sécurisé sera déployé dans tout le bâtiment afin de permettre une connectivité fluide pour les employés et les visiteurs. Ce réseau devra offrir une couverture homogène, avec un signal stable et une sécurité renforcée via l'utilisation de protocoles d'authentification avancés. Des bornes Wi-Fi adaptées seront installées stratégiquement pour assurer une connexion optimale, quel que soit l'endroit dans le bâtiment

2.2 Contraintes

Lors de la mise en place d'une infrastructure informatique pour un nouveau bâtiment, plusieurs contraintes doivent être prises en compte afin de garantir la réussite du projet. Ces contraintes concernent principalement le budget, le respect des délais et la définition précise du périmètre d'intervention.

Ce document détaille les principales contraintes du projet, en mettant en évidence les enjeux liés aux aspects financiers, aux délais imposés ainsi qu'aux éléments qui ne relèvent pas de la responsabilité de notre équipe :

- **Budget** : L'un des principaux défis de ce projet réside dans l'absence d'un budget préalablement défini. Cela signifie que la solution proposée doit être à la fois réaliste et économiquement viable, en tenant compte des besoins fonctionnels et techniques tout en optimisant les coûts. I

  Une approche stratégique consistera à comparer différentes solutions et fournisseurs, en privilégiant des équipements fiables et évolutifs sans pour autant dépasser des coûts raisonnables. De plus, une planification rigoureuse nous permettra d'anticiper les dépenses et d'éviter des surcoûts imprévus en cours de projet

- **Délai** : Le projet est soumis à une contrainte temporelle stricte : le site doit être pleinement opérationnel dans un délai de **7 mois** après son lancement. Ce délai inclut toutes les étapes nécessaires, depuis l'étude et la planification jusqu'à l'installation, la configuration et les tests finaux.

  Pour respecter cette échéance, nous allons suivre un calendrier précis et assurer une bonne coordination entre les différents intervenants. Chaque phase du projet sera clairement définie avec des objectifs intermédiaires permettant de mesurer l'avancement. Toute perturbation ou retard devra être anticipé et géré efficacement afin de ne pas compromettre la mise en service du site.

- **Éléments hors périmètre** : Certains aspects du projet ne relèvent pas de la responsabilité de notre équipe, car ils sont gérés par d'autres prestataires. Il s'agit notamment de :

La téléphonie IP : L'installation et la configuration du système de téléphonie sur IP seront assurées par un fournisseur externe. Cependant nous assurons que l'infrastructure réseau prévue sera bien compatible avec cette solution.

Les imprimantes : La mise en place et la gestion des imprimantes relèvent d'un autre prestataire, mais le réseau peut être configuré pour permettre leur intégration sans problème.

Le système d'alarme : La sécurité physique du bâtiment, notamment les alarmes anti-intrusion et les systèmes de détection, sera mise en place par un partenaire spécialisé.

La sécurité réseau : La gestion des pare-feu et des solutions antivirus est externalisée. Toutefois, nous allons prendre en compte la segmentation du réseau via des VLAN et la sécurisation des accès dans notre conception.

3. Découpage du produit final (PBS)

Afin de structurer et d'optimiser la gestion du projet, le produit final est découpé en plusieurs lots. Cette approche nous permet d'organiser les différentes composantes du projet de manière hiérarchique et logique, facilitant ainsi le suivi et la mise en œuvre des différentes étapes.

Il nous permet aussi une gestion efficace des différentes tâches et une meilleure répartition des responsabilités. Chaque lot correspond à une phase clé du déploiement et garantit que l'ensemble des besoins techniques et organisationnels sont couverts.

Voici la **Product Breakdown Structure (PBS)** sous forme de tableau pour une meilleure lisibilité:

Découpage du Produit Final (PBS - Product Breakdown Structure)

Catégorie	Sous-Catégorie	Détails
1. Réseau	**1.1 Câblage**	- Prises RJ45 - Fibre optique
	1.2 Équipements réseau	- Switchs - Routeurs - Baie de brassage
	1.3 Plan d'adressage IP	- Plan d'adressage global (CIDR) - VLAN
	1.4 Bornes Wi-Fi	- Ubiquiti UAP-AC-Pro - Switch PoE
2. Postes Clients	**2.1 PC portables**	- Achat et configuration

	2.2 Logiciels	- Windows 11 - Microsoft Office 365
3. Locaux Techniques	**3.1 Choix de la salle serveur**	- Caméras de surveillance - Lecteur de badge - Climatisation - Mise à la terre et parafoudre
	3.2 Baie de brassage	- Organisation et installation
4. Inventaire Réseau	**4.1 Nommage des prises**	- Identification et documentation
	4.2 Schéma de la baie	- Création d'un schéma détaillé
	4.3 Plan d'adressage IP	- Documentation complète

4. Plan d'adressage global avec CIDR et VLAN

4.1 Plan d'adressage IP

Le réseau principal utilise le plan d'adressage **CIDR** avec le réseau 192.168.1.0/24. Cela permet d'avoir **256 adresses IP disponibles**, dont **254 adresses utilisables** (de 192.168.1.1 à 192.168.1.254). Le masque de sous-réseau est 255.255.255.0 :

- **Adresse réseau** : 192.168.1.0
- **Adresse de broadcast** : 192.168.1.255
- **Masque de sous-réseau** : 255.255.255.0
- **Adresses utilisables** : 254

Cette structuration garantit une gestion efficace et une séparation logique des différents services grâce à l'utilisation de **VLAN**.

4.2 Répartition des adresses IP et VLAN

Afin de mieux gérer les différents services du réseau et d'optimiser la sécurité et la performance, nous avons décidé de segmenter le réseau en plusieurs **VLAN (Virtual Local Area Network)**. Chaque VLAN est dédié à un service spécifique ou à un groupe d'utilisateurs afin de mieux contrôler le flux de données, renforcer la sécurité et éviter toute congestion du réseau.

La segmentation permet également de limiter la portée des communications réseau à des groupes d'utilisateurs ou de services, ce qui réduit les risques de diffusion de virus ou d'attaques réseau entre les différents segments du réseau.

Service	VLAN	Plage d'adresses	Nombre d'adresses	Description
Réseau administratif	VLAN 10	192.168.1.1 - 192.168.1.50	50	Ce VLAN est dédié à l'infrastructure du réseau administratif, y compris les **routeurs**, **switchs**, et **serveurs**. Il est essentiel pour assurer une gestion centralisée et sécurisée des données et des communications du réseau.
Comptabilité	VLAN 20	192.168.1.51 - 192.168.1.100	50	Ce VLAN est réservé aux **postes clients des secteurs comptables**. Il prend en compte 13 secteurs comptables avec une moyenne de 5 postes par secteur, soit un total de **65 postes clients**. La segmentation permet de garantir une isolation des données financières et comptables.
Services généraux	VLAN 30	192.168.1.101 - 192.168.1.150	50	Ce VLAN regroupe les **postes clients des services généraux**, notamment ceux liés à l'accueil, à l'administration et à la direction. Cette segmentation permet d'assurer une gestion sécurisée des communications internes au sein de l'entreprise.

Caméras de surveillance	VLAN 40	192.168.1.151 - 192.168.1.160	10	Un VLAN spécifique est réservé aux **caméras de surveillance IP du salle des serveurs**.
Imprimantes	VLAN 50	192.168.1.161 - 192.168.1.170	10	Ce VLAN est dédié aux **imprimantes réseau**. Il permet une gestion centralisée et sécurisée des périphériques d'impression, avec un contrôle d'accès strict à ces équipements.
Équipements réseau	VLAN 60	192.168.1.171 - 192.168.1.180	10	Ce VLAN regroupe les **points d'accès Wi-Fi** et autres équipements réseau essentiels, comme les **serveurs** de fichiers ou de données spécifiques. La segmentation garantit une meilleure gestion du trafic réseau.
Wi-Fi (Bornes et clients)	VLAN 80	192.168.1.181 - 192.168.1.200	20	Ce VLAN est dédié aux **bornes Wi-Fi** et aux **clients sans fil**. Une gestion séparée des
				connexions sans fil permet de mieux gérer la bande passante et de garantir une sécurité renforcée pour les utilisateurs mobiles.
Lecteurs de badge RFID	VLAN 90	192.168.1.201 - 192.168.1.210	10	Ce VLAN est réservé aux **lecteurs de badge RFID** utilisés pour l'accès sécurisé au salle du serveur.

Réservé (Extensions futures)	VLAN 70	192.168.1.211 - 192.168.1.254	44	Ce VLAN est **réservé pour des extensions futures** du réseau, comme l'ajout de nouveaux services ou équipements. Les adresses peuvent être attribuées à de futurs **serveurs**, **postes clients**, ou autres équipements réseau.

5. Répartition des prises RJ45

La répartition des prises RJ45 est essentielle pour assurer une connectivité efficace et flexible dans l'ensemble du bâtiment. Chaque secteur, en fonction de son besoin en connectivité, dispose d'un nombre défini de prises pour les postes de travail, les équipements réseau, et les périphériques. La planification du câblage est organisée de manière à garantir une utilisation optimale de l'infrastructure tout en anticipant d'éventuelles extensions futures.

5.1 Rez-de-chaussée (RDC)

Service administratif

- Nombre de bureaux : 5 personnes.
- Prises RJ45 par bureau : 2.
- Total prises RJ45 : 5 bureaux × 2 prises = 10 prises RJ45.

Assistante de direction

- Nombre de bureaux : 2 personnes (assistante et apprentie).
- Prises RJ45 par bureau : 2.
- Total prises RJ45 : 2 bureaux × 2 prises = 4 prises RJ45.

Direction

- Nombre de bureaux : 1 personne (PDG).
- Prises RJ45 par bureau : 2.
- Total prises RJ45 : 1 bureau × 2 prises = 2 prises RJ45.

Salle serveur

- Prises RJ45 : 6 (pour les équipements réseau, serveurs, caméras, etc.).
- Total prises RJ45 : 6 prises RJ45. **Local informatique**

- Prises RJ45 : 4 (pour les techniciens informatiques et les équipements supplémentaires).
- Total prises RJ45 : 4 prises RJ45. **Service informatique**
- Nombre de bureaux : 5 personnes (responsable informatique, administrateur systèmes et réseaux, et 3 techniciens).
- Prises RJ45 par bureau : 2.
- Total prises RJ45 : 5 bureaux × 2 prises = 10 prises RJ45.

Secteurs A à G

- Nombre de bureaux : 7 secteurs × 5 personnes = 35 bureaux.
- Prises RJ45 par bureau : 2.
- Total prises RJ45 : 35 bureaux × 2 prises = 70 prises RJ45.

Local	**Nombre de prises RJ45**
Service administratif	10
Assistante de direction	4
Direction	2
Salle serveur	6
Local informatique	4
Service informatique	10
Secteurs A à G	70

5.2 Étage

Secteur H

- Nombre de bureaux : 5 personnes.
- Prises RJ45 par bureau : 2.
- Total prises RJ45 : 5 bureaux × 2 prises = 10 prises RJ45.

Cuisine

- Prises RJ45 : 2 (pour les équipements de cuisine connectés, si nécessaire).

- Total prises RJ45 : 2 prises RJ45.

2.3 Archives

- Prises RJ45 : 2 (pour les équipements de numérisation ou de gestion des archives).
- Total prises RJ45 : 2 prises RJ45.

2.4 Secteurs I à M

- Nombre de bureaux : 5 secteurs × 5 personnes = 25 bureaux.
- Prises RJ45 par bureau : 2.
- Total prises RJ45 : 25 bureaux × 2 prises = 50 prises RJ45.

Local	**Nombre de prises RJ45**
Secteur H	10
Cuisine	2
Archives	2
Secteurs I à M	50

5.3 Total général des prises RJ45

Étage	**Nombre de prises RJ45**
Rez-de-chaussée (RDC)	106
Étage	64
Total	**170 prises RJ45**

Justification de la répartition

1. **Bureaux individuels** :
    - **2 prises par bureau** : Une pour le PC et une pour le téléphone IP ou un équipement supplémentaire.
    - **Justification** : Cela permet une flexibilité pour les collaborateurs et évite d'avoir à ajouter des multiprises ou des extensions.
2. **Salle serveur** :

- **6 prises** : Pour les équipements réseau (switchs, routeurs), les serveurs, les caméras, et une prise de réserve.
- **Justification** : La salle serveur est le cœur du réseau, donc il est crucial de prévoir suffisamment de prises pour tous les équipements critiques.

3. **Local informatique** :
   - **4 prises** : Pour les techniciens informatiques et les équipements supplémentaires.
   - **Justification** : Les techniciens ont besoin de plusieurs prises pour leurs équipements de test et de maintenance.
4. **Cuisine et archives** :
   - **2 prises** : Pour les équipements connectés (ex : imprimante réseau dans les archives, équipements de cuisine connectés).
   - **Justification** : Ces espaces peuvent nécessiter des connexions réseau pour des équipements spécifiques.

6. Bornes Wi-Fi

6.1 Répartition des bornes Wi-Fi

Étage	**Nombre de bornes Wi-Fi**
Rez-de-chaussée (RDC)	9
Étage	6
Total	**15 bornes Wi-Fi**

6.2 Modèles recommandés

Le choix des bornes Wi-Fi dépend des besoins en termes de couverture, de capacité et de sécurité. Dans ce cas, nous avons choisi les bornes Ubiquiti UAP-AC-Pro en raison de leur fiabilité, de leur capacité à gérer un grand nombre de connexions simultanées, et de leurs fonctionnalités avancées en matière de sécurité et de gestion du réseau.

Modèle de borne Wi-Fi : **Ubiquiti UAP-AC-Pro** • **Technologie** : Wi-Fi 5 (802.11ac)

- **Bande de fréquence** : 2.4 GHz et 5 GHz
- **Capacité de connexion simultanée** : jusqu'à 200 utilisateurs par borne
- **Port PoE** : Permet d'alimenter la borne via le câble Ethernet, facilitant l'installation et réduisant le besoin de prises électriques supplémentaires.

- **Gestion centralisée** : Utilisation du contrôleur UniFi pour gérer les bornes à distance, permettant une configuration, une surveillance et une gestion en temps réel.
- **Ubiquiti UniFi UAP-AC-Pro** : 15 bornes à 150€ HT chacune.
- **Switch PoE** : 1 switch Ubiquiti UniFi Switch 24 ports à 400€ HT.

6.3 Budget pour les bornes Wi-Fi

Élément	Quantité	Prix unitaire (HT)	Total (HT)
Bornes Wi-Fi (Ubiquiti UAP-AC-Pro)	15	150€	2 250€
Switch PoE (Ubiquiti UniFi Switch 24 ports)	1	400€	400€
Total			**2 650€**

---

7. Salle de serveur sécurisée

7.1 Caméras de surveillance

Les caméras de surveillance ont pour objectif principal de surveiller l'accès à la salle serveur afin de prévenir toute intrusion non autorisée. La sécurisation de cet espace critique est essentielle pour garantir l'intégrité et la confidentialité des systèmes informatiques et des données sensibles qu'il héberge. En cas d'incident ou de tentative d'accès non autorisé, les enregistrements vidéo permettent d'identifier les individus concernés et d'analyser la situation en détail.

Pour assurer une couverture optimale, deux caméras ont été installées à des emplacements stratégiques. La première est positionnée à l'entrée de la salle serveur, capturant ainsi chaque accès et sortie. Cette surveillance dissuasive réduit les risques d'intrusion en imposant un contrôle permanent. La seconde caméra est installée à l'intérieur de la salle, permettant un suivi continu des activités qui s'y déroulent. Cette disposition garantit une visibilité complète des mouvements à l'intérieur et prévient tout acte de malveillance ou de manipulation non autorisée des équipements.

Le choix de caméras IP s'inscrit dans une logique d'efficacité et de modernité. Ces caméras offrent une transmission des images en haute résolution sur le réseau informatique, permettant une surveillance en temps réel ainsi qu'un enregistrement sécurisé des flux vidéo sur un serveur dédié. Cette architecture facilite également l'accès aux enregistrements pour une analyse ultérieure, sans risque de perte de données.

Afin d’assurer une gestion optimale et une isolation du trafic vidéo, les caméras sont intégrées dans un VLAN spécifique (VLAN 40), évitant ainsi toute interférence avec d’autres services du réseau. Elles sont configurées avec des adresses IP fixes (192.168.1.151 et 192.168.1.152), ce qui permet une administration centralisée et une maintenance simplifiée. Grâce à cette infrastructure, la surveillance de la salle serveur est renforcée, garantissant une sécurité accrue des installations et une meilleure réactivité en cas d’anomalie.

- **Nombre de caméras** : 2 caméras IP.
- **Adresses IP** : 192.168.1.151 et 192.168.1.152 (VLAN 40).

7.2 Lecteur de badge

Les lecteurs de badge RFID sont essentiels pour le contrôle d'accès dans le bâtiment, en particulier pour sécuriser l'accès aux zones sensibles, telles que la salle serveur. Ces lecteurs permettent de garantir que seules les personnes autorisées puissent entrer dans ces zones.

- Fonctionnement :
  Le lecteur de badge RFID fonctionne en lisant des informations contenues dans des badges électroniques ou cartes RFID. Lorsqu'un badge valide est présenté au lecteur, celui-ci envoie un signal au système de contrôle d'accès pour autoriser ou refuser l'entrée.
- Adresse IP :
  Le lecteur de badge est configuré sur le réseau local et se voit attribuer l'adresse IP 192.168.1.153 dans le VLAN 40(VLAN dédié aux caméras de surveillance et aux équipements de sécurité). Cela permet une gestion centralisée et une communication fluide avec le serveur de contrôle d'accès, tout en séparant le trafic de sécurité du reste du réseau pour plus de sécurité.
- Installation et placement :
  Les lecteurs de badge seront installés à l'entrée de la salle serveur et éventuellement dans d'autres zones sensibles, telles que les bureaux exécutifs ou les zones de stockage sécurisées. Il est crucial que ces lecteurs soient placés à des endroits stratégiques pour contrôler efficacement l'accès.
- Sécurisation des communications :
  Les communications entre le lecteur de badge et le serveur de contrôle d'accès seront sécurisées par des protocoles de cryptage, afin de prévenir toute tentative de piratage ou de manipulation des données d'identification.

7.3 Climatisation

La climatisation dans une salle serveur est une composante essentielle pour assurer le bon fonctionnement des équipements informatiques. En effet, une température trop élevée peut endommager les composants électroniques et affecter les performances des serveurs.

- Objectif principal :
  L'objectif de la climatisation est de maintenir une température stable et optimale (généralement entre 18°C et 25°C) pour les équipements sensibles dans la salle serveur. Cela garantit que les serveurs, équipements réseau et autres dispositifs électroniques ne surchauffent pas, prolongeant ainsi leur durée de vie et réduisant les risques de panne.

- Système de climatisation :
  Le système de climatisation sera conçu pour être évolutif et fiable. Il sera équipé de capteurs de température pour ajuster automatiquement le flux d'air en fonction des besoins, assurant une répartition homogène de la température dans la salle. Une ventilation adéquate sera aussi intégrée pour éviter l'accumulation de chaleur.

- Surveillance et alertes :
  Un système de surveillance à distance de la température sera mis en place pour détecter toute anomalie (augmentation excessive de la température). En cas de problème, une alerte automatique sera envoyée au responsable informatique ou à l'équipe de maintenance.

- Redondance et sécurité :
  Pour éviter les risques liés à une défaillance du système de climatisation, un système de redondance sera installé. Cela comprend l'ajout d'un deuxième système de climatisation qui prendra le relais en cas de panne du principal.
  Un plan de maintenance régulière garantira le bon fonctionnement des équipements.

7.4 Mise à la terre et parafoudre

La mise à la terre et le parafoudre sont des dispositifs essentiels pour la protection des équipements électriques et électroniques contre les surtensions et les décharges électriques, souvent causées par des orages ou des pannes d'alimentation.

- Objectif principal :
  L'objectif de la mise à la terre et du parafoudre est de protéger tous les équipements informatiques (serveurs, commutateurs, routeurs, points d'accès Wi-Fi, etc.) contre les risques de surtensions et d'éclairs, qui peuvent endommager irrémédiablement les équipements électroniques et causer des pannes réseau majeures.

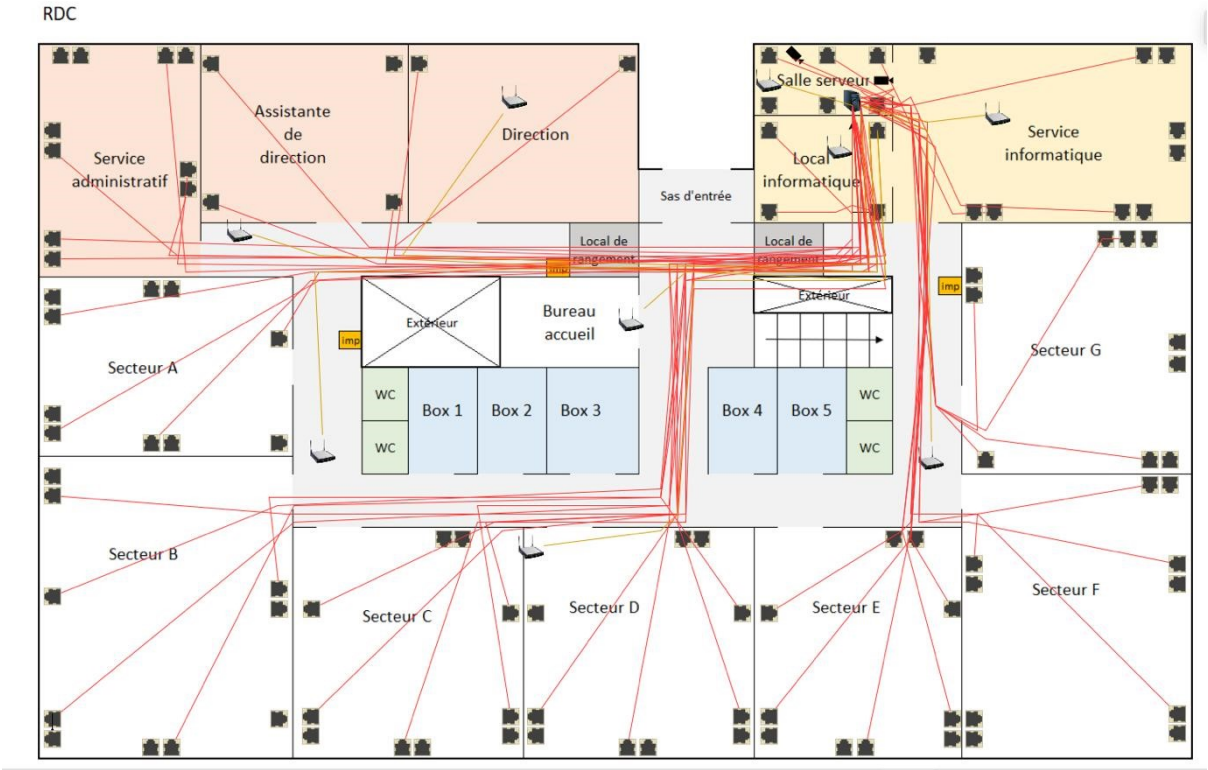
- Mise à la terre :
  La mise à la terre consiste à connecter les équipements à un système de dispositif de mise à la terre qui permet de dissiper toute charge électrique excédentaire (issue d'une surtension ou d'un choc électrique) vers le sol.
  Cela protège non seulement les équipements, mais aussi les utilisateurs contre les risques électriques.

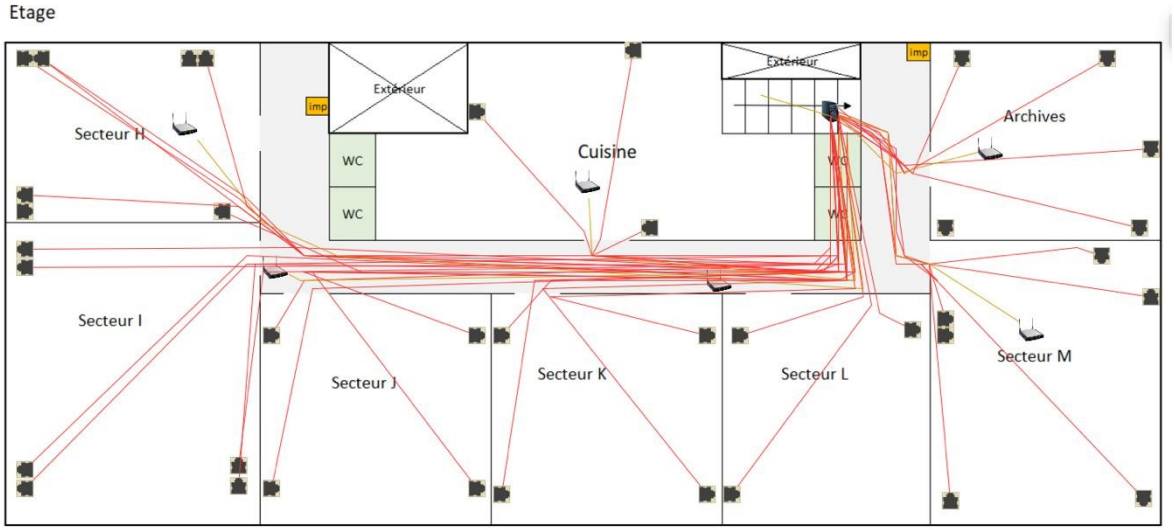
    - Installation :

Un réseau de conducteurs de mise à la terre sera installé, reliant les équipements critiques (serveurs, baies de brassage, équipements réseau) à une prise de terre sécurisée.

- Parafoudre :
  Le parafoudre est un dispositif installé pour intercepter les surtensions liées à des événements externes, comme la foudre, avant qu'elles n'atteignent les équipements sensibles. Cela permet de protéger les composants électroniques des dégâts causés par de tels événements.
    - Installation :
      Des parafoudres seront installés sur les circuits d'alimentation électrique de la salle serveur et des équipements réseau. Ces dispositifs agissent comme des fusibles en cas de surtension, détournant l'excès d'énergie vers la terre.
- Maintenance et vérification :
  Des tests réguliers seront effectués sur le système de mise à la terre et les parafoudres pour s'assurer de leur bon fonctionnement. Cela inclut la vérification de la résistance à la terre et la vérification du bon état des dispositifs de protection contre les surtensions.

7.5 SCHEMA DU BÂTIMENT





8. Budget global

Élément	**Quantité**	**Prix unitaire (HT)**	**Total (HT)**
Câblage RJ45	170 prises	150€	25 500€
Switch 24 ports	3	300€	900€
Routeur	1	400€	400€
PC portables	80	800€	64 000€
Caméras IP	2	200€	400€
Lecteur de badge RFID	1	300€	300€
Climatisation	1	1 500€	1 500€
Parafoudre	1	500€	500€
Mise à la terre	1	1 000€	1 000€
Bornes Wi-Fi (Ubiquiti UAP-AC-Pro)	15	150€	2 250€
Switch PoE (Ubiquiti UniFi Switch 24 ports)	1	400€	400€
Total			**97 150€**

9. Planning

Le planning du projet EXPERTY est structuré de manière à garantir une exécution fluide et respectueuse des délais impartis. Chaque mois, des tâches spécifiques sont assignées pour mener à bien la mise en place de l'infrastructure réseau et de sécurité,

en tenant compte des différentes phases nécessaires à la réussite du projet. Voici le détail des différentes étapes du planning

Diagramme de Gantt pour le projet EXPERTY

Tâches	Mois 1	Mois 2	Mois 3	Mois 4	Mois 5	Mois 6	Mois 7	Mois 8
Analyse des besoins, choix des solutions, découpage du projet (PBS)								
Planification du câblage, commande des équipements réseau								

Détails supplémentaires sur chaque étape :

Mois 1 - Analyse des besoins et choix des solutions : Cette phase initiale est cruciale pour définir avec précision les besoins de l'entreprise en termes de connectivité, de sécurité et d'évolutivité. Cela comprend des réunions avec les équipes de l'entreprise pour recueillir leurs exigences et prévoir une architecture réseau adaptée.

Mois 2 - Planification du câblage et commande des équipements : Après avoir déterminé les besoins et solutions à mettre en place, un plan de câblage détaillé est élaboré, spécifiant l'emplacement des prises RJ45 et des points de raccordement fibre. Les équipements sont ensuite commandés auprès des fournisseurs.

Mois 3-4 - Installation du câblage réseau : Cette phase voit l'exécution physique du câblage réseau dans le bâtiment. Les prises RJ45 seront installées dans chaque bureau et zone critique, tandis que la fibre optique sera posée pour relier les différents secteurs du bâtiment.

Mois 5 - Installation des équipements réseau : Une fois le câblage en place, les switchs, routeurs et autres équipements de réseau seront installés et configurés pour garantir une communication fluide entre les différents services. Cette étape inclut également la mise en place de la baie de brassage.

Mois 6 - Installation des postes clients : Les postes clients (PC portables) seront configurés avec **Windows 11** et les logiciels nécessaires pour l'entreprise, y compris **Microsoft Office 365**. Cette phase inclut également la mise en place du système de gestion à distance pour assurer le suivi des équipements.

Mois 7 - Installation des équipements de sécurité et confort : Les équipements critiques de sécurité, tels que les caméras de surveillance, les lecteurs de badge RFID, ainsi que la climatisation, seront installés dans la salle serveur et les zones sensibles. De plus, la mise en place de la mise à la terre et des parafoudres assurera la protection contre les risques électriques.

Mois 8 - Tests, recette et mise en service : Enfin, la phase de tests assurera que tout le réseau fonctionne de manière optimale. Cela comprend la validation de la couverture Wi-Fi, la vérification de l'accès sécurisé à la salle serveur via le lecteur de badge, et la mesure des performances des équipements réseau. Une fois les tests passés avec succès, le réseau sera mis en service pour une utilisation quotidienne.

Conclusion

Ce document présente de manière détaillée tous les éléments essentiels au bon déploiement du projet pour l'entreprise **EXPERTY**, visant à créer une infrastructure réseau performante et sécurisée pour leur nouveau bâtiment. En combinant une planification précise, des choix techniques adaptés et des solutions de sécurité robustes, ce projet constitue la base solide pour un environnement de travail moderne et fiable.

L'un des points centraux du projet est le **plan d'adressage CIDR et la gestion des VLAN**. Grâce à l'adoption du plan d'adressage 192.168.1.0/24, l'entreprise bénéficie d'une structure de réseau simple, évolutive et bien organisée, avec une séparation claire des différents services via les VLAN. Ce découpage offre une meilleure gestion du trafic et assure la sécurité des données en isolant les différents services. Les VLAN dédiés, tels que celui des caméras de surveillance et des équipements de sécurité, permettent de renforcer encore cette approche en séparant les réseaux de gestion sensibles du reste de l'infrastructure.

La **répartition des prises RJ45 et des bornes Wi-Fi** garantit une couverture réseau optimale dans tout le bâtiment. L'installation des prises RJ45 dans chaque pièce clé et l'ajout de bornes Wi-Fi sécurisées permettent à chaque utilisateur de bénéficier d'une connexion fiable et rapide, que ce soit pour un travail de bureau classique ou pour des

usages plus exigeants comme la visioconférence ou l'accès à distance. Le choix d'**Ubiquiti UAP-AC-Pro** pour les bornes Wi-Fi assure une performance élevée et une gestion centralisée, essentielle dans un environnement d'entreprise en croissance.

La sécurité du bâtiment est une priorité essentielle. Le **système de surveillance** dans la salle serveur, incluant les **caméras de surveillance**, le **lecteur de badge RFID**, et la **climatisation**, permet non seulement de surveiller et de contrôler l'accès aux zones sensibles mais aussi de garantir que les équipements serveurs restent dans un environnement optimal. De plus, la mise en place de **systèmes de mise à la terre et parafoudre** offre une protection indispensable contre les risques électriques, assurant ainsi une sécurité maximale pour les équipements critiques du réseau. Chaque mesure mise en place contribue à la stabilité et à la sécurité de l'infrastructure.

Pour assurer la viabilité financière du projet, un **budget détaillé** a été élaboré. Celui-ci tient compte de toutes les dépenses nécessaires, du câblage au matériel réseau, en passant par l'équipement de sécurité et les logiciels. Ce budget prend en considération les besoins de l'entreprise à court et moyen terme, en s'assurant qu'il reste raisonnable et réaliste par rapport aux objectifs du projet. En parallèle, un **planning réaliste** a été mis en place, définissant les étapes clés du projet et les délais associés pour s'assurer que l'ensemble du réseau soit opérationnel dans les **7 mois** suivant le lancement.

Ce projet est conçu pour répondre aux besoins immédiats de l'entreprise EXPERTY tout en anticipant ses futures extensions. La mise en œuvre des solutions proposées permet à l'entreprise d'acquérir une infrastructure réseau fiable, moderne et sécurisée, capable de soutenir ses objectifs de croissance. Chaque élément du projet, de la gestion des adresses IP à la sécurité physique, est interconnecté pour offrir une solution cohérente et efficace.

En somme, ce projet représente une étape majeure dans l'évolution technologique d'EXPERTY. Il permettra à l'entreprise non seulement de sécuriser son environnement de travail mais aussi de poser les bases solides pour son développement futur. Grâce à une planification soignée et des choix techniques rigoureux, l'entreprise sera prête à relever les défis liés à la gestion de son réseau tout en assurant la sécurité, l'efficacité et la performance des services informatiques