BTS SIO – ETUDE DE CAS

Centre de formation	Formation	Module
IRIS Strasbourg	BTS SIO Année 1	Bloc 1 Option SISR

EXPERTY

Rédacteurs	Date	Nb de pages
Enzo ROESCH	14/02/2025	25
Tsiaroniaina RAMANANTSIALONINA		
Thomas KLEIN-DOMINIONE		

TABLE DES MATIÈRES

Glossaire

- RJ45 : Type de prise et de connecteur utilisé pour les câbles réseau Ethernet, permettant des connexions filaires.
- Fibre optique : Câble utilisant des fibres de verre ou de plastique pour transmettre des données à haute vitesse via des signaux lumineux.
- Baies de brassage : Armoires ou racks centralisant les connexions de câblage réseau et facilitant leur gestion.
- Switchs : Commutateurs réseau permettant une gestion et une configuration avancées du trafic de données.
- VLAN : Réseau local virtuel, permettant de segmenter un réseau physique en plusieurs réseaux logiques distincts.
- Pare-feu : Dispositif de sécurité filtrant les connexions entrantes et sortantes pour protéger le réseau contre les menaces.
- VPN : Réseau privé virtuel, permettant des connexions sécurisées et chiffrées à un réseau distant via Internet.
- Mise à la terre : Connexion des équipements électriques et réseau à la terre pour prévenir les surtensions et interférences.
- Bande passante : Capacité maximale de transmission de données d'un réseau, mesurée en bits par seconde (bps).
- **FTP (Foiled Twisted Pair)** : Type de câble Ethernet blindé pour réduire les interférences électromagnétiques et améliorer la transmission de données.
- **Cat 6A FTP** : Catégorie de câble Ethernet offrant des débits allant jusqu'à 10 Gbps, utilisé pour les connexions réseau à haute performance.
- **MDF (Main Distribution Frame)** : Cadre principal de distribution où les connexions réseau de l'immeuble sont centralisées.
- **OM4/OM5** : Types de fibres optiques multimodes utilisées pour des transmissions de données à haute vitesse et sur de longues distances.
- **Routeur multi-WAN** : Routeur capable de gérer plusieurs connexions Internet, assurant une répartition optimale du trafic et une redondance en cas de panne.

Introduction

L'entreprise **EXPERTY**, cabinet d'expertise comptable en pleine expansion, prévoit l'aménagement d'un **nouveau bâtiment** situé dans la banlieue ouest de Strasbourg afin d'accompagner sa croissance et d'améliorer les conditions de travail de ses collaborateurs. Ce projet vise à doter l'entreprise d'une infrastructure informatique moderne et performante, garantissant une connectivité optimale et une organisation efficace des ressources numériques. L'installation devra permettre une gestion fluide des échanges de données, assurer une sécurité renforcée et offrir une évolutivité adaptée aux besoins futurs. La mise en place d'un réseau structuré et fiable sera essentielle pour soutenir les activités de l'entreprise et assurer un environnement de travail adapté aux exigences actuelles.

Analyse besoins et contraintes

1. Besoins

Dans le cadre de l'aménagement du nouveau bâtiment d'EXPERTY, une infrastructure réseau complète et performante est indispensable afin de répondre aux exigences des collaborateurs et garantir une connectivité optimale. L'analyse des besoins met en évidence plusieurs éléments essentiels à prendre en compte pour assurer un réseau fiable, sécurisé et évolutif.

Tout d'abord, un **câblage structuré** doit être mis en place afin de garantir une connexion stable et performante pour l'ensemble des postes de travail. Chaque bureau devra être équipé d'au moins **deux prises RJ45** afin de privilégier une connexion filaire, réduisant ainsi la dépendance au réseau Wi-Fi et minimisant les risques de saturation. Pour assurer des performances optimales, l'utilisation de **câbles Ethernet de catégorie 6 ou 6A** est requise, permettant un débit élevé et une meilleure résistance aux interférences.

Par ailleurs, il est nécessaire de prévoir des **liaisons en fibre optique** pour interconnecter les différents étages et garantir une transmission rapide et stable des données. L'ensemble du câblage devra être **centralisé dans des baies de brassage**, situées dans des locaux techniques adaptés et sécurisés, bénéficiant d'une ventilation suffisante afin d'éviter toute surchauffe des équipements.

L'infrastructure réseau devra également intégrer des **switchs manageables**, permettant une gestion optimisée du trafic et une segmentation efficace via des **VLAN**. Cette organisation favorisera une meilleure isolation des flux de données et renforcera la sécurité interne du réseau. De plus, un **routeur professionnel** est nécessaire pour gérer les connexions internes et externes, avec la mise en place d'une **redondance via un second lien Internet** afin d'assurer la continuité de service en cas de panne du fournisseur principal.

En complément du réseau filaire, une **couverture Wi-Fi performante** est indispensable pour garantir la mobilité des collaborateurs, notamment dans les **salles de réunion** et les **espaces de travail partagés**. Pour répondre à ce besoin, il est recommandé de **déployer des bornes Wi-Fi 6** de manière stratégique, assurant ainsi une couverture homogène et limitant les interférences.

La **sécurité du réseau** doit être une priorité afin de protéger les **données sensibles** de l'entreprise. Il est donc essentiel d'installer un **pare-feu professionnel**, capable de filtrer les connexions entrantes et sortantes, de prévenir les intrusions et de garantir un **haut niveau de protection contre les cybermenaces**.

Enfin, le télétravail étant une nécessité pour EXPERTY, l'infrastructure devra être conçue pour offrir un accès distant sécurisé et performant. Il sera indispensable de mettre en place **un serveur VPN** permettant aux collaborateurs de se connecter à distance au réseau de l'entreprise en toute sécurité. Une **authentification forte** (comme le **MFA – Multi-Factor Authentication**) devra être activée afin de garantir que seuls les utilisateurs autorisés puissent accéder aux ressources internes. La gestion des accès devra être centralisée et contrôlée via une **solution de gestion des identités et des accès (IAM)**, permettant de restreindre l'accès aux seules ressources nécessaires selon le profil de chaque utilisateur. De plus, une **priorisation du trafic réseau** devra être envisagée pour garantir la fluidité des connexions à distance, en particulier pour les applications métier essentielles.

L'intégration d'un **système de supervision** sera également nécessaire afin de surveiller en temps réel la qualité des connexions à distance et d'identifier d'éventuels problèmes de latence ou de bande passante. Pour renforcer la **protection des données en télétravail**, les postes distants devront être équipés de **solutions de chiffrement**, garantissant que toutes les communications entre les collaborateurs et les serveurs de l'entreprise restent confidentielles.

2. Contraintes

L'installation informatique dans les nouveaux locaux d'EXPERTY devra respecter plusieurs contraintes qui influenceront la conception et le déploiement de l'infrastructure réseau. Tout d'abord, l'ensemble de l'installation devra se conformer aux **normes ISO/IEC 11801**, garantissant compatibilité des équipements, ainsi qu'aux **normes NF C 15-100**, qui imposent des distances minimales entre les câbles électriques et informatiques afin de prévenir les interférences et d'assurer la sécurité des installations.

La mise à la terre des équipements réseau et électriques sera une exigence essentielle afin de garantir la sécurité et la stabilité du réseau. Conformément aux normes citées plus haut, toutes les baies de brassage, switchs et prises réseau doivent être reliés à une mise à la

terre efficace pour éviter les surtensions et les interférences électromagnétiques. Une mauvaise mise à la terre peut entraîner des dysfonctionnements réseau et réduire la durée de vie des équipements informatiques.

Le projet devra être réalisé dans un **délai de 7 mois**, ce qui exigera une planification stricte et une coordination rigoureuse avec les prestataires responsables du câblage et de l'installation des équipements. La disponibilité des matériaux et des équipements devra être anticipée pour éviter tout retard pouvant compromettre le respect des échéances.

Le bâtiment étant totalement neuf et dépourvu de toute installation informatique, l'intégration du câblage devra être pensée de manière à ne pas perturber l'aménagement des locaux. L'espace disponible dans les murs, plafonds et planchers techniques étant limité, l'agencement des câbles devra être optimisé tout en assurant une bonne traçabilité et en respectant les espaces techniques dédiés.

Les locaux techniques, notamment les salles serveurs et les baies de brassage, devront être aménagés en tenant compte des **contraintes environnementales**, notamment la gestion de la température et de l'humidité, afin d'assurer un fonctionnement stable des équipements. L'alimentation électrique devra être fiable et exempte de fluctuations pouvant affecter le matériel. De plus, la capacité électrique du bâtiment devra être suffisante pour supporter l'ensemble de l'infrastructure et anticiper d'éventuelles extensions.

La **sécurité physique** des équipements devra être garantie, en particulier pour les baies de brassage et les serveurs, qui devront être protégés contre tout accès non autorisé. Il sera essentiel de mettre en place un **contrôle d'accès** aux locaux techniques pour assurer l'intégrité des installations. Par ailleurs, si des systèmes de surveillance ou d'alarme doivent être installés, leur compatibilité avec l'infrastructure réseau devra être prise en compte.

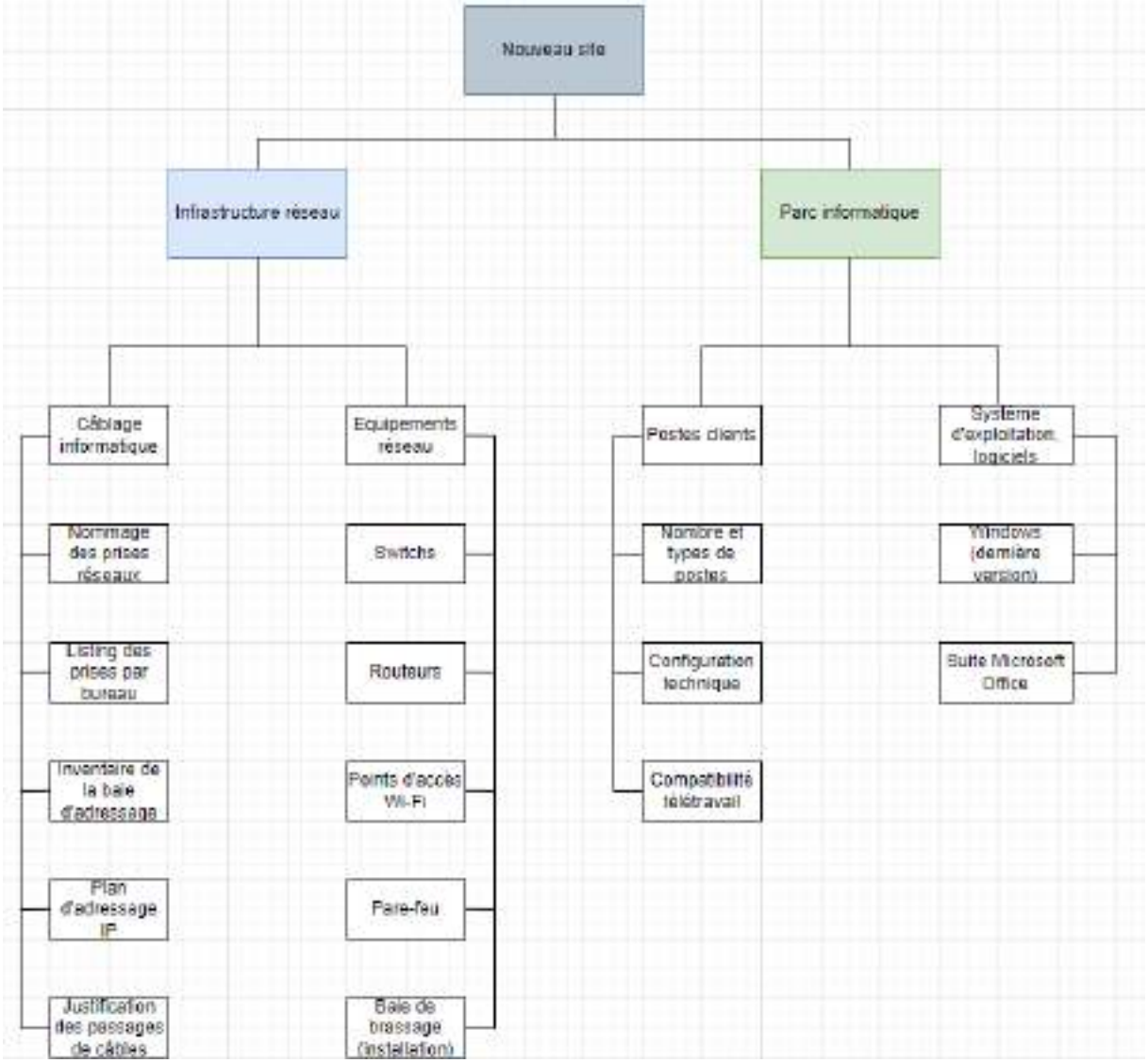
L'infrastructure devra être conçue pour être **évolutive**, afin d'accompagner la croissance de l'entreprise. Il sera donc nécessaire d'anticiper une capacité de bande passante suffisante, de prévoir un espace disponible dans les baies de brassage et d'intégrer des équipements modulables permettant d'ajouter de nouvelles technologies sans perturber le fonctionnement du réseau.

L'entreprise souhaitant favoriser le **télétravail**, l'infrastructure devra également permettre des accès distants sécurisés. Cela impliquera la mise en place d'un système garantissant l'authentification et la gestion des connexions à distance tout en protégeant les données sensibles.

Le budget alloué au projet n'étant pas précisément défini, il sera nécessaire d'établir une estimation des coûts en veillant à optimiser les choix technologiques pour respecter un cadre budgétaire réaliste. Certains compromis devront être faits entre performance, évolutivité et coûts d'installation.

Enfin, une fois l'infrastructure en place, elle devra être supervisée en continu afin de détecter d'éventuelles anomalies et d'assurer un fonctionnement optimal du réseau. Cette exigence nécessitera la mise en place d'un suivi rigoureux des performances et des incidents, ce qui impliquera des ressources humaines et techniques adaptées.

Product Breakdown Structure



Nous avons découpé notre PBS en 3 grandes catégories :

- L'infrastructure réseau : Pour regrouper tout ce qui concerne la mise en place du réseau informatique du nouveau bâtiment.

  Le câblage est la base de l'infrastructure. Il permet de relier tous les équipements informatiques entre eux et d'assurer une connexion fiable. Toutes les étapes nécessaires à la mise en place d'un câblage efficace sont listées, incluant l'étude des besoins, la planification, l'installation et la validation des connexions.

  La baie de brassage est l'élément central de l'infrastructure, organisant les connexions réseau. Les équipements tels que les switchs, routeurs et points d'accès Wi-Fi permettent de gérer et réguler le trafic du réseau, assurant une connexion stable et sécurisée.

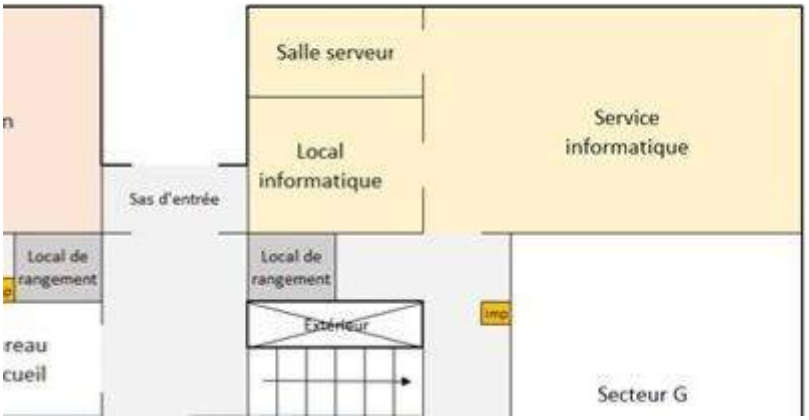
- Le parc informatique : Pour tout ce qui est lié aux équipements des utilisateurs et à leur bon fonctionnement. Cela inclut la gestion des postes clients, l'installation des logiciels nécessaires et la configuration des périphériques. Il comprend aussi la mise en place d'un accès distant sécurisé et l'intégration des solutions collaboratives pour le télétravail.

- La gestion de projet : Elle regroupe la liste des toutes les étapes nécessaires jusqu'à la fin du projet.

  On a une première sous-catégorie comprend le travail préparatoire en amont, incluant l'analyse des besoins, les estimations des coûts et la planification des différentes tâches. La mise en place d'un planning structuré permet d'anticiper et d'optimiser les différentes phases du projet. Et ensuite la deuxième partie orientée sur la finalisation et le déploiement physique du projet. Cela inclut le suivi budgétaire, la coordination avec les prestataires, la documentation technique et la formation des utilisateurs pour assurer une transition fluide vers la nouvelle infrastructure.

Choix des locaux techniques

Les locaux techniques jouent un rôle central dans la gestion du réseau informatique. Leur emplacement doit être stratégique afin de minimiser les distances de câblage, garantir une connectivité optimale et assurer la sécurité des équipements.



Sur notre plan, la salle serveur et le local informatique sont à accès restreint par badge pour limiter les accès non autorisés, avec un accès venant uniquement de la salle du service informatique, cela facilité l'accès pour les employés concernés tout en limitant les accès non autorisés. De plus, l'emplacement de la salle serveur est le moins exentéré centré possible compte tenu des plans pour réduire au mieux la longueur des câbles réseau et fluidifier la latence des connexions. Et pour garantir un réseau stable et sécurisé, un circuit de la mise à la terre pour la baie de brassage principale sera réalisé.

Dans la salle serveur se trouvera les équipements les plus sensibles avec la baie de brassage principale pour centraliser toutes les connexions du réseau, le switch cœur du réseau qui sera de niveau 3. Également, il y a aura le routeur principal pour l'accès à internet et le pare-feu pour sécuriser les connexions entrantes et sortantes. Etant donnée que la salle serveur reste relativement étroite et que les équipements génèreront une chaleur assez importante, nous recommandons d'équiper un système de climatisation dédié à ces locaux.

Pour le local informatique, nous prévoyons d'utiliser cette salle pour gérer le matériel, les interventions et les différentes configurations nécessaires. A l'intérieur, nous stockerons tous le matériel informatique (PC, switchs de secours, câbles RJ45), aussi nous inclurons un poste de travail qui sera spécifique pour configurer les équipements du réseau. Etant donné le volume d'employé, nous prévoyons de rajouter un banc de test dans cette pièce pour être plus apte à mettre en production les nouveaux équipements. Cela permettra d'anticiper d'éventuels problèmes techniques et d'assurer une transition fluide lors de la mise en service des équipements réseau.

Solutions retenues

1. Câblage

Tout d'abord, la mise à la terre sera réalisée sur l'ensemble des infrastructures réseau afin de garantir un fonctionnement optimal et une protection efficace contre les surtensions. Tous les racks de brassage et équipements actifs (switchs, routeurs, pare-feu) seront reliés à une prise de terre dédiée, conformément aux bonnes pratiques de câblage. De plus, les câbles blindés (FTP ou STP) seront connectés à la terre pour limiter les interférences électromagnétiques et garantir une transmission stable des données. Un test de continuité et de résistance sera effectué avant la mise en production pour s'assurer de l'efficacité du dispositif.

L'installation du réseau informatique dans le nouveau bâtiment d'EXPERTY doit répondre à plusieurs exigences techniques pour assurer une performance optimale, une flexibilité et une sécurité à long terme. Le câblage horizontal sera effectué en utilisant des câbles **Cat 6A FTP**, qui sont capables de supporter des débits allant jusqu'à 10 Gbps. Ce choix est non seulement suffisant pour répondre aux besoins des bureaux, mais il offre également un bon blindage pour réduire les interférences électromagnétiques (EMI) et garantir la durabilité du système. Le blindage FTP est essentiel dans un environnement où les interférences électriques pourraient affecter la qualité du réseau. Ce type de câblage est particulièrement adapté pour une installation pérenne et évolutive.

Pour garantir la sécurité et la conformité des installations électriques, il est essentiel d'utiliser des **goulottes murales compartimentées**, permettant de séparer les câbles réseau des câbles électriques. Cette séparation est cruciale pour éviter toute interférence électromagnétique qui pourrait perturber les communications réseau. En outre, ces goulottes facilitent l'organisation du câblage, rendant le réseau plus facile à gérer, à maintenir et à étendre. L'installation sera réalisée sous faux plancher dans les espaces de bureaux ouverts (open spaces), ce qui permettra une grande flexibilité pour les aménagements futurs. Ce choix est particulièrement utile pour les bureaux qui peuvent nécessiter des réorganisations fréquentes, permettant ainsi de déplacer les câbles de manière rapide et simple sans perturber l'ensemble du réseau. Les **passages par faux plafonds dans les couloirs** permettront également de minimiser l'encombrement au sol et d'optimiser l'espace disponible tout en assurant une gestion discrète et pratique du câblage.

Pour le **câblage vertical**, utilisé pour la liaison entre les étages (notamment entre la **MDF** et l'**IDF**), des **fibres optiques OM4/OM5** seront déployées. Ces types de fibres sont idéaux pour les connexions longues distances (notamment entre le rez-de-chaussée et le premier étage) et sont capables de supporter des débits élevés allant jusqu'à 40 Gbps, voire plus. La fibre optique, contrairement au cuivre, n'est pas sujette aux interférences et offre une bande passante bien plus large. Afin de protéger ces câbles sensibles, ils seront installés dans des

gainages techniques verticaux spécifiquement conçus pour éviter toute détérioration. De plus, il sera impératif de veiller à ce que les fibres ne subissent pas de courbures excessives, ce qui pourrait endommager le signal. Ces gaines permettent également de prolonger la durée de vie de la fibre optique et de garantir une transmission de données optimale sur le long terme.

Concernant la **liaison backbone** entre les baies de brassage, une **fibre optique OM4 ou OM5** sera utilisée pour assurer des débits de 40 Gbps ou plus. Cela permettra de garantir une performance maximale entre les différents équipements réseau, y compris les serveurs et les commutateurs, tout en réduisant le risque de goulots d'étranglement dans les transmissions de données à haute vitesse.

Les **prises murales** seront des **RJ45 Cat 6A ou Cat 7**, choisies pour leur capacité à supporter des débits élevés, jusqu'à 10 Gbps, et pour leur compatibilité avec les équipements modernes. Ces prises sont aussi prêtes pour de futures évolutions, telles que le passage à des débits plus élevés, ce qui permet d'assurer une installation à l'épreuve du temps. Elles garantiront une excellente qualité de connexion pour les utilisateurs tout en assurant la compatibilité avec l'ensemble des équipements prévus dans le réseau.

Il est essentiel de respecter les règles de **distances maximales** entre le panneau de brassage et la prise murale, qui ne doit pas dépasser 90 mètres. Cela est nécessaire pour éviter une dégradation du signal et garantir que les performances réseau soient optimales. Si certaines distances dépassent ces limites, des équipements comme des répéteurs ou des switches devront être installés pour maintenir la qualité du réseau. De plus, il est impératif de prévoir des **chemins de câbles séparés** pour l'alimentation électrique et le réseau informatique. Cela réduira les risques d'interférences électromagnétiques et assurera la sécurité de l'installation. Ainsi, cette approche intégrée de la gestion du câblage horizontal, vertical, et de la liaison backbone, combinée à l'utilisation de fibre optique et à des baies de brassage bien dimensionnées, permettra d'assurer la stabilité et la performance du réseau d'EXPERTY à long terme, tout en offrant la flexibilité nécessaire pour faire face à l'évolution des besoins.

2. Le Matériel

Pour répondre aux besoins de l'entreprise EXPERTY, le parc informatique sera renouvelé avec des équipements performants et adaptés au télétravail.

Les postes clients seront fournis par **Lenovo ThinkPad X1 Carbon**. Ces modèles sont robustes, performants et légers, offrant une grande fiabilité pour les employés en télétravail. Ils seront équipés de **processeurs Intel Core i7** (génération récente), de **16 Go de RAM**, et de **SSD de 512 Go** pour garantir des performances optimales. Un écran de **14" ou 15" Full**

HD offrira une expérience visuelle agréable pour le travail bureautique et les visioconférences.

L'infrastructure réseau sera modernisée avec des équipements **Cisco Meraki** et des **switches Cisco Catalyst**. Ces solutions permettront de gérer le réseau de manière centralisée et sécurisée, avec des fonctionnalités adaptées au télétravail. Des équipements **VPN Cisco AnyConnect** assureront des connexions sécurisées pour les employés travaillant à distance.

Pour améliorer l'environnement de télétravail, des **moniteurs Dell UltraSharp 27" 4K** et des **webcams Logitech Brio** seront fournis, afin d'optimiser la productivité et la qualité des visioconférences. Des **casques Jabra Evolve2 65** garantiront des appels audios clairs et confortables.

Le système d'exploitation sera mis à jour vers **Windows 11 Pro**, offrant une gestion à distance efficace et une sécurité renforcée. La suite **Microsoft 365 Business Premium** sera utilisée pour les outils bureautiques, incluant **Word**, **Excel**, **PowerPoint**, **Outlook**, et **Teams**, tout en permettant le stockage et l'accès aux fichiers via **OneDrive for Business**.

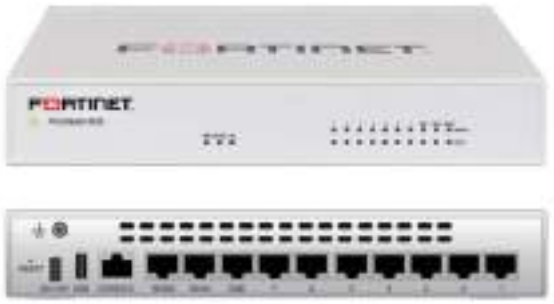
La sécurité sera renforcée avec **Microsoft Defender for Business** et **Sophos Endpoint Protection**, tandis que des solutions de sauvegarde des données, telles que **Veeam** ou **Acronis**, garantiront la protection et la récupération rapide des informations sensibles.

Enfin, pour la gestion des appareils en télétravail, **Microsoft Intune** sera utilisé pour assurer une gestion centralisée et sécurisée de tous les équipements.

Pour les **points d'accès Wi-Fi, l**es **Ubiquiti UniFi 6**. Ces équipements offrent une couverture optimale, une gestion centralisée via le contrôleur UniFi, et sont parfaitement adaptés à un environnement avec de nombreux utilisateurs en télétravail et sur site. Le Wi-Fi 6 permet des débits plus élevés et une meilleure gestion des appareils connectés, réduisant les interférences, ce qui est essentiel pour EXPERTY.

Pour les **switches réseau**, le choix se porte sur les **Ubiquiti UniFi Switch**. Ces équipements offrent une gestion simplifiée et une fiabilité optimale pour gérer un réseau avec un grand nombre de terminaux connectés. Ils sont compatibles avec les configurations avancées, telles que les **VLAN** et la **QoS**, qui permettent de prioriser certains types de trafic, comme les visioconférences.

En matière de **sécurisation du réseau**, le choix se fait sur un **pare-feu FortiGate**. Il offre une sécurité robuste, idéale pour protéger le réseau contre les menaces externes tout en permettant une gestion facile des accès à distance pour les employés en télétravail. Pour les connexions distantes sécurisées, une solution **FortiGate SSL VPN** sera également mise en place, garantissant des connexions sécurisées.



Pour contrôler les accès réseau, la solution **802.1X** sera choisie, offrant un contrôle centralisé des permissions d'accès et garantissant que seuls les appareils autorisés se connectent au réseau.

Enfin, pour la gestion centralisée du réseau, on choisira du **Ubiquiti UniFi Controller**, qui permet une administration facile, une surveillance en temps réel et le déploiement rapide des configurations et mises à jour sur l'ensemble des équipements réseau.

3. Connexion :

Pour la connexion internet, en prenant en compte tous les paramètres qui nécessite une connexion Internet fiable, sécurisée et performante, deux principales solutions sont envisageables : la fibre FTTO (Fiber To The Office) et la fibre FTTH Pro (Fiber To The Home Pro).

Après analyse des besoins de l'entreprise EXPERTY, il est recommandé d'opter pour la fibre FTTO. Avec 80 employés répartis sur deux étages, les besoins en connectivité sont importants, notamment pour l'accès aux logiciels métiers, les échanges de données comptables et la sécurisation des connexions des employés en télétravail via VPN.

La fibre FTTO garantit un débit stable et symétrique, ce qui évite les ralentissements pouvant impacter la productivité. De plus, elle offre une sécurité accrue grâce à une connexion privée et un service contractuel assurant une intervention rapide en cas de panne. En raison de la nature sensible des données traitées par EXPERTY, il est essentiel de disposer d'une infrastructure réseau fiable et performante.

Bien que la fibre FTTH Pro puisse constituer une alternative plus économique, elle présente des risques en termes de disponibilité et de stabilité. Son débit étant partagé avec d'autres entreprises, les performances peuvent fluctuer aux heures de pointe, ce qui peut perturber le bon fonctionnement des services comptables.

Ainsi, l'investissement dans une fibre FTTO représente un choix stratégique pour EXPERTY, garantissant une continuité de service optimale et une sécurité renforcée pour l'ensemble des employés et clients du cabinet.

Pour l'entreprise EXPERTY, il est conseillé d'opter pour deux connexions fibre afin d'assurer une **haute disponibilité** et une **résilience** du réseau. Avec un nombre important d'employés

et des besoins accrus en télétravail, avoir deux connexions permettrait de garantir une **continuité de service** en cas de panne de l'une des lignes, tout en augmentant la **bande passante** disponible pour le télétravail, les visioconférences et les applications cloud. En cas de défaillance d'une ligne, la deuxième connexion prendrait automatiquement le relais, évitant ainsi toute interruption de service.

Le choix de l'opérateur se portera sur **Orange Business Services**, reconnu pour la fiabilité de ses connexions fibre et son service client dédié aux entreprises. Orange offre une couverture géographique étendue, avec des services adaptés aux besoins de performance et de sécurité des entreprises en croissance. De plus, ses solutions de gestion de la connectivité et de sécurité réseau, telles que les **réseaux privés virtuels (VPN)** et la **sécurisation des accès à distance**, sont particulièrement adaptées pour une entreprise ayant une forte demande en télétravail.

Pour l'aménagement, il est recommandé de mettre en place un **routeur multi-WAN** pour gérer les deux connexions fibre. Ce type de routeur permettra de répartir le trafic de manière optimale grâce au **load balancing**, tout en assurant un **failover automatique** si l'une des connexions tombe en panne. Cela garantit que les employés continueront de travailler sans interruption, que ce soit sur site ou en télétravail, pour l'entreprise EXPERTY notre choix s'est porté sur le modèle de chez Ubiquiti, l' **Ubiquiti EdgeRouter 4, qui** est un routeur performant avec 3 ports WAN, capable de gérer plusieurs connexions Internet simultanément. Il est doté de capacités de **load balancing** et de **failover** pour une redondance réseau, ainsi que des fonctionnalités de pare-feu et VPN . En outre, il est essentiel d'intégrer un **pare-feu de niveau entreprise**, tel que **FortiGate**, pour sécuriser l'ensemble du réseau, ainsi que des outils de **monitoring** pour surveiller en temps réel l'état des connexions et détecter rapidement tout problème.

Afin d'optimiser la gestion du réseau interne, nous mettons en place un Wi-Fi séparé pour les employés et les visiteurs. Cette séparation permet de sécuriser l'accès aux ressources internes tout en offrant une connexion contrôlée aux invités sans compromettre

l'infrastructure principale de l'entreprise. Pour ce faire, nous configurons deux réseaux distincts via des points d'accès Wi-Fi : un réseau interne réservé aux employés, qui donne accès aux ressources critiques de l'entreprise, et un réseau invité isoler, permettant uniquement l'accès à Internet avec un débit limité pour éviter toute surcharge.

4. VPN

Par ailleurs, pour garantir une connexion sécurisée aux collaborateurs travaillant à distance, un VPN est déployé. Celui-ci permet aux employés en télétravail de se connecter aux systèmes internes de l'entreprise de manière chiffrée et sécurisée, réduisant ainsi les risques d'intrusion ou de fuite de données sensibles.

Dans le cadre de la mise en place d'un **VPN sécurisé** pour le télétravail, deux solutions ont été envisagées : **FortiGate (Fortinet) et Cisco ASA (Adaptive Security Appliance)**. Après comparaison des performances, de la sécurité, de la facilité d'administration et des coûts, le choix s'est porté sur **FortiGate** pour plusieurs raisons.

FortiGate offre une **interface de gestion intuitive**, facilitant l'administration et la configuration des accès distants. Contrairement à Cisco ASA, qui repose principalement sur une interface en ligne de commande (CLI), FortiGate propose une gestion centralisée et simplifiée via une interface graphique ergonomique, adaptée aux besoins d'EXPERTY.

En matière de **sécurité et de gestion du VPN**, FortiGate intègre **nativement les protocoles SSL VPN et IPSec**, ainsi que des fonctionnalités avancées telles que l'**Intrusion Prevention System (IPS)**, un **antivirus** et un **filtrage applicatif**, sans nécessiter de licences supplémentaires. De plus, l'authentification forte via **MFA (Multi-Factor Authentication)** est directement prise en charge, renforçant ainsi la sécurité des connexions à distance.

Sur le plan de la **scalabilité**, FortiGate permet d'évoluer facilement en intégrant des fonctionnalités de **SD-WAN**, optimisant ainsi la gestion des connexions Internet et la répartition du trafic en fonction des performances des liens disponibles. Cette flexibilité est un atout pour anticiper les besoins futurs de l'entreprise.

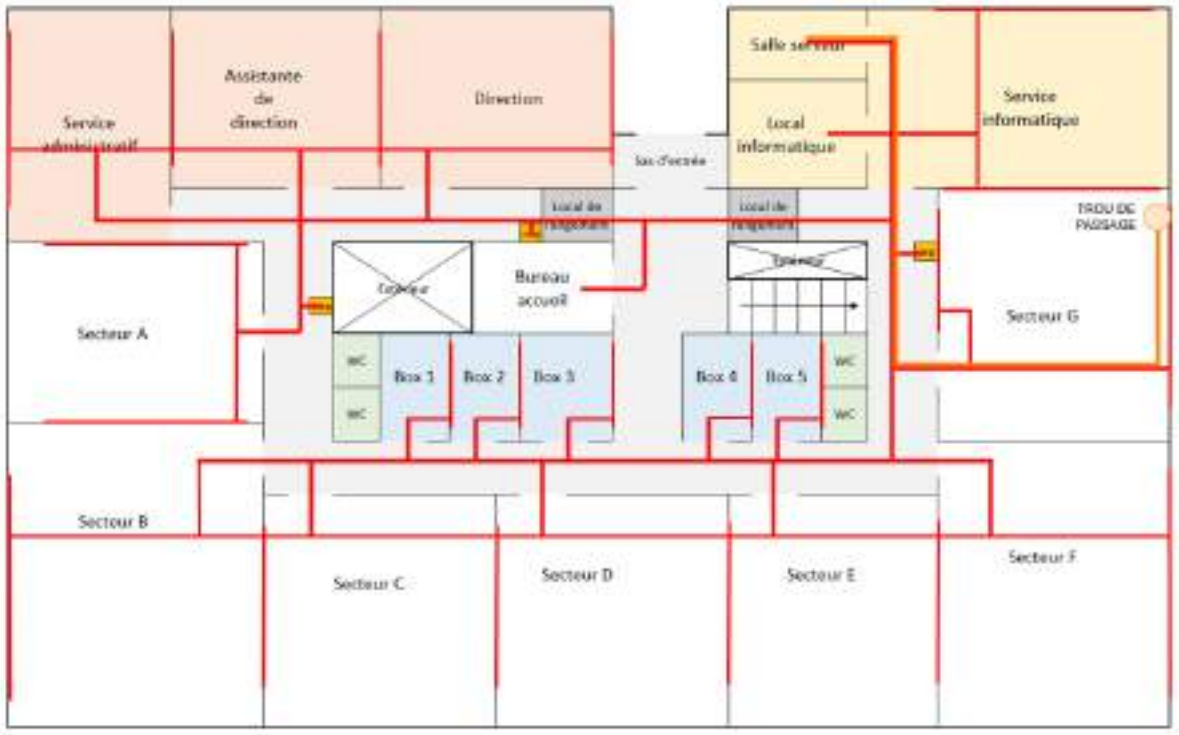
Enfin, le **coût** a également été un critère déterminant. Contrairement à Cisco ASA, où certaines fonctionnalités nécessitent l'achat de licences supplémentaires, FortiGate propose un **ensemble complet de fonctionnalités** directement incluses dans l'appliance, offrant ainsi un meilleur **rapport qualité/prix**.

Pour répondre aux besoins d'EXPERTY, le modèle **FortiGate 60F** a été retenu, offrant une capacité adaptée à une cinquantaine d'utilisateurs distants simultanés. En cas d'évolution du nombre de connexions, une montée en gamme vers le **FortiGate 100F** pourra être envisagée, notamment pour mettre en place une **architecture redondante (HA - High Availability)** afin d'assurer une continuité de service optimale.

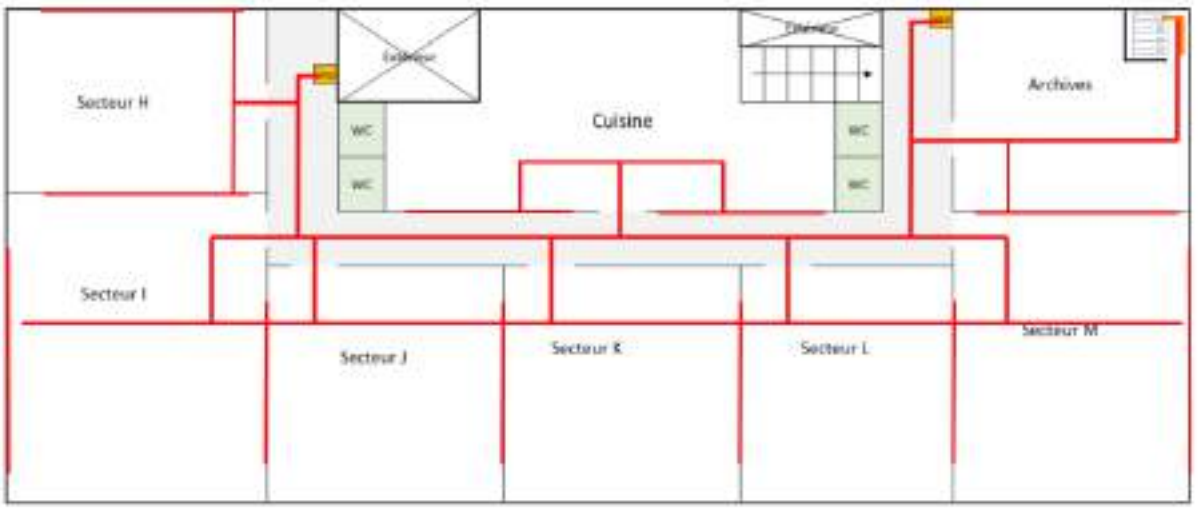
Partie réseau

1. Plan de câblage

RDC



Etage



2. Nombre de prises pour chaque bureau

Numéro de Prise	Nom de la Prise	Localisation		Nombre
ETAGE 1				
1 -- 2	1E-100-01 - 1E-100-02	Direction		2
3 -- 6	1E-101-01 - 1E-101-04	Assistante de direction		4
7 -- 16	1E-102-01 - 1E-102-10	Service administratif		10
17 -- 26	1E-103-01 - 1E-103-10	Service informatique		10
27 -- 30	1E-104-01 - 1E-104-04	Accueil		4
31 -- 38	1E-A-01 - 1E-A-08	Secteur A		8
39 -- 48	1E-B-01 - 1E-B-10	Secteur B		10
49 -- 56	1E-C-01 - 1E-C-08	Secteur C		8
57 -- 64	1E-D-01 - 1E-D-08	Secteur D		8
65 -- 72	1E-E-01 - 1E-E-08	Secteur E		8
73 -- 82	1E-F-01 - 1E-F-10	Secteur F		10
83 -- 90	1E-G-01 - 1E-G-08	Secteur G		8
91 -- 92	1E-B1-01 - 1E-B1-02	Box 1		2
93 -- 94	1E-B2-01 - 1E-B2-02	Box 2		2
95 -- 96	1E-B3-01 - 1E-B3-02	Box 3		2
97 -- 98	1E-B4-01 - 1E-B4-02	Box 4		2
99 -- 100	1E-B5-01 - 1E-B5-02	Box 5		2
ETAGE 2				
101 -- 108	2E-H-01 - 2E-H-08	Secteur H		8
109 -- 118	2E-I-01 - 2E-I-10	Secteur I		10
119 -- 126	2E-J-01 - 2E-J-08	Secteur J		8
127 -- 134	2E-K-01 - 2E-K-08	Secteur K		8
135 -- 142	2E-L-01 - 2E-L-08	Secteur L		8
143 -- 152	2E-M-01 - 2E-M-10	Secteur M		10
153 -- 153	2E-A-01 - 2E-A-01	Archives		0
154 -- 155	2E-C-01 - 2E-C-02	Cuisine		2
MIX				
156 -- 158	1E-IMP-01 - 1E-IMP-03	Imprimantes		3
159 -- 160	2E-IMP-01 - 2E-IMP-04	Imprimantes		2

Pour la salle du service administratif, qui compte 5 personnes, nous avons prévu 10 prises RJ45. Chaque employé disposera ainsi d'une prise principale pour son poste de travail. De plus, afin d'assurer une continuité en cas de problème matériel ou de besoin supplémentaire

(ajout d'un équipement, changement de poste, etc.) nous avons prévu une prise de secours par personne.

Le nommage des prises suit une convention spécifique. Par exemple pour la salle du service administratif, la 1ère prise sera nommée "1E-102-01". Voici la signification de ce nommage :

- **1E** : Représente le premier étage.
- **102** : Désigne la salle du service administratif.
- **01** : Indique la première prise de cette salle.

Ainsi, la deuxième prise sera nommée "1E-102-02", et ainsi de suite jusqu'à la dixième prise, "1E-102-10".

Dans le bureau de l'assistante de direction, où travaillent deux personnes, nous installerons quatre prises RJ45. Chacune disposera d'une prise pour son poste de travail, tandis que les deux prises supplémentaires permettront d'anticiper d'éventuels besoins futurs.

Le nommage de la première prise pour cette salle sera "1E-101-01". Les prises suivantes seront numérotées de manière séquentielle, allant jusqu'à "1E-101-04".

Pour le bureau du directeur, nous prévoyons deux prises RJ45. La première sera dédiée à son poste de travail principal, tandis que la seconde servira de solution de secours.

Le nommage pour ces prises sera le suivant : la première prise portera le nom "1E-100-01", et la seconde "1E-100-02".

En ce qui concerne le service informatique, où travaillent 5 personnes, nous avons prévu 10 prises RJ45. Chaque technicien disposera d'une prise dédiée pour son poste de travail, tandis que les prises supplémentaires permettront de connecter des équipements additionnels tels que des serveurs temporaires ou encore des périphériques réseau. Le nommage des prises pour cette salle sera "1E-103-01" jusqu'à "1E-103-10".

En ce qui concerne l'accueil, où travaillent 2 personnes, nous avons prévu 4 prises RJ45. Chaque standardiste disposera d'une prise dédiée pour son poste de travail. Le nommage des prises pour cette zone sera "1E-104-01" à "1E-104-04"

Pour les secteurs B et F du rez-de-chaussée, qui sont les plus grandes salles de cet étage et accueillent 5 personnes, nous avons prévu 10 prises RJ45. Cela permet à chaque personne de disposer d'une prise dédiée pour son poste de travail, ainsi qu'une prise de secours pour anticiper tout besoin supplémentaire ou pallier une éventuelle panne. Le nommage des prises pour la salle B sera "1E-B-01" à "1E-B-10", et pour la salle F, ce sera "1E-F-01" à "1E-F-10".

Pour les autres salles du rez-de-chaussée, qui accueillent également 5 personnes chacune, nous avons prévu 8 prises RJ45. Chaque employé disposera d'une prise pour son poste de

travail, et les trois prises supplémentaires permettront de connecter des équipements additionnels comme des imprimantes, téléphones IP ou encore des postes temporaires si nécessaire. Le nommage des prises pour les autres salles sera le suivant : pour les salles A, C, D, E et G, les prises seront numérotées de "1E-A-01" à "1E-A-08", "1E-C-01" à "1E-C-08", "1E-D-01" à "1E-D-08", "1E-E-01" à "1E-E-08" et "1E-G-01" à "1E-G-08" respectivement.

Nous installons deux prises RJ45 dans chaque box d'accueil des clients pour garantir une connectivité fiable et continue. Deux prises offrent la redondance nécessaire en cas de défaillance. Le nommage des prises pour les box sera le suivant : pour les cinq box, les prises seront numérotées de "1E-B1-01" à "1E-B1-02", "1E-B2-01" à "1E-B2-02", "1E-B3-01" à "1E-B3-02", "1E-B4-01" à "1E-B4-02" et "1E-B5-01" à "1E-B5-02".

La même logique est appliquée aux salles de l'étage. Pour les secteurs I et M, qui sont les plus grandes salles, nous avons prévu 10 prises RJ45 afin de répondre aux besoins des 5 collaborateurs présents dans chacune d'elles. Chaque personne disposera d'une prise dédiée, et les prises supplémentaires permettront d'anticiper l'ajout d'équipements ou de servir de solution de secours en cas de problème technique. Le nommage des prises pour la salle I sera "2E-I-01" à "2E-I-10", et pour la salle M, ce sera "2E-M-01" à "2E-M-10".

Pour les autres salles de l'étage, qui comptent également 5 personnes, nous avons prévu 8 prises RJ45. Chaque employé disposera d'une prise pour son poste de travail, et les trois prises supplémentaires permettront de connecter des équipements additionnels comme des imprimantes, téléphones IP ou encore des postes temporaires si nécessaire. Le nommage des prises pour ces salles sera le suivant : pour les salles H, J, K et L, les prises seront numérotées de "2E-H-01" à "2E-H-08", "2E-J-01" à "2E-J-08", "2E-K-01" à "2E-K-08" et "2E-L-01" à "2E-L-08" respectivement.

Pour la cuisine, nous avons prévu deux prises RJ45 afin de répondre aux éventuels besoins futurs. En effet, avec les avancées technologiques, il est possible que des appareils de cuisine nécessitent des connexions réseau. Cette prévision permet de garantir que la cuisine sera équipée pour accueillir ces innovations sans nécessiter de modifications majeures à l'installation électrique. Le nommage des prises pour la cuisine sera "2E-C-01" à "2E-C-02".

Nous installons une prise RJ45 pour chaque imprimante afin d'assurer une connectivité fiable et directe. Une seule prise est suffisante pour répondre aux besoins spécifiques des imprimantes, offrant ainsi une configuration simple et efficace. Le nommage des prises pour les imprimantes au premier étage sera "1E-IMP-01" à "1E-IMP-03", et pour le deuxième étage, ce sera "2E-IMP-01" à "2E-IMP-02".

3. Segmentation avec les VLANs

Afin d'optimiser la gestion du réseau et d'améliorer la sécurité, nous mettons en place une segmentation en VLAN (Virtual Local Area Network) sur l'ensemble de l'infrastructure. Cette organisation permet :

- Une meilleure isolation des flux de données pour éviter toute contamination entre services.
- Une gestion simplifiée du trafic réseau en affectant des règles spécifiques à chaque VLAN.
- Une sécurité accrue, en limitant la communication entre les réseaux selon les besoins.

L'interconnexion entre ces VLAN sera gérée via un switch de niveau 3 (L3), permettant un routage optimisé tout en appliquant des politiques de sécurité strictes via le pare-feu. Aussi nous privilégieront des adresse IP fixes pour les équipements sensibles comme les serveurs, imprimantes, caméras, switchs, routeurs. Et des adresses dynamiques pour les postes de travails.

Voici notre plan d'adressage :

Usage	VLAN	Sous-Réseau	Masque
Admistration	10	192.168.10.0/24	255.255.255.0
Service Comptabilité	20	192.168.20.0/24	255.255.255.0
Service Informatique	30	192.168.30.0/24	255.255.255.0
Poste Employés	40	192.168.40.0/24	255.255.255.0
Wi-Fi Employés	50	192.168.50.0/24	255.255.255.0
Wi-Fi Invités	60	192.168.60.0/24	255.255.255.0
Imprimantes	70	192.168.70.0/24	255.255.255.0
Téléphonie IP	80	192.168.80.0/24	255.255.255.0
Equipement Réseau	90	192.168.90.0/24	255.255.255.0

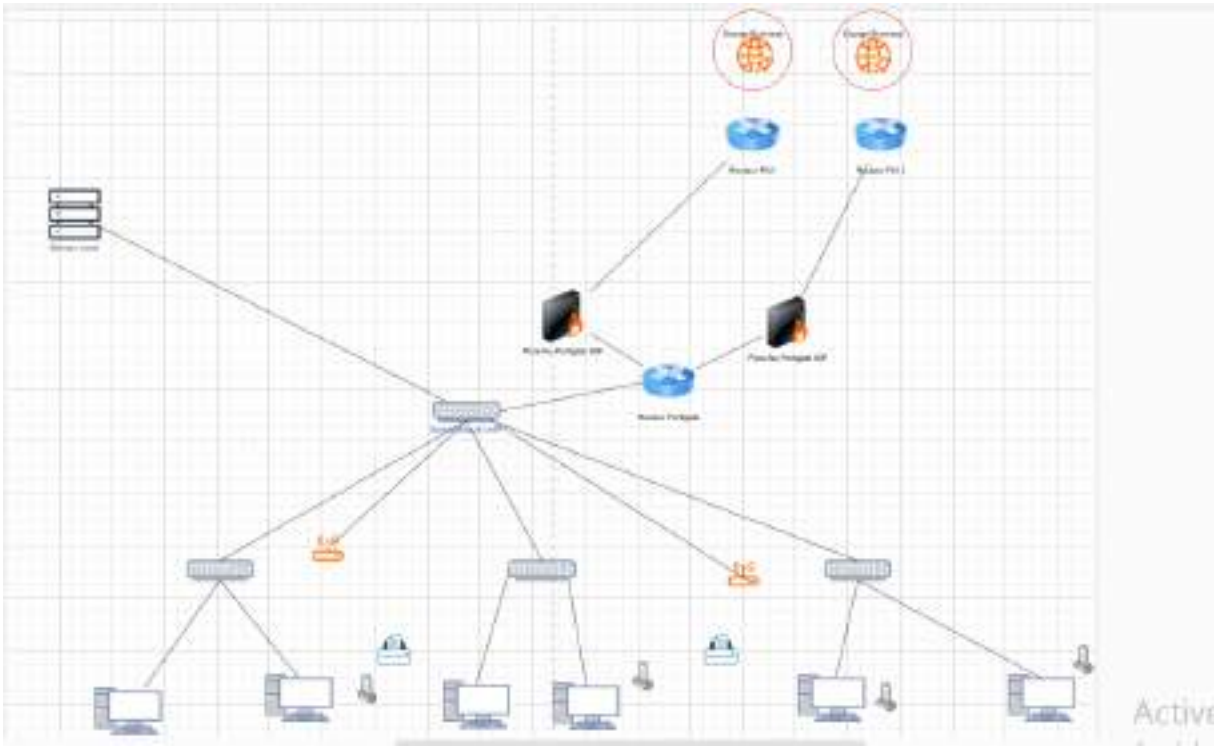
4. Justification le passage des câbles

Faire passer les câbles RJ45 et fibre optique dans le plafond présente plusieurs avantages importants. Tout d'abord, cela rend l'espace plus esthétique en évitant les câbles visibles qui peuvent encombrer et donner un aspect désordonné. En plus, les câbles dans le plafond sont mieux protégés contre les dommages accidentels causés par des chocs ou des manipulations involontaires.

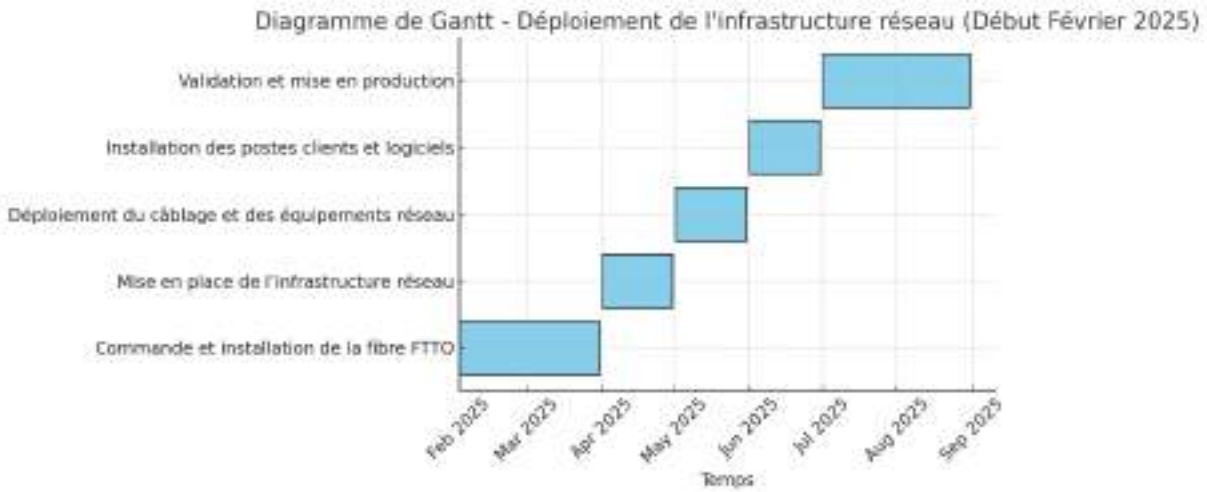
En termes de sécurité, les câbles dans le plafond sont moins exposés aux risques d'incendie et d'humidité, offrant ainsi une protection supplémentaire. De plus, cela facilite la maintenance et les mises à jour. En cas de besoin, il est plus simple d'accéder aux câbles dans le plafond sans perturber les activités au sol.

Cela permet également de libérer de l'espace au sol et sur les murs, offrant plus de possibilités pour d'autres équipements ou mobiliers. Enfin, elle respecte les normes de câblage qui recommandent souvent cette méthode pour des raisons de sécurité et d'organisation.

5. Schéma réseau



Planning



Détails :

Commande et installation de la fibre FTTO :

- Commande de la fibre FTTO auprès de l'opérateur.
- Installation du point d'entrée de la fibre dans l'entreprise.

Mise en place de l'infrastructure réseau :

- Installation de la baie de brassage principale (RDC).
- Installation de la baie de brassage secondaire (Étage).

Déploiement du câblage et des équipements réseau :

- Câblage réseau (RJ45 dans les bureaux + fibre optique entre les baies).
- Installation des switchs et brassage des connexions réseau.
- Installation et configuration du Wi-Fi (Employés & Invités).
- Configuration du pare-feu et du VPN pour le télétravail sécurisé.

Installation des postes clients et logiciels :

- Réception et déploiement des nouveaux postes clients (PC, écrans, périphériques).
- Installation des systèmes d'exploitation (Windows + mises à jour).
- Installation et configuration des logiciels métiers (Suite Microsoft Office, logiciels comptables, outils internes).
- Création et configuration des comptes utilisateurs (AD, messagerie, accès VPN, droits d'accès réseau).

Validation et mise en production :

- Tests réseau et validation des performances et de la sécurité.
- Tests des postes clients et vérification des logiciels installés.
- Mise en production et formation des employés sur l'utilisation du réseau et des équipements.

Budget

Liste des équipements				
Nom	Quantité	Prix unitaire	Total	Mensualité
PC Lenovo TP X1 Carbon	85	2 100 €	178 500 €	
Moniteurs Dell UltraSharp 27" 4K	40	320 €	12 800 €	
Webcams Logitech Brio 305	40	70 €	2 800 €	
Casques Jabra Evolve2 65	85	150 €	12 750 €	
Sacoche ESSENTIELB 17"	85	20 €	1 700 €	
Souris sans fil LOGITECH	85	18 €	1 530 €	
Cordons RJ45	159	150 €	23 850 €	
Licences Windows	80	37 €	2 960 €	
Microsoft Office	80		0 €	1 440 €
Switches	6	612 €	3 672 €	
Routeurs	1	206 €	206 €	
Baie de brassage	2	2 600 €	5 200 €	
Point accès long portée Ubiquiti	2	195 €	390 €	
Onduleur APC SMC1500IC	2	815 €	1 630 €	
Mise à la terre	1	500 €	500 €	
Climatisation Salle serveur	1	1 300 €	1 300 €	(Entretien) 15 €
Abonnement Fibre Orange				55 €
TOTAL			249 788 €	1 510 €

Dans le cadre du projet d'aménagement du nouveau bâtiment d'EXPERTY, un budget détaillé a été établi afin d'assurer l'acquisition et l'installation des équipements informatiques et réseaux nécessaires.

L'estimation du coût total des équipements s'élève à 249 788 €, couvrant :

- Le renouvellement du parc informatique avec 85 PC Lenovo ThinkPad X1 Carbon, accompagnés d'écrans Dell UltraSharp, webcams et casques pour optimiser le télétravail.
- L'infrastructure réseau, incluant switchs, routeurs, points d'accès Wi-Fi Ubiquiti et baies de brassage, garantissant une connectivité optimale.
- Les équipements de sécurité et de confort, tels qu'un onduleur APC, une climatisation dédiée à la salle serveur, ainsi qu'une mise à la terre pour assurer la stabilité électrique des installations.
- Les licences logicielles, notamment Windows et Microsoft Office, indispensables au bon fonctionnement des postes de travail.

Un abonnement à la fibre Orange ainsi que des coûts d'entretien ont également été intégrés dans l'estimation. Ce budget vise à garantir un environnement de travail performant, sécurisé et évolutif, répondant aux besoins de l'entreprise et de ses collaborateurs.