Projet Carnofluxe

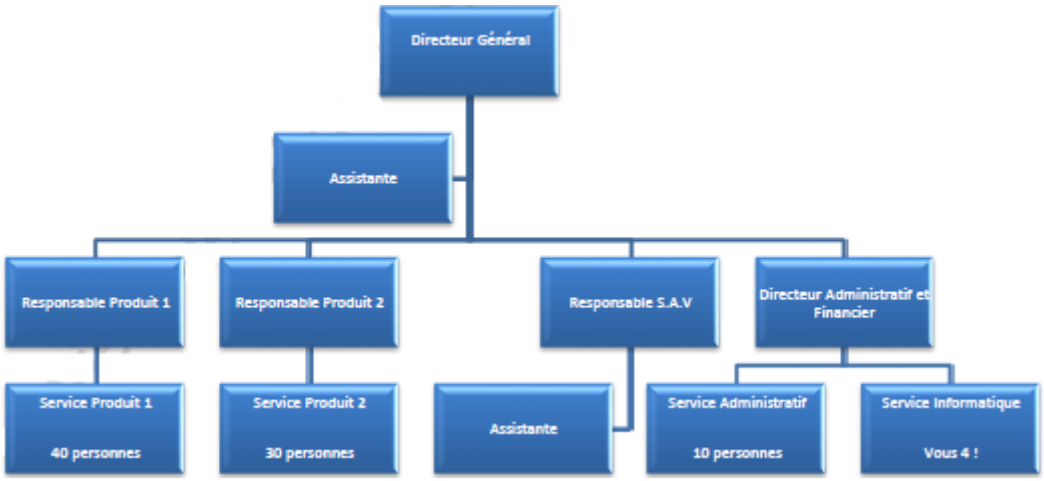
Contexte du projet
Architecture physique et logique
Déploiement réseau
Emplacement de l'infrastructure
La sécurité
Clonage et déploiement des systèmes

Groupe 3 :

Chef de projet : Bruno DOUCET
Alexandre TAVERNIER
Anthony TRESSARD
Kerim YASAR

Contexte du projet :

Nous faisons partie du service informatique de l'entreprise Carnofluxe, chargé de fournir une logistique d'approvisionnement optimisé. L'entreprise vient d'acquérir un nouveau site pour ses 91 employés et il faut faire une nouvelle architecture réseau afin de répondre aux attentes de l'entreprise.



Les services auront besoin de machines clientes en Windows 7 sauf le service produit 2 qui utilisent un système GNU/Linux. Nous devons fournir une maquette avec ces systèmes d'exploitation, les configurations Linux devront être faites via les fichiers de configuration.

Les deux maquettes seront sur un même sous-réseau IP. On doit pouvoir effectuer un Ping (envoi d'un message) entre eux. La configuration TCP/IP doit être statique et non pas en DHCP.

Nous devons fournir une solution de clonage de disque exécutable depuis un média bootable (image iso, liveCD). On doit également rédiger une procédure de clonage et de déploiement. On doit réaliser un plan physique du câblage des bâtiments.

Le dossier de câblage physique doit indiquer :

- L'emplacement, la longueur et le type du câblage. Le passage des câbles devra être apparent sur les schémas.
- Votre plan ne devra pas indiquer l'emplacement exact des prises dans la salle. En revanche, le câblage des bureaux est à prendre en compte dans les calculs
- Les calculs permettant d'avoir à commander la longueur de câble la plus proche possible de la réalité.
- Les emplacements des locaux techniques et des équipements
- Les matériels/accessoires annexes permettant le passage et le brassage des câbles
- Un argumentaire sur le choix du/des supports, leurs caractéristiques techniques, les concepts scientifiques sur lesquels reposent ces technologies, les avantages et limites et enfin les normes respectées.
- Les mises à la terre
- Les emplacements des différents services
- Evaluer le coût de votre solution, devis à l'appui

Nous devons proposer une topologie logique permettant de relier les réseaux des trois bâtiments.

On doit préparer le plan d'adressage du réseau.

Le plan devra indiquer :

- Le nombre de sous réseaux (utiliser la technique VLSM)
- Identification de chaque sous-réseau avec les adresses de réseau, masques de sous-réseaux, de diffusion ainsi que la plage utilisable

On aura le choix et le placement des commutateurs ainsi que leurs configurations de base.

Ces équipements devront pouvoir être administrés à distance. On a besoin d'une maquette de notre solution. Les aspects concernant la sécurité doivent aussi être abordés**.**

Pour les commutateurs aussi nous devons proposer une architecture pour la connectivité sans-fil.

On doit proposer une maquette de l'infrastructure proposée ainsi qu'une représentation de la couverture du Wi-Fi dans les bâtiments.

Architecture physique et logique :

L'entreprise à acheter trois bâtiments, il faut donc savoir comment on peut les relier et comment on peut mettre en place une architecture à l'intérieur des bâtiments afin d'avoir accès au réseau. Nous sommes donc partis sur une topologie en arbre pour les bâtiments car il permet de centraliser le réseau et de créer des nouvelles branches si le réseau a besoin d'être étendu. Comme nous devons prendre en compte une extension possible de l'entreprise et donc la possibilité de rajouter facilement des postes au réseau internet de l'entreprise. L'utilisation de la topologie arbre permet d'ajouter facilement et rapidement un commutateur afin de créer des places supplémentaires dans le réseau.

Maintenant que l'on a choisi une topologie qui va permettre de communiquer au sein d'un même bâtiment, il faut relier les trois bâtiments au point de présence afin qu'ils puissent accéder à internet. On veut pouvoir relier les bâtiments afin qu'ils puissent communiquer rapidement avec internet afin d'obtenir les meilleures performances possibles pour l'entreprise. Notre choix c'est donc porter sur la fibre optique. On s'est orienté vers une topologie qui prend en compte la fibre optique et nous sommes arrivés à la conclusion que pour relier les bâtiments le FDDI (Fiber Distributed Data Interface). Il s'agit d'une topologie anneau reliée par fibre jusqu'au pop (point de présence ou internet arrive dans le bâtiment). Le FDDI est un anneau à jeton à détection et correction d'erreurs (c'est là que l'anneau secondaire prend son importance). Le jeton circule entre les machines à une vitesse très élevée dû à la connexion par fibre optique. Si celui-ci n'arrive pas au bout d'un certain délai, la machine considère qu'il y a eu une erreur sur le réseau.

Cela va donc permettre une connexion rapide entre les bâtiments avec un contrôle des données envoyées grâce aux tokens.

Déploiement réseau :

Nous avons des composants à disposition mais ils ne sont pas adaptés aux nouvelles technologies disponibles ainsi qu'à l'utilisation que l'on veut en faire. Ils ne permettent pas un débit suffisant pour une entreprise de grande catégorie ainsi que la limitation à 5 ports sur le commutateur n'est pas suffisant pour accueillir 91 utilisateurs.

Le commutateur ou switch est un matériel réseau permettant de relier plusieurs équipements entre eux. Il possède différents ports RJ45 femelles permettant de relier plusieurs équipements grâce à des paires torsadées. Il s'agit d'un équipement réseau agissant sur la 2ème couche du modèle OSI en utilisant les trames pour faire circuler des informations entre différents équipements.

Dans chaque switch on retrouve une base de données appelée table MAC (Medium-Access-Control), permettant de faire le lien entre les ports physiques (E0, E1, E2…) et les adresses MAC qui arrivent sur les ports.

Nous avons donc fait des recherches afin de trouver des nouveaux composants cette fois-ci adapter à notre utilisation.

Le commutateur choisi est CISCO Ethernet Cisco SF200-24P géré c'est-à-dire que l'on peut le configurer depuis internet.

Ce qui le rend donc compatible avec nos demandes.

VOICI SES CARACTERISTIQUES :	
ADMINISTRATION	Depuis internet.
PROTOCOLE DE GESTION A DISTANCE	RMON, http, TFTP.
TYPE DE CABLE	100 BASE-T, 1000BASE-TX.
MODE DE COMMUNICATION	Utilisation du full duplex.
CAPACITE DE COMMUTATION	8.8 Gbit/s.
TAILLE DE LA TABLE MAC	8K d'adresses.
DEBIT	6.5 mpps.
MEMOIRE FLASH	16Mo.
PRIX	350€

La deuxième chose à regarder est le type de câble. Nous avons à disposition des câbles de catégorie 4, ils sont vraiment vieux et bien moins performant que les nouveaux câbles. On a décidé d'utiliser un câble RJ45 catégorie 6 à la place du câble RJ45 catégorie 4 car il offre une plus grande bande passante et un débit binaire plus important.

Ce type de câble est compatible avec le switch que nous avons choisie et nous avons pris un câble blindé afin de limiter les phénomènes d'interférences notamment avec le Wi-Fi.
En ce qui concerne ses caractéristiques techniques, le cable RJ-45 Catégorie 6 a une bande passante de 250MHz.
Il utilise des paires torsadées blindées afin de limiter les interférences avec le Wi-Fi.
Composé de 4 paires torsadées dans une gaine en PVC. Son prix est de 1.67€ le mètre.

Maintenant que l'on a le réseau filaire il nous faut celui non filaire c'est-à-dire le Wi-FI Comme il n'y a pas de composant déjà présent il va falloir en trouver des nouveaux qui puissent répondre aux attentes éxigées.

La premiere chose est un routeur qui va permettre de recuperer le réseau internet au point de présence. Comment fonctionne un routeur ?

Un routeur est un élément permettant l'intermédiaire de deux réseaux. Il assure le routage de paquets entre réseaux indépendants. Ce routage est réalisé selon un ensemble de règles formant la table de routage. C'est un équipement de la couche 3 du modèle OSI.

Le routeur traite les adresses IP en fonction de leur adresse réseau définie par le masque de sous réseaux et les redirige selon l'algorithme de routage et sa table associée.

Celui que l'on a choisi est un routeur ASUS 4G-N12 qui est à seulement 109 euros. Il est en Wi-Fi N et il peut délivrer jusqu'à 300 Mb/s. Il a des ports Ethernets. C'est un modem intégré.

Notre choix s'est porté sur celui la parce que :

- Son prix est très convenable.
- Il délivre un débit amplement suffisant pour 91 personnes.
- Sa portée est suffisamment grande avec 50m

Mais pour pouvoir transférer le réseau dans tous les bâtiments il faut rajouter des points d'accès. Les points d'accès permettent de donner un accès au réseau filaire aux différentes stations avoisinantes équipées de carte Wi-Fi.

Il existe deux modes : mode infrastructure et mode ad hoc.

Le mode infrastructure est un réseau sans fil qui est fondé sur une architecture cellulaire où chaque cellule est contrôlée par un point d'accès le tout formant un réseau appelé ESS. Les points d'accès sont reliés entre eux par des liaisons filaires ou radio. Les utilisateurs doivent s'identifier auprès du réseau afin de pouvoir en bénéficier (SSID). Un point d'accès sur un réseau sans fil est comparable à un concentrateur sur un réseau filaire.

Le mode de communication ad hoc est aussi disponible. Il s'agit d'un mode point à point entre les équipements sans fil. Les machines clientes se connectent les unes aux autres afin de constituer un réseau point à point. Dans ce mode chaque machine joue en même temps le rôle de client et le rôle de point d'accès.

Mais dans notre cas la borne va être en mode infrastructure car notre but est de faire communiquer les machines à internet. C'est un point d'accès ASUS RP-N12. Il a une externe qui améliore la couverture et la qualité du signal Wi-Fi. Il a une installation facile et rapide en appuyant sur un seul bouton. Il y a un indicateur de signal à LED qui aide à trouver le meilleur signal Wi-Fi pour l'installer idéalement.

Notre choix s'est porté sur ce point d'accès parce que :

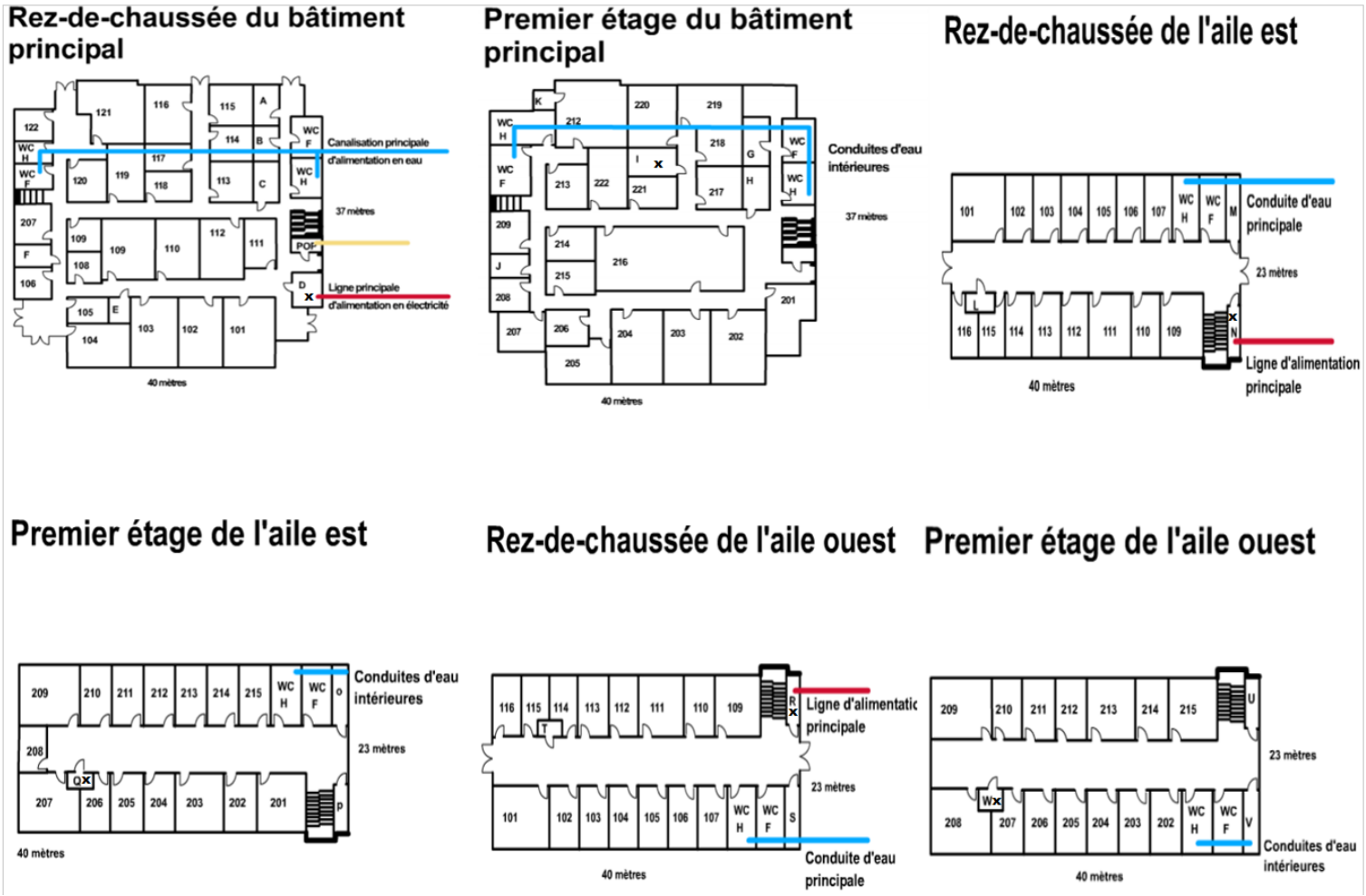
- Son prix est très convenable seulement 30 euros.
- Il utilise une norme Wi-Fi N tout comme le routeur
- Son taux de transfert est de 300 Mb/s ce qui correspond au débit du routeur.

Emplacement de l'infrastructure :

Une fois que l'on sait ce qu'il faut comme composant pour effectuer le réseau il faut une zone pour le stocker.
On a donc plusieurs choix pour les emplacements en fonction des étages. Après analyse des normes on a réussi à synthétiser des paramètres qui vont ensuite pouvoir nous orienter dans le choix du local.

Les voici :
Les murs du local technique doivent avoir de la peinture ignifuger afin d'éviter la propagation des incendies et la pièce doit avoir un plafond non suspendu.
Il doit y avoir au moins deux prises de courants sur un circuit séparer pour éviter de faire disjoncter le réseau principal.
Pas d'éclairage fluorescent car il peut provoquer des interférences avec les câbles cuivre.
Et enfin la porte doit s'ouvrir vers l'extérieur pour des normes de sécurité où l'on doit pousser la porte pour sortir et elle doit posséder un verrou afin de la sécuriser des intrusions.
Comme il y a du matériel qui peut chauffer il faut ajouter un détecteur de fumée, un thermomètre et une climatisation pour refroidir la pièce lors des grandes chaleurs. Et bien sûr il faut un extincteur dans chaque salle.

Maintenant que l'on sait ce que l'on doit avoir dans nos pièces on peut choisir la salle qui possède les caractéristiques pré requises. Voici le plan final, nous allons voir les détails pour chaque salle.



Les salles sont marquées d'une croix mais on va quand même préciser le nom de chaque salle.
Pour le Rez-de-chaussée la salle D a été choisie car elle possède en emplacement proche du point de présence, une lumière incandescente, de la peinture ignifuger, l'alimentation électrique principale ainsi qu'un plafond non suspendu et une porte avec un verrou et qui s'ouvre vers l'extérieur.

Pour le premier étage du bâtiment principale il s'agit de la salle I car elle aussi répond aux normes que nous avons fixé plus haut. La différence est qu'elle possède six prises de courant au lieu de l'alimentation principale.

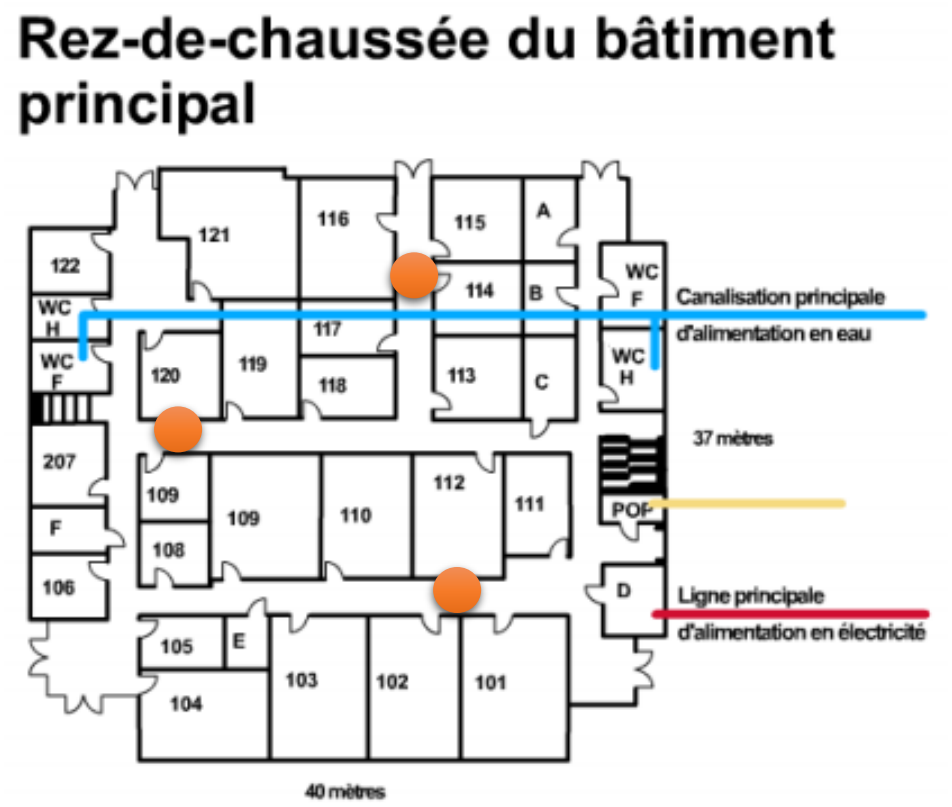
En ce qui concerne le rez-de-chaussée de l'aile est, c'est la pièce N qui a été choisie car c'est à cette endroit que la ligne de courant arrive dans le bâtiment et que la pièce répond elle aussi aux normes.

Le premier étage de l'aile est, c'est la salle a Q a été retenue même si elle est plus petite que les autres. Car les autres pièces n'étaient pas aux normes, on peut bien sûr modifier les autres pièces pour les mettre conforme aux normes. Par exemple pour la salle P il faut changer le type d'éclairage.

Changeons de bâtiment, pour le rez-de-chaussée de l'aile ouest, la salle R a été choisie car elle possède en plus d'être aux normes elle possède la ligne d'alimentation principale.

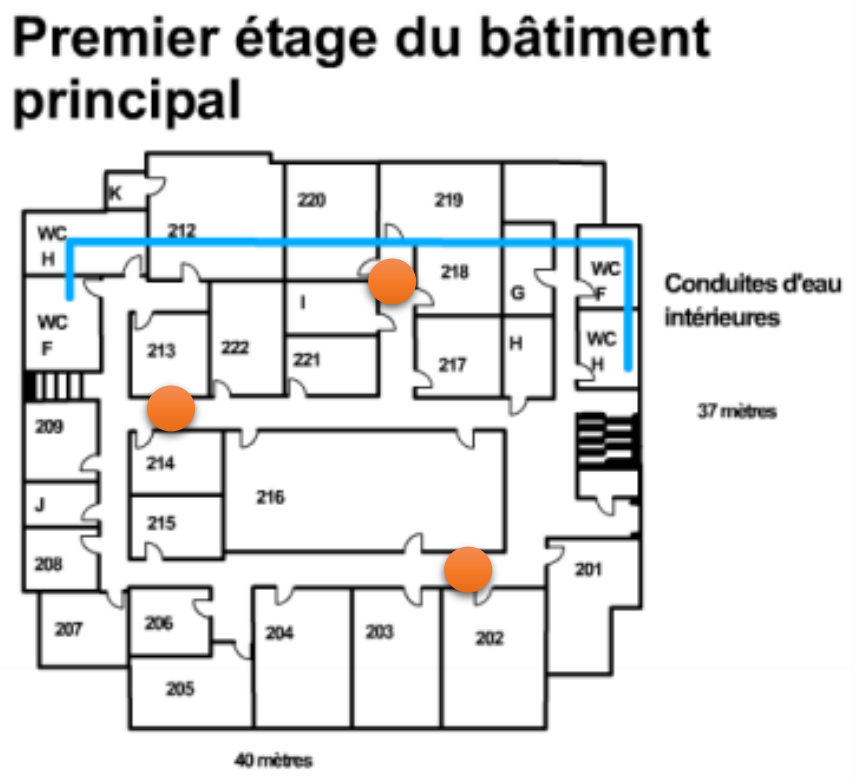
Et enfin pour le premier étage de l'aile ouest on a la salle W car elle respecte aussi les normes mais elle est petite. On peut donc faire comme pour le premier étage de l'aile est, c'est-à-dire modifier la salle U pour la mettre aux normes en changeant le type d'éclairage.

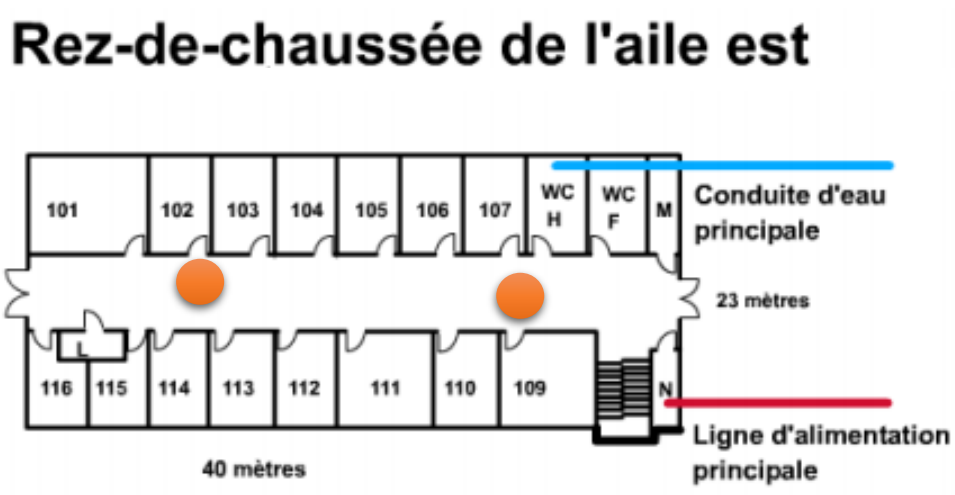
Une fois la salle choisie, on peut commencer à faire passer les câbles et à mettre les points d'accès dans les bâtiments.



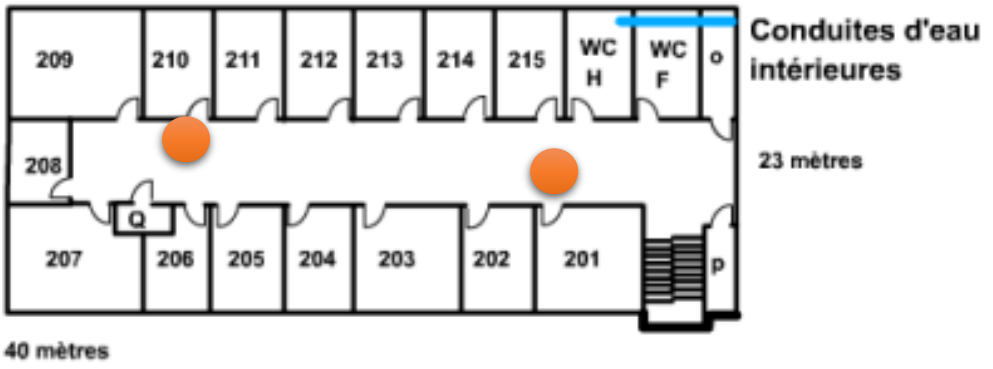
Pour le bâtiment principal au rez-de-chaussée et à l'étage la disposition des bornes Wi-Fi va être la même. On a choisi une disposition en triangle pour couvrir un maximum de place et si une borne tombe en panne les utilisateurs du réseau Wifi pourront toujours se connecter sur les autres bornes.

Les points orange représentent les points d'accès Wifi qui sont ensuite relier a des commutateurs dans les salles de stockage pour être enfin connecter au routeur principal qui sert de modem internet pour accéder à internet.

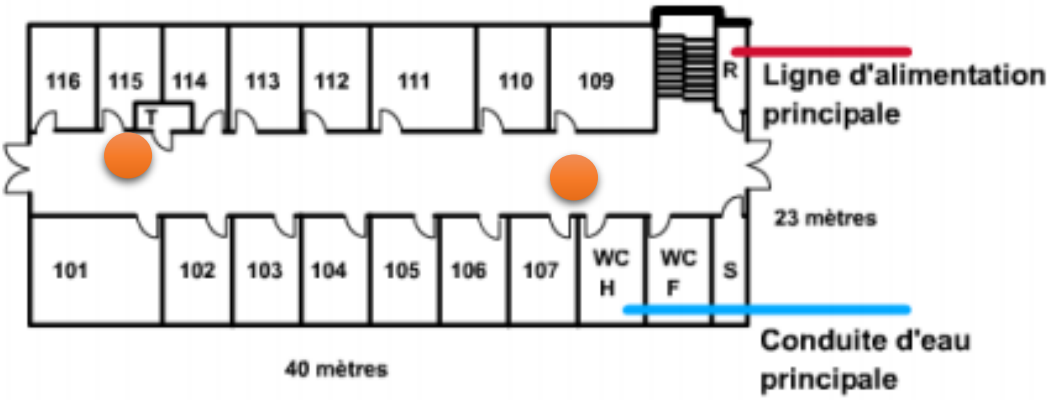




Premier étage de l'aile est

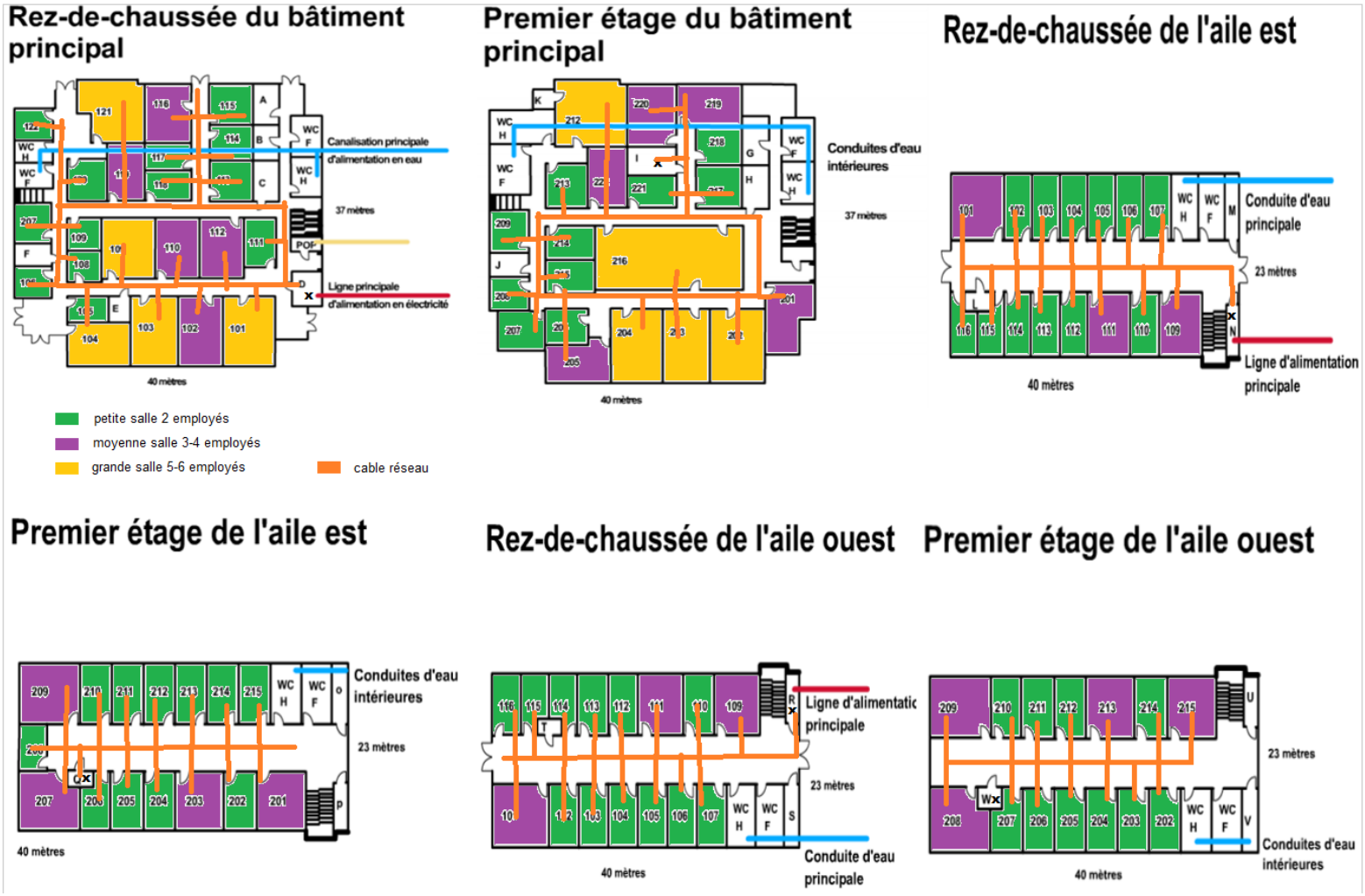


Rez-de-chaussée de l'aile ouest



Premier étage de l'aile ouest

Nous allons ensuite disposer les câbles RJ45 dans le bâtiment pour qu'ils puissent connecter toutes les salles. La première chose est donc de mesurer les salles pour ensuite calculer la distance exacte pour les câbles.



Les salles ont été colorer en en fonction de la taille des salles et du nombre d'employés qu'elle peut contenir. En fonction des normes sur le nombre de personne que l'on peut avoir par pièce on a fait des zones.

La sécurité :

Lorsque l'on met en place un système réseau il faut prendre en compte la sécurité. C'est-à-dire comment on peut faire pour sécuriser un réseau et éviter que des personnes non autoriser y accède.

La première chose est de verrouiller physiquement la salle où l'on range les appareils réseau. Cela va permettre d'éviter que l'on touche à l'infrastructure et le branchement des commutateurs, ou qu'une personne ce branche au port console et puisse administrer le réseau alors qu'il n'est pas autorisé à le faire.

Il existe différentes manières de contourner la sécurité d'un commutateur :

→S'approprier l'adresse MAC d'un ordinateur connecté au commutateur et l'utiliser afin d'espionner les autres ordinateurs.

→*Mac flooding*, consiste à surcharger le commutateur avec des milliers d'adresse MAC. Le commutateur tombe alors dans un failopen et envoie les trames vers les différents postes du réseau.

Il faut donc trouver des solutions pour éviter ces problèmes.

Sécurisation manuelle de l'accès :

Il consiste à attribuer une adresse MAC d'un ordinateur à un ports du commutateur en particulier. Ainsi tout autre ordinateurs voulant se connecter à ce même port aura son accès refusé.

```
Switch>enable
Switch#Configure terminal
Switch(config)#interface FastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address xxxx.xxxx.xxxx
```

Sécurisation automatique de l'accès:

C'est le 1er ordinateur qui envoie une trame sur le port du switch qui bloque l'accès du port. Il devient en quelque sorte le propriétaire du port et personne d'autre à part lui peu se connecter sur celui-ci.

Tant que l'ordinateur connecté n'envoie pas de trame, le port n'enregistre pas son d'adresse MAC.

```
Switch>enable
Switch#Configure terminal
Switch(config)#interface FastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky
```

Configurer la réaction d'un commutateur face à une violation de sécurité :

Lors d'une violation de la sécurité un commutateur peut réagir avec la commande « switchport port-security violation » qui possède 3 options différentes :

→ « shutdown », le commutateur désactive l'accès au port lorsqu'il y a violation.

→ « protect », toutes les trames ayant des adresses MAC inconnues sont bloquées et les autres sont autorisées.

→ « restrict », une alerte SNMP est envoyé et le compteur de violation est incrémenté. SNMP est un protocole réseau permettant aux utilisateurs de gérer les équipements réseaux et de diagnostiquer et superviser les problèmes réseaux.

```
Switch>enable
Switch#Configure terminal
Switch(config)#interface FastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security violation nom_methode
```

Augmenter les nombres d'adresses MAC autorisées :

Il est possible d'augmenter le nombre maximum d'adresses MAC autorisées sur un port à l'aide la commande :

```
switchport port-security
maximum x
```

Il est aussi possible de mettre un mot de passe sur le commutateur afin de limiter l'accès à sa configuration avec la commande passeword.

Et enfin lorsque l'on installe un réseau sans fil généralement nous le sécurisons aussi car installer un réseau sans fil sans le sécuriser peut permettre à des personnes non autorisées d'écouter et de modifier l'accéder à ce réseau. Il est donc primordial de sécuriser les réseaux sans fil dès leur installation. Il existe plusieurs moyens de sécuriser son réseau de façon plus ou moins forte selon les ressources et leur importance.

Nous pouvons par exemple changer les mots de passe par défaut comme par exemple celui de l'administrateur, modifier la configuration par défaut, désactiver les services disponibles non utilisés ou régler la puissance d'émission du point d'accès au minimum nécessaire.

Il faut faire les mises à jour dès que celle-ci sont possibles. Nous pouvons aussi changer le SSID par défaut car il est plus judicieux de ne pas choisir un SSID attractif.

Pour sécuriser correctement les données qui transitent sur un réseau on peut y ajouter un chiffrement. L'absence de chiffrement dans un réseau sans fil laisse l'ensemble des données qui transitent sur ce réseau à la merci d'une personne munie d'une carte Wi-Fi.

Le protocole initialement proposé pour le chiffrement des communications entre éléments d'un réseau sans fil est le WEP. Ce protocole WEP utilise une clé d'une longueur de 64 à 256 bits dont 24 ne sont pas utilisés pour le chiffrement. Cela fait une clé, si on la compare à un mot, d'une longueur de 5 à 29 caractères. La majorité des clés sont composées de 13 caractères. L'algorithme utilisé dans le chiffrement possède une grande faiblesse qui est exploitée. Le WEP est rapidement incapable d'offrir un niveau de sécurité suffisant pour la plupart des utilisateurs car il est possible en surveillant

une quantité de trafic suffisante de casser une clef WEP en seulement quelques secondes. De plus, le chiffrement WEP introduit des problèmes de gestion de clefs qui dégradent rapidement la sécurité du réseau.

Le protocole WPA offre une protection d'un niveau bien supérieur à WEP. Il utilise le même algorithme de chiffrement et est basé sur le même principe. En revanche le TKIP (Temporal Key Integrity Protocol ou Protocole d'intégrité par clé temporelle) a été ajouté, permettant ainsi une permutation plus importante des clés sans que le vecteur d'initialisation ne puisse être reconstitué de manière utile. Le protocole WPA2 quant à lui utilise un algorithme de chiffrement beaucoup plus puissant, utilisé dans le cryptage des documents sensibles et possédant une clé très forte. Il s'agit de la dernière norme du protocole WPA permettant de protéger votre réseau WLAN.

Clonage et déploiement des systèmes :

Maintenant que le réseau est sécurisé il faut ajouter les machines sur le réseau.
Pour faire cela nous avons adressé une plage d'adresses en fonction des services présents dans l'entreprise.

Pour l'instant l'entreprise comporte 91 salariés mais veut pouvoir s'étendre et rajouter des postes ainsi que des serveurs sur le réseau.
Comme il s'agit d'une entreprise de taille moyenne nous sommes partis sur un réseau priver de classe C mais un peu modifier.
C'est-à-dire que nous avons changé le masque de sous-réseau afin de rajouter des adresses pour mieux les attribuer en fonction des différents services. On est parti d'une adresse en 192.168.0.0 avec un masque réseau de 255.255.255.255.0 et on a modifié le masque de réseau afin d'avoir plus de réseau disponible. Ce qui nous a donné un masque réseau de 255.255.248.0

Voici le plan d'adressage :

Attribution Réseau	Masque Réseau	Début de la plage	Fin de la plage
192.168.0.0	/21	192.168.0.1	192.168.0.254
192.168.1.0	/21	192.168.1.1	192.168.1.254
192.168.2.0	/21	192.168.2.1	192.168.2.254
192.168.3.0	/21	192.168.3.1	192.168.3.254
192.168.4.0	/21	192.168.4.1	192.168.4.254
192.168.5.0	/21	192.168.5.1	192.168.5.254
192.168.6.0	/21	192.168.6.1	192.168.6.254

Maintenant que l'on a des adresses disponibles on peut les donner pour chaque service de l'entreprise

192.168.0.0 va être le réseau de la direction.
192.168.1.0 serra le réseau du service produit 1.
192.168.2.0 pour réseau du service produit 2. Fonctionne sous Linux
192.168.3.0 pour le réseau administratif.
192.168.4.0 qui va servir au réseau du SAV.
192.168.5.0 pour le réseau du service informatique.
192.168.6.0 comme réseau supplémentaire pour des serveurs.

La dernière chose à prendre en compte pour les adresses IP est qu'elles doivent être choisi en statique et surtout en fonction du service auquel appartient l'ordinateur.

Pour savoir exactement comment déployer une machine nous avons fait un fichier annexe qui se nomme : « Procédure technique Configurations des postes clients »
Cela va permettre de savoir comment mettre en place une machine le plus efficacement possible et lui attribuer une adresse peu importe le type de système le service a besoin.

Si un commutateur tombe en panne il faut être capable de le remplacer et de reconfigurer le nouveau commutateur. Cependant au lieu de reconfigurer le switch depuis le début il existe une méthode beaucoup plus simple.

En effet, il est possible de configurer un routeur et de sauvegarder sa configuration afin de la mettre sur les autres switches sans les faire un par un.

Pour cela on a besoin de mettre en place un server TFTP (Trivial File Transfert Protocol). Et il faut aussi assurer la connexion entre le serveur et les différents switches.

Pour cela il faut :

→1) A l'invite du commutateur, rentrer la commande « ***enable*** » afin de passer en mode privilégié.

→2)Copier la configuration en cours sur le serveur TFTP grâce à la commande en mode privilégié « ***copy running-config tftp :*** »

→3) Ouvrir la configuration du switch avec un traitement de texte et supprimer toutes les lignes commencent par « AAA ».

Il s'agit de commande de sécurité pouvant interdire l'accès au switch.

→On peut maintenant copier le fichier de configuration du serveur TFTP au deuxième switch. Il faut se mettre en configuration privilégié et utiliser la commande « ***copy tftp : running-config*** ».

C'est une solution rapide qui permet d'avoir une trace des configurations des switch et donc de pouvoir comme pour les machines réattribuer rapidement une configuration.

Planning :

Pour mettre en place tout le système on va commencer par faire tous les raccordements électriques, afin de pouvoir installer ensuite les infrastructures réseau.

Il faut prendre en compte les tests, c'est-à-dire que dès qu'une pièce va être raccorder au réseau il va falloir qu'ils testent les prises afin de pouvoir dire que tous les branchements sont bons. Cela va permettre d'avoir un suivi de la mise en place du système.

Dès que toutes les pièces sont raccordées au réseau de l'entreprise il faut faire un dernier teste pour vérifier si toutes les pièces sont toujours connectées. Celui-ci va durer environ 2 mois.

Et enfin, ils vont installer tous les ordinateurs dans leurs salles respectives, puis ils vont installer le système d'exploitation et adresser l'adresse IP qui correspond à leurs services en fonction de la procédure qui a été choisi. Cela va prendre environ 1 semaine pour l'installation.

Puis, pour assurer le bon fonctionnement du réseau sur une longue durée on peut effectuer un suivi du réseau en faisait des maintenances et vérifier si tous le réseau fonctionne.

Conclusion :

La mise en place d'une architecture réseau prend en compte beaucoup de paramètre.
La première chose à faire est de trouver une architecture réseau qui répond aux attentes du contrat. Dans notre cas, il fallait une architecture qui puisse être étendue facilement dans le but de rajouter des nouvelles machines pour une future extension.

Maintenant que l'on sait sur quel type d'architecture on va travailler il faut savoir ou placer les composants et les câbles. Il faut calculer la distance parcourue par les câbles afin de pouvoir acheter la bonne distance de câble. Dans notre cas, nous avons 10km800 de câble réseau RJ 45 pour relier l'infrastructure des bâtiments et entre les trois bâtiments nous avons 180 mètres de câble de type fibre optique pour relier les commutateurs entre les bâtiments et les commutateurs principaux.
De même que la mise à terre qui permet d'avoir une sécurité supplémentaire pour le réseau électrique.

Les plages d'adressage citer plus haut permettent de modifier le réseau pour prévoir une expansion du réseau de l'entreprise en prenant des plages qui peuvent contenir 254 utilisateurs.

Lorsque l'on met en place un réseau il faut prendre en compte aussi tous les composants qui ne sont pas présents, c'est-à-dire que l'on va cloner des licences pour les machines mais il faut posséder ces licences sinon l'entreprise peut avoir des problèmes judiciaires. Pareil pour les logiciels de traitement de texte, il faut que l'entreprise possède le nombre suffisant de licences.

Tout ceci est à prendre en compte lorsque l'on veut mettre en place un réseau informatique. Au même niveau que le type de topologie ou le type de câble.

Le projet a donc été fini dans les temps et il répond aux attentes exigées par l'entreprise.