# Table des matières :

Table des matières :.....1
1.Spanning Tree Protocol.....2
2.Redondance de cartes réseaux.....4
3.Audit du réseau informatique – Cartographie réseau.....6
4.Annexes.....7

# Avant-Propos

# 1. Analyse des criticités des risques :

Pour effectuer un plan de reprise d'activité, plus précisément, j'ai listé un certain nombre d'incidents possibles avec une solution de correction au problème. Pour déterminer les incidents les plus risqués, j'ai effectué un tableau sur la criticité des risques.

J'ai fini la semaine par déterminer la criticité des risques dans le secteur informatique. Ça consiste à déterminer le risque mineur ou critique d'un incident dans l'entreprise. À l'aide du tableur excel, pour déterminer le taux de risque, on compare 3 critères qui sont la gravité (danger), la fréquence du scénario (jamais, rare ou souvent) et la détectabilité de l'incident.

Chaque critère dispose de 4 niveaux du plus tolérant au plus urgent à traiter.

| Gravité des risques | Définitions des termes |
|---|---|
| 4 = Critique | Risque pouvant avoir de graves conséquences sur le réseau |
| 3 = Sérieux | Risque pouvant avoir des conséquences minimes sur le réseau |
| 2 = Moyen | Le résultat de la mesure n'a pas systématiquement de conséquence sur le réseau |
| 1 = Faible | Le résultat de la mesure n'a aucune conséquence sur le réseau puisque des mesures préventives ou des étapes ultérieures permettent d'éviter le danger |

| La Fréquence | |
|---|---|
| 4 = Critique | Défaut très fréquent |
| 3 = Sérieux | Défaut rencontré deux à trois fois dans l'année |
| 2 = Moyen | Défaut très rare mais déjà rencontré dans l'entreprise |
| 1 = Faible | Défaut jamais rencontré dans l'entreprise |

| La Détectabilité | |
|---|---|
| 4 = Critique | Faible probabilité de détecter le défaut |
| 3 = Sérieux | Défaut difficile à détecter |
| 2 = Moyen | Grande probabilité de détecter le défaut mais des oublies peuvent subsister |
| 1 = Faible | Défaut très facilement détectable |

Pour évaluer la criticité du risque, on multiplie les 3 critères et on tient compte du résultat suivant :

- Criticité du risque compris entre 1 et 11 : risque mineur

- Criticité du risque supérieur ou égale à 12 : risque critique.

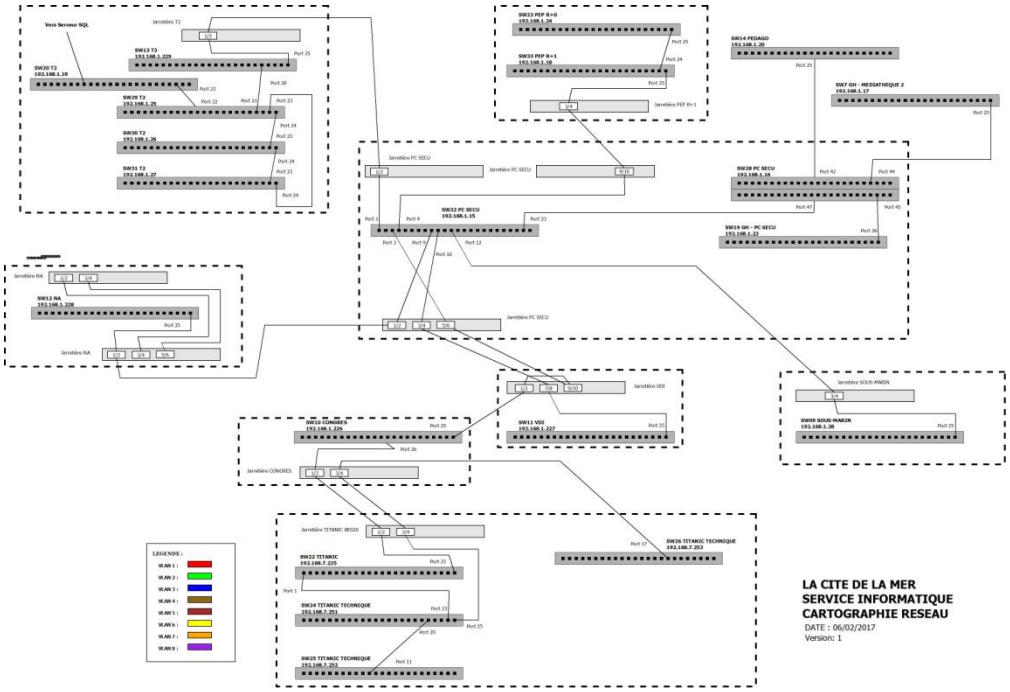
Résultat du tableau :

| *Type* | *Événement* | *La Gravité* | *La Frequence (Probabilité)* | *La Détectabilité* | La criticité des risques | Risque mineur<br>Risque critique |
|---|---|---|---|---|---|---|
| Absence accidentelle de personnel | Absence de personnel informatique | 4 | 1 | 1 | 4 | Risque mineur |
| Absence ou indisponibilité accidentelle de service | Absence de service : Climatisation | 2 | 2 | 4 | 16 | Risque critique |
| | Absence de service : Énergie | 4 | 3 | 1 | 12 | Risque critique |
| | Absence de maintenance applicative ou maintenance applicative impossible | 2 | 2 | 1 | 4 | Risque mineur |
| | Absence de maintenance système ou maintenance système impossible | 2 | 2 | 1 | 4 | Risque mineur |
| Accident grave d'environnement | Foudroiement | 4 | 1 | 3 | 12 | Risque critique |
| | Incendie | 4 | 1 | 3 | 12 | Risque critique |
| | Inondation | 4 | 2 | 3 | 24 | Risque critique |
| Accident matériel | Panne d'équipement | 4 | 3 | 2 | 24 | Risque critique |
| | Panne d'équipement de servitude (alimentation électrique, alimentation en fluide, etc.) | 3 | 3 | 2 | 18 | Risque critique |
| Erreur de conception | Bug bloquant dû à une erreur de conception ou d'écriture de programme (interne) | 2 | 2 | 3 | 12 | Risque critique |
| Erreur matérielle ou de comportement du personnel | Perte ou oubli de document ou de media | 1 | 2 | 2 | 4 | Risque mineur |
| | Erreur de manipulation ou dans le suivi d'une procédure | 2 | 2 | 2 | 8 | Risque mineur |
| | Erreur de saisie ou de frappe | 2 | 2 | 2 | 8 | Risque mineur |
| Incident dû à l'environnement | Dégât dû au vieillissement | 4 | 2 | 3 | 24 | Risque critique |
| | Dégât des eaux | 4 | 1 | 3 | 12 | Risque critique |
| | Dégât dû à la pollution | 4 | 1 | 3 | 12 | Risque critique |
| | Surcharge électrique | 4 | 1 | 2 | 8 | Risque mineur |
| Incident logique ou fonctionnel | Incident d'exploitation | 2 | 2 | 2 | 8 | Risque mineur |
| | Bug bloquant dans un logiciel système ou un progiciel | 4 | 2 | 2 | 16 | Risque critique |
| | Saturation bloquante pour cause externe (ver) | 4 | 2 | 1 | 8 | Risque mineur |
| | Virus | 4 | 2 | 2 | 16 | Risque critique |
| Malveillance menée par voie logique ou fonctionnelle | Attaque en blocage de comptes | 3 | 2 | 3 | 18 | Risque critique |
| | Effacement volontaire ou pollution massive de configurations systèmes | 4 | 2 | 3 | 24 | Risque critique |
| | Effacement volontaire direct de supports logiques ou physiques | 4 | 2 | 3 | 24 | Risque critique |
| | Captation électromagnétique | | | | 0 | Risque mineur |
| | Falsification logique (données ou fonctions) | 2 | 1 | 3 | 6 | Risque mineur |
| | Création de faux (messages ou données) | 2 | 1 | 3 | 6 | Risque mineur |
| | Saturation malveillante d'équipements informatiques ou réseaux | 4 | 2 | 2 | 16 | Risque critique |
| | Destruction logique totale (fichiers et leurs sauvegardes) | 4 | 1 | 2 | 8 | Risque mineur |
| | Détournement logique de fichiers ou données (téléchargement ou copie) | 3 | 1 | 4 | 12 | Risque critique |
| Malveillance menée par voie physique | Manipulation ou falsification matérielle d'équipement | 3 | 1 | 4 | 12 | Risque critique |
| | Vandalisme | 2 | 1 | 3 | 6 | Risque mineur |
| | Vol physique | 3 | 1 | 4 | 12 | Risque critique |

## 2. Analyse de risque d'un plan de continuité d'Activité PCA

Mon Projet consiste à faire un plan du réseau pour estimer les problèmes possible et ensuite d'établir leurs résolutions.

Le plan du réseau actuel :



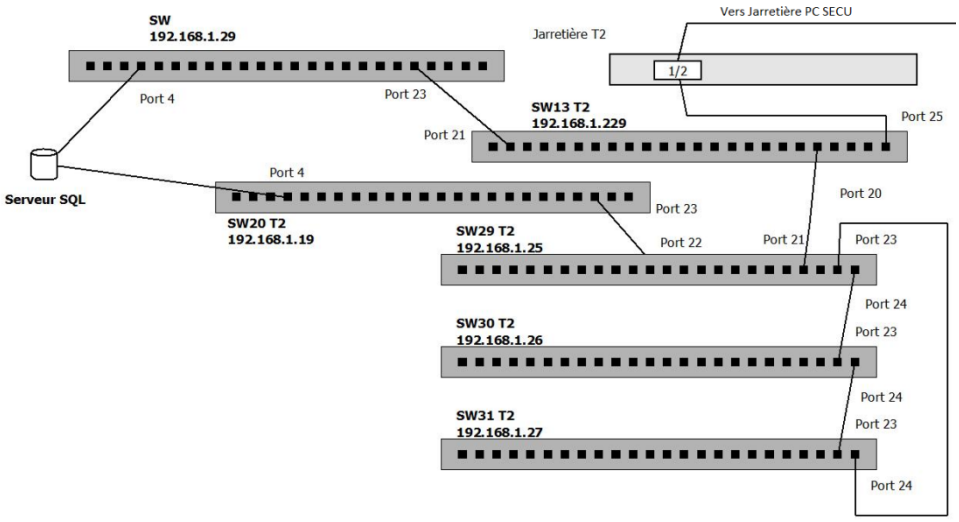

## 1. Problèmes possibles & Solution envisageable :

A l'aide des cartographies réseaux et du tableau de criticité, je vais pouvoir faire la liste des problèmes urgents à corriger ainsi que des propositions pour d'autres problèmes.

1) L'un des problèmes majeurs serait que le switch 20 de la salle serveur (T2) ne soit plus disponible. Différents serveurs sont reliés aux switchs comme le serveur SQL qui sert de base donnée pour la billetterie du musée.

   Pour anticiper le problème, on peut prévoir un second switch (le SW 27) qui serait aussi relié aux différents serveurs comme le serveur SQL. Le Switch continuerait sa route directement à la passerelle, il ne passe pas par le SW 29 pour éviter le cas où c'est le SW29 qui est indisponible. Pour sa mise en marche, la solution d'un système de répartition de charge avec les modes actif et passif est la plus adaptée, les deux switchs devront alors communiquer directement entre eux. Ce système permet dès lors que le switch (SW20) actif tombe, que le switch (SW27) passif prend la suite du service. Les switchs devront disposer du protocole spanning tree. Enfin pour un meilleur débit, la connexion entre les switchs en Fibres est primordiale par rapport à une connexion en Rj45. (il faut vérifier la disponibilité du SFP)

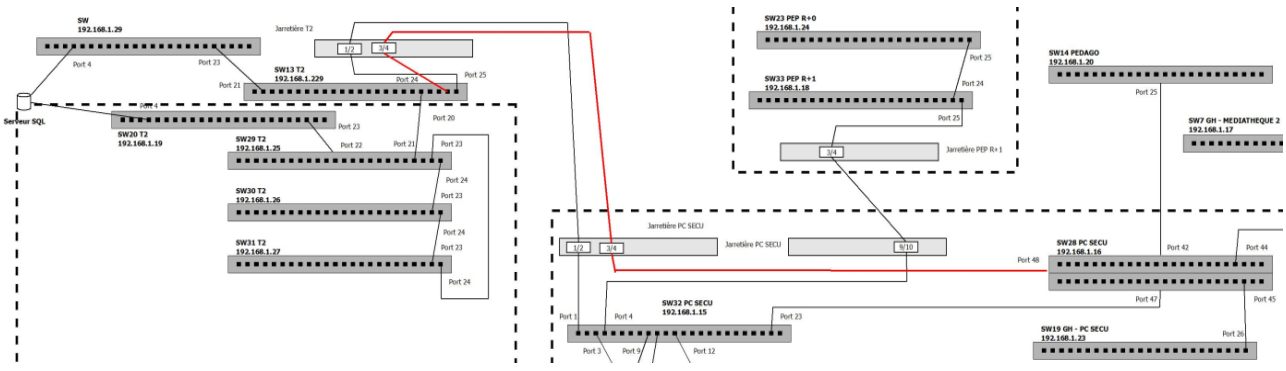
   Voici un plan après solution, le Serveur SQL représente aussi les autres serveurs.




2) Le réseau se compose de différents bâtiments. Le bâtiment principal est le terminal 2 (T2) qui contient la salle serveur pour le lien avec le serveur SQL, la passerelle… Le réseau du terminal 2 est relié au reste du réseau du site par un seul lien fibre. La fibre passe par un réseau de canalisation se trouvant en dessous d'une route et d'un parking. En cas de dégât sur la fibre qui la rendrait indisponible, le reste cite n'aurait plus aucune connexion avec les serveurs. Le site dispose d'une deuxième fibre qui fait l'interconnexion entre le terminal 2 au reste du site. La solution serait de configurer cette 2e fibre qui serait relié au switch 28. Les switchs devront disposer du protocole spanning tree. Enfin, pour un meilleur, la connexion entre les switchs en Fibres est primordiale par rapport à une connexion en Rj45. (il faut vérifier la disponibilité du SFP)

Voici un plan après solution (fil rouge) :

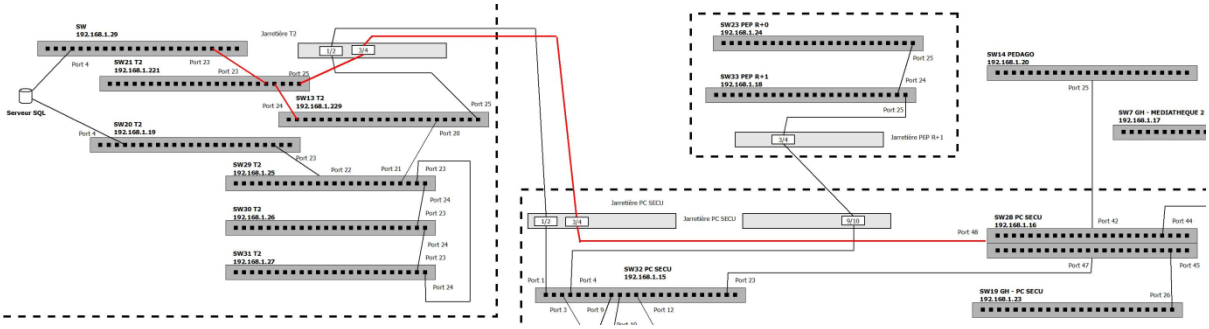
Cela permet aux billetteries de continuer à fonctionner même si les matériels suivants ne sont plus disponibles : SW20, le SW25, la fibre en jarretière 1 / 2 et le SW 32.



3) Un autre problème majeur serait la perte de la passerelle, son indisponibilité aurait des faits négatifs sur l'activité de l'entreprise. La solution qui se pose alors est la mise en place d'une deuxième passerelle. Actuellement une 2e passerelle est disponible, ne restant plus que son installation dans la baie pour sa mise en marche. Avec l'ajout d'une deuxième passerelle, une refonte du plan précédent est à revoir. Les switchs devront disposer du protocole spanning tree. Enfin pour un meilleur débit, la connexion entre les switchs en Fibres est primordiale par rapport à une connexion en Rj45. (il faut vérifier la disponibilité du SFP)

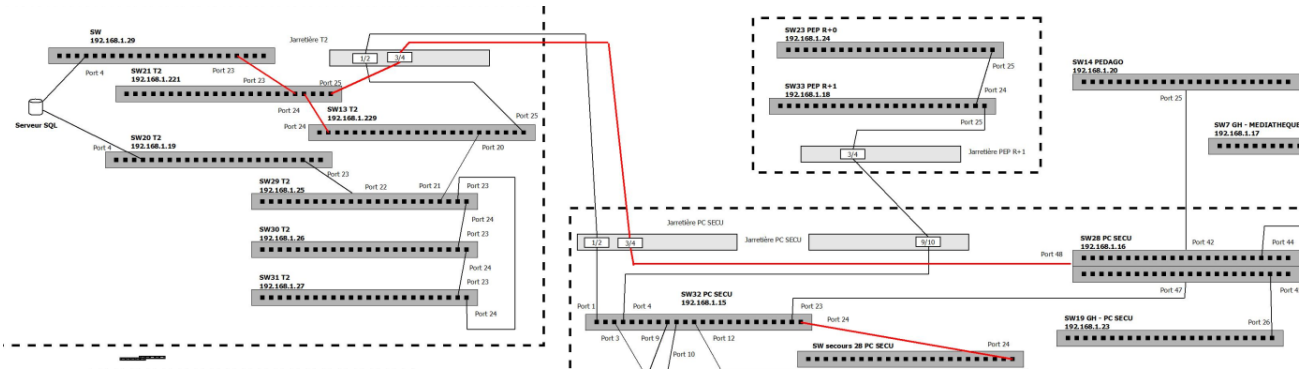
Voici le plan complet des 3 dernière solution :

Avec ce plan, on voit que la 2eme passerelle (SW21) fait le lien entre le SW 27, la 1ère passerelle (SW13) et enfin vers la jarretière en fibre 3/4




4) La tolérance de panne continue par la mise en place d'un switch de redondance pour le SW28. Le switch sera relié au SW32 et utilisé seulement si le SW28 tombe en panne. Dans ce cas-là, il faut préciser qu'une intervention physique devra être nécessaire pour intervertir les branchements entre SW28 et le nouveau switch.

Voilà le plan de la solution final :



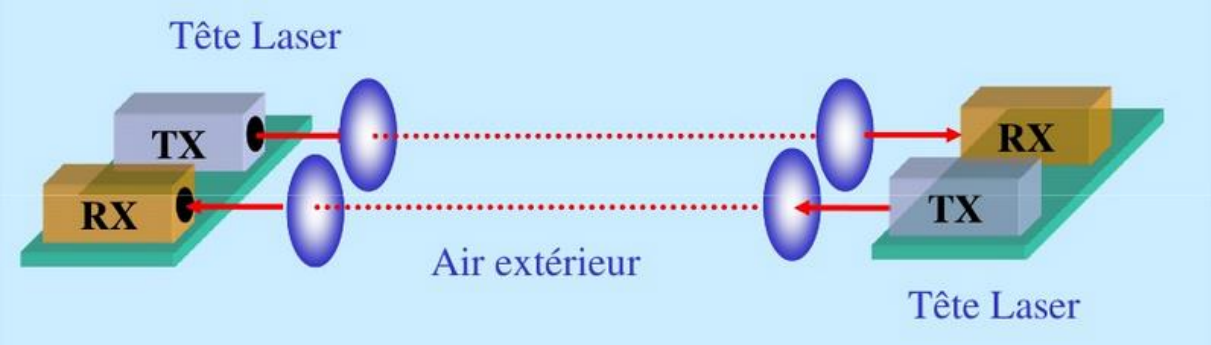

5) Comme dit dans le 2eme problème « La fibre passe par un réseau de canalisation se trouvant en dessous d'une route et d'un parking. » Les deux fibres se trouvent dans la même canalisation, si un incident arrive sur la canalisation, le bâtiment T2 n'aura plus aucune connexion avec le site. Il faut alors proposer un système pour que l'interconnexion entre les bâtiments reste disponible. De plus un système non canalisé pour éviter de perdre le système de base et le système de secours de la même manière.

Pour choisir la bonne technologie, voici les différents paramètres recommandé :

- Une bande passante avec débit correcte
- Une distance de liaison assez longue
- Sécurité des données à transférer
- Qualité du Service

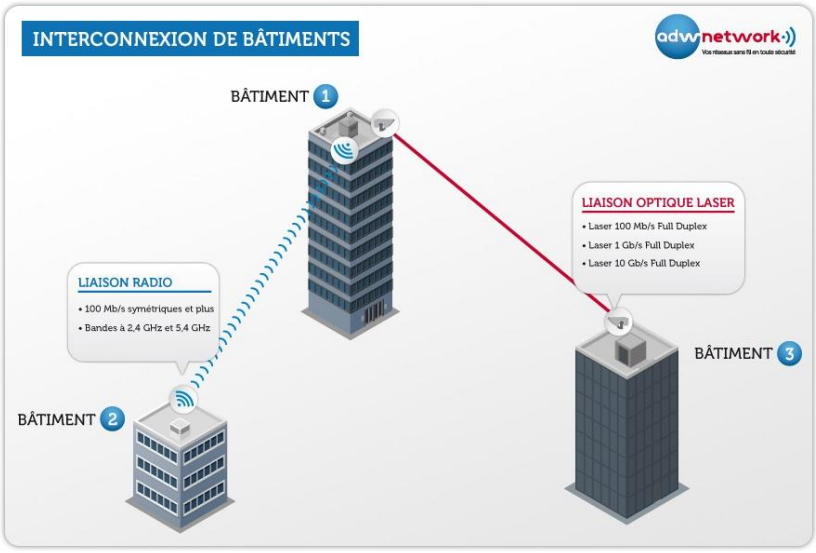
Apres de nombreuses recherches, deux solutions avec des avantages & inconvénients sont adapté pour le site.

- La première solution est la technologie Laser. Elle propose un débit jusqu'à 10Gb/s, la distance inter-batiment est 2km maximum. Elle dispose d'un niveau de sécurité des transmissions de données. Le cout de la technologie est faible comparé une installation fibre Optique, pour un débit de 100Mb/S, le prix d'une paire Terescope est disponible à partir de 5 660€. Une autre paire est disponible à partir de 11 821€ pour un débit de 10G/s. Enfin, l'installation et la maintenance sont simples et limitée.




- La seconde solution est la technologie Radio qui propose un débit allant jusqu'à 300 Mb/s et une distance de 10km maximum. Le cout d'une paire d'antenne wimax varie en fonction du débit et de sa distance de porter, on peut estimer 1000€ pour la paire d'une bonne antenne.

Voilà une image des deux technologies :




Maintenant lorsqu'on compare les deux technologies, elle se démarque plus pour leur inconvénient que pour leur avantage. L'avantage du Laser est son débit, son installation rapide et le fait qu'il n'y est pas de perturbation électromagnétique. Concernant les inconvénients, c'est le cout du matériel qui est supérieur à celui de la technologie Radio, ensuite il y a aussi la sensibilité à l'intempérie comme le brouillard. Pour les inconvénients du Radio (wimax), ce sont les sensibilités aux électromagnétiques et aussi l'inconvénient de répondre a certain norme.

Au final la technologie la plus confortable serait le laser, seul grand défaut, son prix.

6) Mettre en place un doublon de matériel brassé pour le switch 10 du Congrès car en cas de panne du switch 10, c'est toute l'attraction du Titanic qui suit, qui tombe en panne (SW22, SW24, SW25 et SW26)

7) Relier le SW25 au SW 22 pour éviter que le SW25 ne soit dépendant que d'un seul switch qui est le SW24. Prévoir alors la mise en place de spanning tree.

## 2. Installation & Configuration des Solution envisageables :

Pour notre installation, il faut réfléchir d'abord sur les connexions entre les switchs, choisir si on utilise des câbles rj45 ou alors utilise le SFP (un adaptateur pour Fibre)

- 4 facteurs rentrent en fonction (Le débit, le prix, installation et la distance)

Plus le débit et la distance seront hauts, plus le prix n'augmentera.

Donc pour le facteur débit, les deux solutions proposent des débits corrects car ils dépassent tout les deux le débit max d'un switch (1Gbits/s), ce qui va les partager est le facteur prix et installation. A ce niveau c'est le câble RJ45 qui prend l'avantage car il propose une meilleure installation et une meilleure résistance que l'utilisation d'une fibre aux matériaux fragiles qui demande en plus l'installation d'une jarretière entre chaque extrémité ce qui engendre un cout de temps supplémentaire pour son installation.

Donc le choix se porte plus vers un câble RJ45 de catégorie 5e (1Gbits/s), 6 (10Gbits/s), 6a (10Gbits/s), & 7 (>40Gbits/s), évidement plus la catégorie est haute plus le débit augmente.

1) Installation & configuration des 4 premières solutions proposées précédemment.

   Liste du matériel à configurer :

   - SW 27 - 192.168.1.29
   - SW 21 – 192.168.1.221
   - SW13 – 192.168.1.229
   - SW28 – 192.168.1.16 PC SECU
   - Un nouveau SW qui servira de secours pour le SW 28 PC SECU -

   Au niveau des connexions entre les switchs :

   Le SW 27 en 192.168.1.29 sera relié en câble rj45 (port 23) jusqu'au SW 21 en SFP (port 23), les deux ports devront être Tagged en Vlan 1, Vlan 6 et Vlan 7. Il faudra enfin vérifier que le Spanning tree est activé.

   Ensuite, le SW21 s'exporte de deux cotés :

- Du port 24 jusqu'au SW13 en port 24. Les deux ports devront être Tagged en Vlan 1, Vlan4, Vlan5, Vlan 6 et Vlan 7. Il faudra enfin vérifier que le Spanning tree est activé.
- Du port 25 en SFP jusqu'à la jarretière 3 / 4 de la salle serveur, ensuite c'est la 2eme fibre qui prend le relai jusqu'à la Jarretière 3 / 4 du PC Sécurité. Enfin un SPF de la jarretière jusqu'au port 48 du SW 28 du PC SECU. Les deux ports devront être Tagged en Vlan 1, Vlan3, Vlan4, Vlan5 et Vlan6. Il faudra enfin vérifier que le Spanning tree est activé.

Il reste enfin l'ajout du SW de secours pour la tolérance de panne du SW28.

Il suffit alors de connecter sur le port 24 en SFP du SW32 jusqu'au nouveau SW en port 24 SFP. Les deux ports devront être Tagged en Vlan 1, Vlan3, Vlan4, Vlan5 et Vlan6. Il faudra enfin vérifier que le Spanning tree est activé.

Configuration SW matériel :

Maintenant il faut que le SW 27 est la même configuration que le SW20. Le SW 27 Sera en mode passif et ne passera en mode actif seulement si le SW20 tombe en panne.

Concernant le SW secourt du SW 28, il faudra brasser les ports pour les appareils prioritaires du SW 28 comme les caisses, les boutiques, les tripodes ainsi que les imprimantes.

Par contre en cas de panne du SW28, une intervention physique devra interagir pour intervertir les connexions des équipements du SW28 vers le nouveau switch.