Université Toulouse
III Paul Sabatier

Filière STRI

Architecture de réseaux - B.E. Sujet A

Extension évolutive d'un réseau hospitalier

Auteurs :
Massip Thomas, Roques Nicolas, Tosi Émeric

04 Novembre 2015

Table des matières

Introduction

Dans le cadre de notre formation du Master STRI, nous réalisons par groupe de 3 un bureau d'étude sur une architecture de réseau.

Notre sujet porte sur l'extension et la révision d'un réseau d'un bâtiment hospitalier, plus précisement une clinique.

Cette clinique connaît une expansion, un nouveau pôle médical voit le jour. Ce nouveau bâtiment a besoin d'une architecture réseau nécessaire dans le travail journalier du personnel.

Nous proposons donc plusieurs architectures matérielles et logiques dans ce document afin de répondre aux besoins de la clinique.

1 Besoins Métier

1.1 Contexte

On se situe dans le cadre d'un établissement hospitalier, une clinique, qui souhaite développer une offre médicale dédiée aux maladies des voies respiratoires. Pour cela un nouveau pôle est construit à 50 mètres du bâtiment déjà existant de la clinique. Nous sommes chargés de réaliser l'étude de l'architecture réseau à implanter dans ce nouveau bâtiment.

Ce réseau devra répondre à une certaine tolérance aux pannes puisque utilisé à des fins médicales. Une interconnexion avec le bâtiment adjacent sera aussi nécessaire. Dans l'architecture réseau actuelle le cœur de réseau et l'accès à Internet se trouvent dans le bâtiment adjacent. Le déploiement de la nouvelle portion de réseau ne devra avoir aucune incidence sur le réseau déjà existant de la clinique. Les dimensions du bâtiment sont d'environ 35 mètres de long pour 11 mètres de large. Il est composé de 6 étages ayant chacun différents usages. Les différences entre ces étages seront un point de départ important pour établir l'architecture réseau : par exemple certains équipements médicaux nécessitent d'être inter-connectés, d'autres ne doivent en aucun cas être parasités pour assurer leur fonctionnement.

L'objectif principal est d'assurer un service performant, péren et sécurisé tant pour le personnel que pour les patients. Le réseau d'un hôpital ne dispose pas spécialement de performances de débit minimum mais demande une stabilité, une haute disponibilité et une sécurité très importante. Plusieurs solutions peuvent répondre à ce cahier des charges en respectant les critères suivants et les contraintes suivantes :

- La fiabilite ;
- Le coût ;
- La sécurité ;
- La durée de mis en place.

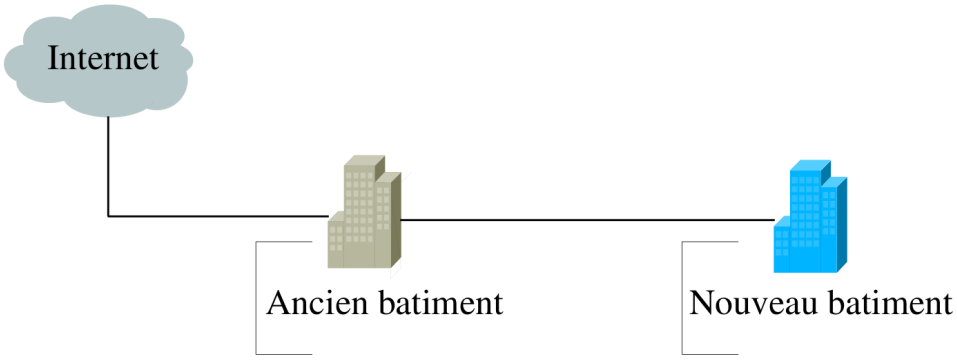

FIGURE 1 – Interconnexion du nouveau bâtiment avec l'ancien

L'ensemble du personnel doit pouvoir communiquer via les téléphones disponibles dans l'hôpital. Dans l'enceinte du bâtiment, la connection d'équipements sans fil doit être rendu possible pour le personnel dans le cadre de leur travail. L'accès à internet est fournit aux patients via une connexion sans fil.

Il n'est pas nécessaire de disposer d'une grande bande passante de façon continue. Le personnel ne fait que de la consultation d'informations ponctuelle et les visiteurs ont un accès internet limité et non prioritaire.

1.2 Description du bâtiment

Il est important de savoir comment le bâtiment est conçu afin de définir les équipements et périphériques utiles aux personnels et aux patients. Ces informations seront utiles pour déterminer l'architecture du réseau. Dans un premier temps nous allons nous intéresser aux spécificités de chaque étage.

Le niveau -2 contient seulement un parking et les vestiaires du personnel. Aucun accès réseau n'est nécessaire au niveau métier. Ce niveau est aussi l'arrivée du tunnel reliant les deux bâtiments, c'est donc ici que le lien d'interconnexion des deux bâtiments est installé. Ce lien doit monter jusqu'au rez-de-chaussée afin d'atteindre une salle dédié au infrastructure du réseau.

Le niveau -1, est l'étage le plus critique car il héberge deux blocs opératoires et quatre salles d'imageries, c'est donc ici que les équipements médicaux se situent. Ces équipements posent certaines contraintes comme par exemple des contraintes en terme de pollution électromagnétique pour les IRM. Les ordinateurs connectés sur ces appareils sont aussi très vulnérables : ces postes tournent sous des versions obsolètes de systèmes d'exploitation. Ils doivent donc être isolés dans le réseau et ne pas être connectés a Internet.

Le rez-de-chaussée, appelé par la suite niveau 0, contient une salle d'accueil, une salle d'attente, trois bureaux dédiés aux personnels administratif (deux personnes par bureaux) et une salle dédiée au réseau informatique. C'est dans cette dernière que le lien vers l'autre bâtiment sera connecté. Cette salle contiendra donc le cœur de réseau de ce bâtiment. Le maximum d'équipements y est aussi installer pour alléger les armoires techniques de dimensions limitées des autres étages.

Le premier étage, niveau 1, est composé de cinq bureaux de médecins, deux salles de réunions et deux laboratoire. Cet étage est donc dédié uniquement aux personnels de la clinique.

Les trois derniers étages, les niveaux 2 à 4, sont composés des chambres des patients. Chaque étage comporte 15 chambres ayant chacune des dimensions avoisinant les $12m^2$ ($4m*3m$). Enfin, à chaque étage, un petit local (une armoire technique) est prévu afin de recevoir quelques équipements réseaux.

1.3 Besoins matériels

Il est important de connaître les technologies et périphériques nécessaires pour répondre aux besoins. On va donc ici détailler les technologies et équipements nécessaires par étage.

1.3.1 Niveau -2

Aucun accès réseau n'est nécessaire à ce niveau. Il y a l'arrivée de la fibre reliant les deux bâtiments à ce niveau. Cette fibre est redondée et connectée à la salle réseau (le coeur du réseau) au rez-de-chaussée.

1.3.2 Niveau -1

Chaque bloc opératoires doit avoir au moins 2 prises Ethernet de type RJ45 afin d'y brancher les ordinateurs reliant les machines. Un téléphone IP et un ordinateur sont installés dans chaque salle de préparation d'opération. Dans les salles d'imageries un poste par salle et un téléphone IP sont à dispositions pour le personnel. Les équipements médicaux sont directement reliés aux ordinateurs.

1.3.3 Rez-de-chaussée

C'est à ce niveau que la salle dédiée aux infrastructures réseau est située. On y trouve une baie, sur laquelle sont raccordés les équipements tels que les serveurs, routeurs, commutateurs et le stockage des données. L'accueil est constitué de deux téléphones IP et deux ordinateurs. Les trois bureaux administratif ont deux téléphones et deux ordinateurs. Des bornes WiFi sont présentes afin de fournir un accès réseau aux visiteurs.

1.3.4 Niveau 1

N 1 : Les bureaux des médecins contiennent chacun un téléphone IP, un ordinateur et une prise RJ45 supplémentaire. Les imprimante peuvent être reliées en USB directement aux ordinateurs. Les deux salles de réunions sont composées d'un téléphone IP et d'un ordinateur. Les deux laboratoires de recherche ont un téléphone IP, deux ordinateurs et deux prises RJ45 supplémentaires. L'étage est couvert par la WiFi.

1.3.5 Niveaux 2 à 4

Chaque étage contient quinze chambres pour les patients. Les chambre disposent d'un téléphone IP. Nous ne prenons pas en compte les prises électriques ainsi que la télévision. Le personnel présent dans l'ensemble de ces étages, bénéficient de deux postes connectés à Internet. Un accès WiFi sera aussi disponible et bien séparé pour les patients et le personnel. Pour la longueur du bâtiment, sur ces trente cinq mètres, deux bornes WiFi suffisent pour couvrir chaque étages. La technologie PoE (Power Over Ethernet) sera privilégiée, permettant d'alimenter les téléphones et les bornes WiFi par le câble Ethernet.

2 Architecture Logique

Pour répondre au besoin présenter ci-dessus, nous allons d'abord établir une architecture logique de l'infrastructure. Cela permet de représenter les équipements ainsi que leur interconnexion. Elle a pour but d'identifier les différents rôles et services de chaque équipement à installer. C'est cette architecture qui justifie la qualité du réseau que nous proposons vis à vis des services attendus.

2.1 Couches logiques

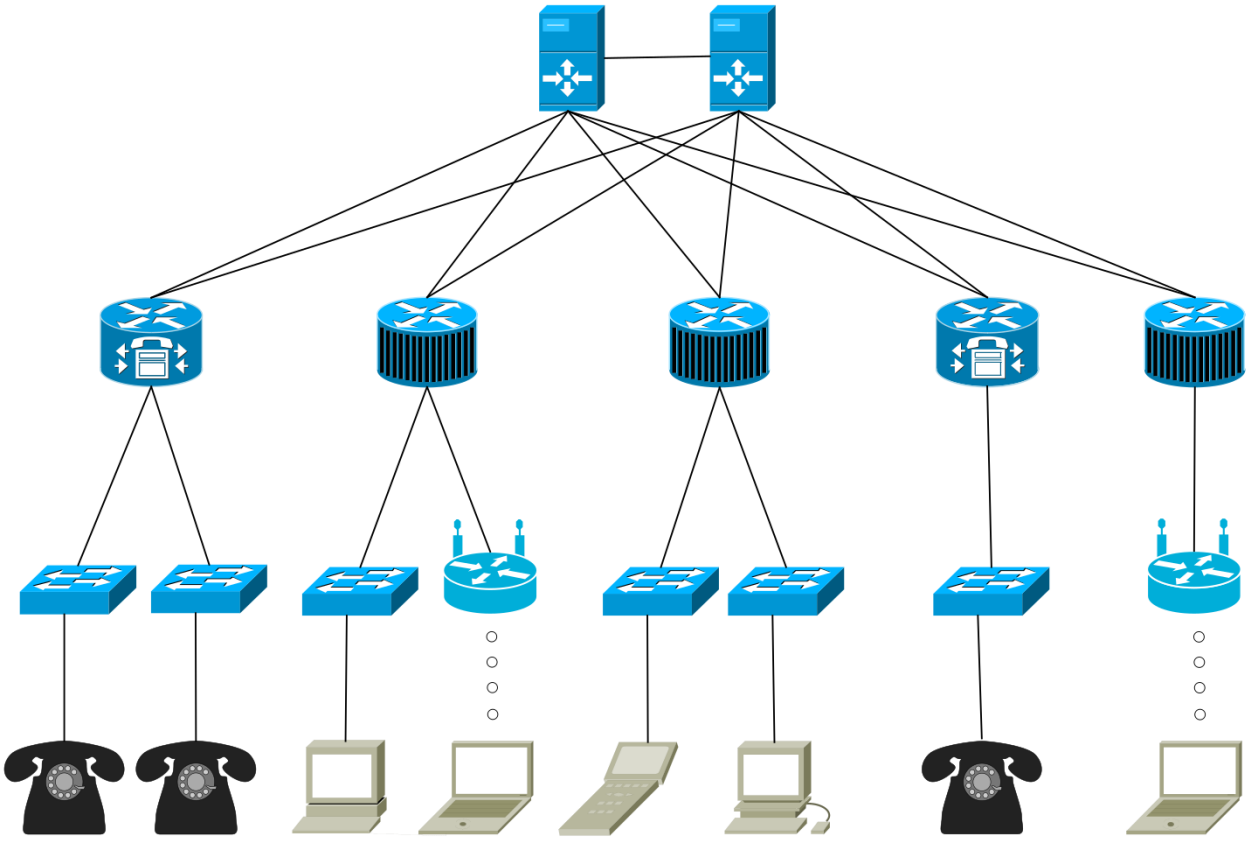

FIGURE 2 – Schéma logique hiérarchique du réseau

2.1.1 Couche coeur

C'est la couche supérieure. Son rôle est de relier entre eux les différents segments du réseau, par exemple les sites distants, les LANs ou les étages d'une société. Dans notre cas le coeur du réseau sera constitué de deux routeurs.

2.1.2 Couche distribution

Cette couche consiste à router, filtrer autoriser ou non les paquets. C'est a ce niveau que nous allons donc crée des VLANs sur les routeurs afin de délimiter l'étendu du réseau. Nous décidons de faire deux VLAN principaux : VLAN Interne, VLAN Visiteur.

2.1.3 Couche accès

Cette couche est la dernière avant de transmettre le paquet à l'hôte. Elle ne contient que des commutateurs qui permettrons de relayer l'information.

2.1.4 Couche hôtes

Il s'y trouve ici les différents types de terminaux .Tels que les terminaux portatifs, les ordinateurs fixes, les appareils médicaux(Scanner, radio etc).

2.2 VLANs

Nous avons décider de séparer le réseau interne avec celui des visiteurs pour une raison de qualité de service. Le besoin et la sécurité ne sont pas la même entre ses deux réseaux.

2.2.1 VLAN interne

Le VLAN Interne est divisé à l'intérieur en 3 VLANs.

VLAN Données-Interne : Il regroupe les différents équipements des bureaux administratif, des salles de réunions et de l'accueil.

VLAN VoIP-Interne : Il regroupe tous les équipements téléphoniques du personnel de l'hôpital, afin d'assurer une qualité de service vis a vis de la communication dans l'hôpital.

VLAN Médical : Il regroupe tous les équipements médicaux tels que les scanners , IRM et autre machines a usage médicales. Il y a aussi les informations des patients stocké dans celui-ci.

2.2.2 VLAN visiteur

Le VLAN Visiteur est lui divisé en 2 VLANs.

VLAN Données-Visiteur : Il regroupe toutes les données qui seront émises par le visiteur a l'aide de son téléphone portable ou tablette par exemple.

VLAN VoIP-Visiteur : Il regroupe tous les équipements téléphoniques fixe installer dans les chambres pour les patients.

2.3 Plan d'adressage

Étages	VLAN interne	Plage d'adresses
tous	VoIP-Interne	10.0.0.0/16
tous	Médical	10.1.0.0/16
0 à 4	Données-Interne	10.2.0.0/16
2 à 4	VoIP-Visiteur	10.128.0.0/16
0 à 4	Données-Visiteur	10.129.0.0/16

3 Architecture matérielle du réseau

3.1 Architecture physique

Après avoir vu l'architecture logique de notre réseau, nous pouvons maintenant établir l'architecture physique du réseau ainsi que le nombre d'équipements requis.

Tout d'abord, les deux bâtiments sont reliés à l'aide de deux fibres optiques de 100m (afin d'effectuer de la redondance en cas de coupure d'une de ces deux fibres) que l'on intègre dans le faux plafond du tunnel reliant les deux bâtiments. Les fibres sont relié aux routeurs qui ce situant au N0. Elles sont connectées au routeur à l'aide de connecteur SFP+.

Le niveau -1 est le niveau où les scanners, radio s'effectuent ainsi que les opérations. Comme vue précédemment, il n'y a ni de WiFi, n'y d'accès à internet à ce niveau. Les équipements médicaux étant branchés directement sur les ordinateurs a l'aide de câble console, on relie les ordinateurs ainsi que les téléphones au commutateur du niveau -1 situé dans un local prévu à cet effet. De ce fait, les terminaux du niveau -1 font partie du VLAN Médical.

Au niveau 0, une salle est entièrement dédié aux équipements réseau. Cette salle contient une armoire. On y installe deux routeurs, deux lames serveur qui sont sur deux machines différentes, un NAS, un onduleur afin de palier aux pannes de courant ainsi que trois commutateurs. Deux commutateurs de coeur de 24 ports où sont relié tous les équipements de l'infrastructure réseau et un commutateur 24 ports concernant le raccordement des terminaux du niveau 0. Tous les équipements dans la salle sont doublés afin de garantir une haute disponibilité.

Il y a aussi trois bornes WiFi, une fournissant internet pour les visiteurs et deux autres pour le personnel. La borne WiFi fournissant internet pour les visiteurs fait partit du VLAN DonnéesVisiteur. Les téléphones pour l'accueil et les bureaux administratif font partie du VLAN VoIPInterne. Les ordinateurs et les bornes WiFi destinés aux personnels eux font partie du VLAN Données-Interne.

Le niveau 1 contient uniquement des terminaux faisant partit du VLAN Interne. Les terminaux téléphoniques font partie du VLAN VoIP-Interne, les ordinateurs et les deux bornes WiFi du VLAN Données-Interne. Tous les terminaux sont raccordés sur deux commutateurs de 24ports qui se situent dans le local de l'étage prévue à cet effet. Les équipements téléphoniques sont raccordés à un commutateur et les autres types de terminaux tels que les ordinateurs, bornes WiFi et prises RJ45 supplémentaires sur le deuxième commutateur.

Pour les niveaux de 2 à 4, on place une borne WiFi afin de fournir Internet aux patients. Cette borne fait partit du VLAN Données-Visiteur. Les téléphones pour les patients se situant dans chaque chambres font partie du VLAN VoIP-Visiteur. Pour les médecins, infirmières, deux bornes WiFi sont mise en place et deux ordinateurs. Ces terminaux font partie du VLAN Données-Interne. Deux téléphones sont aussi présent pour le personnel, ils font partie du VLAN VoIP-Interne. Tous les terminaux sont raccordés à un commutateur. Du au grand nombre de

terminaux à ces étages, deux commutateurs seront mis en place. Pour une question d'installation et de maintenance, tous les téléphones sont relié à un commutateur et les autres terminaux de type ordinateur et borne sont reliés au deuxième commutateur.

Les commutateurs se trouvant aux étages sont reliés directement sur les deux commutateur de coeur qui se situe dans la salle du niveau 0.

Les téléphones et les bornes WiFi sont alimentés en PoE pour éviter d'installer des prises électriques à coté de ceux-ci. Tous les raccordements sont fait à l'aide de câbles Ethernet SSTP catégorie 6 RJ45 sans halogène.

3.2 Détails par étage

Étages	Équipements	Prises RJ45
N -1	— 6 Téléphones — 8 Ordinateurs — 1 commutateur 24ports	14 + 6 libres
N 0	— 3 Bornes WiFi — 8 Téléphones — 8 Ordinateurs — 2 routeurs — 2 Pare-feux logique — 3 commutateur 24ports — 1 NAS	16 + 4 libres
N 1	— 2 Bornes WiFi — 9 Téléphones — 9 Ordinateurs — 2 commutateur 24ports	18 + 9 libres
N 2 à 4	— 3 Bornes WiFi — 17 Téléphones — 2 Ordinateurs — 2 commutateur 24ports	19 + 2 libres

3.3 Schéma du réseau

3.4 Équipement du coeur du Réseau

3.4.1 Routeur

Le besoin essentiel de nos routeurs est de pouvoir gérer chaque trames qui circulent dans le réseau.

Tout d'abord nos deux routeurs auront la même fonction, les mêmes services installés. Pour cela l'équilibrage de charge de chacun d'eux permettra de limiter les pannes et faciliter la tolérance aux pannes. En effet dès lorsqu'un routeur est amené à être défaillant, l'autre routeur écoute celui-ci et sans retour, il prend l'initiative de prendre le relais. Les différents VLANs sont crées sur les routeurs.

Chaque routeur a la responsabilité d'administrer le coeur de réseau. Ils sont configurés pour assurer intégralement la sécurité et la gestion de routage du nouveau bâtiment. Les ports 80 (navigateur Web consultation d'un site HTTP) et 443 (sécurisé HTTPS utilisant la couche SSL) sont ouvert afin de gérer au mieux les requêtes. Un pare-feu UFW est lui aussi configuré pour simplifier la gestion des iptables. Pour finir un ensemble de protocoles destinés au routage au transport etc.. rendent le service d'un routeur totalement fonctionnel.

OSPF : c'est un protocole de routage, or RIP a ses limites et OSPF répond à une dynamique de routage plus moderne. OSPF est à mettre en place dans chaque routeur pour faciliter le routage. Les avantages de ce protocoles assurent ces bonnes caractéristiques :

Il n'y a pas de limite du nombre de sauts. Avec OSPF chaque routeur possède déjà une connaissance complète du réseau. Dès lors qu'il y a modification d'un lien ou ajout, une mise a jour des tables de routage se fait automatiquement. Bien évidemment le protocole OSPF ne connaît que sa zone. L'usage du VLSM améliore l'organisation du plan d'adressage. De même OSPF utilise une IP multicast pour envoyer à chaque routeur ses mises à jour d'état de lien.

Nous avons expliqué la fonctionnalité essentielle de la répartition de charges entre routeurs, mais aussi entre les serveurs lames que nous installerons. Nous pouvons dire également que OSPF assure un rendu efficace pour la répartition de charge. Contrairement à RIP, OSPF dispose d'une meilleure convergence des changements de routages grâce aux relations de voisinage qu'il affectionne.

3.4.2 Serveurs d'applications

Pare Feu : Le choix de la configuration du pare-feu se fait en mode logiciel sur le routeur sélectionné. En effet l'outil UFW qui est un mode de configuration permet de simplifier les iptables en ligne de commande. Cet outil UFW propose donc une alternative à l'outil iptables en toute simplification. Il est même possible de bénéficier d'une configuration automatique de UFW et gérer le pare-feu sans pour autant avoir manipulé le programme. La configuration de UFW se fait sur les deux routeurs du coeur de réseau. Ce Pare-Feu assure la sécurité des accès Internet et filtre les entrées et sorties.

NAS : c'est un serveur de stockage réseau appelé Network Attached Storage. Il s'agit d'un serveur de fichier autonome relié à un réseau. Contrairement à un SAN plus cher à l'achat traite au niveau de l'ensemble réseau à l'aide d'une capacité de stockage à grande quantité, il est composé de commutateurs, un ensemble de disques de stockage. Souvent le SAN est câblé par une fibre optique pour assurer la rapidité des échanges. Dans un réseau restreint comme celui-ci, bénéficier d'un serveur de stockage NAS suffit amplement.

Voici les raisons : Usage du stockage uniquement dans le réseau local de l'hôpital Données sauvegardées sont à titre professionnelles (locales) L'ensemble des données touche les informations de cet hôpital.

Le serveur NAS est à usage identique comme un serveur de fichiers. C'est pour cela qu'il fournit des services à travers un réseau dit IP. Le NAS se configure via une interface Web et via également un gestionnaire de fichiers Web. Pour cela dans le réseau de stockage, il est possible d'avoir le choix de traiter des protocoles tels que : le NFS (Network File System) Le CIFS (Common Internet File System) Le FTP (File Transfert Protocol)

3.5 Équipement de distribution

3.5.1 Commutateurs

Chacun de nos commutateur a pour rôle de bien diffuser les paquets. Ainsi chaque commutateur à cinq VLAN configurés pour bien différencier ceux-ci.

Explication de création de VLAN : un commutateur de 24 ports a n ports tagger pour chaque VLAN. Nous nous contenterons de voir dot1q dans le cas présent. Toutefois il est bon de savoir que chacun a son propre fonctionnement. ISL pour sa part encapsule toute les trames, quelque soit le VLAN. dot1Q, lui ne fait qu'insérer un tag (un marqueur) dans l'entête de la trame ethernet ... et uniquement sur les VLANs autres que le VLAN natif. (Le VLAN natif est celui utilisé par les protocoles comme CDP par exemple pour s'échanger les informations)

3.6 Équipement d'accès

3.6.1 Bornes WiFi

Nous proposons deux sortes de bornes Wi-Fi. Par conséquent deux usages bien différents sont à séparer pour bien sécuriser les zones d'accès de chaques personnes.

Pour cela, un accès est dédié en Wi-Fi pour les visiteurs appelés les patients. Cet accès propose une navigation internet sécurisée mais aussi limitée par un pare-feu UFW configuré à cet effet pour bloquer différentes navigations interdites (argent, téléchargement). La norme 802.11b est une norme la plus répandue est parfaite pour le besoin des patients et visiteurs. Elle propose un débit de 11 Mbps avec une portée de 300 mètres environs en lieu extérieur. Sa fréquence est de 2.4Ghz, avec 3 canaux radio disponibles. Un deuxième réseau wifi est mis en place pour le personnel. Ainsi le personnel peut travailler dans un réseau sécurisé, performant et sans dysfonctionnement. La norme 802.11a permet d'obtenir un haut débit de 30 Mbps réels environs. Sa fréquence est de 5 Ghz, avec 8 canaux radio.

3.7 QOS

Mettre en place un équilibrage de charges sur chaque routeur à l'aide du principe du Heart-Beat, chaque routeur mais aussi serveur lame écoutent son voisin. La répartition appellée en anglais "load Balançing" sert de rendre les services opérationnels en cas de défaillance d'un équipement. C'est pour cela que dans le cas d'un établissement hospitalier si un routeur ou un serveur n'est plus fonctionnel alors le second équipement pourra toujours répondre à la demande et fourni les ressources nécessaire telles que l'accès à la base de données, ou à internet.

4 Choix des équipements

4.1 lol

Conclusion

Pour conclure, avec LaTeX on obtient un rendu impeccable mais il faut s'investir pour le prendre en main.

Références

[REF] auteur. *titre*. édition, année.

[LPP] Rolland. *LaTeX par la pratique*. O'Reilly, 1999.