Haute école d'ingénierie Fribourg

Réseaux IP

Projet intégré

Études préliminaires

Auteur :
M. Pascal Roulin

Professeur :
M. François Buntschu

24 mars 2017

Table des matières

1 Introduction

L'évolution des technologies et surtout des réseaux informatiques faits qu'il n'est aujourd'hui plus concevable pour une entreprise de ne pas en disposer. Un réseau d'entreprise permet le partage de multiples ressources internes et l'accès à Internet. Les technologies à mettre en oeuvre afin de rendre tout cela possible sont nombreuses et nécessitent une étude afin de choisir parmi les possibilités laquelle est la plus adaptée au contexte.

Ce document concerne l'analyse du fonctionnement de différents composants d'un réseau d'entreprise comme son architecture globale, les réseaux sans-fil, les services Web et les protocoles DNS, DNS64 et NAT64.

La première partie se concentrera sur l'architecture des réseaux. Il s'agit d'une notion importante et de la première étape lorsque l'on souhaite mettre en place un réseau d'entreprise.

La seconde concernera l'accès au réseau de manière sans-fil. Cette technologie est communément appelée WiFi. Ce sujet touche de plus en plus les entreprises, car ses avantages ne sont pas négligeables. Cette technologie offre de la mobilité à ses utilisateurs tout en permettant à ceux-ci de profiter des mêmes accès aux ressources qu'avec le réseau câblé.

Il sera ensuite question des protocoles DNS, DNS64 et NAT64. DNS est un protocole permettant la traduction de noms de domaine en adresses IP, et inversement. Il traduit ce que nous utilisons, et préférons utiliser, en ce que les machines ont besoin pour fonctionner. Quant à DNS64 et NAT64, ce sont deux protocoles apparus afin de permettre la cohabitation des protocoles IPv4 et IPv6 durant la transition. Respectivement, ils permettent l'obtention d'une réponse à une requête autant IPv6 qu'IPv4 et la liaison entre des réseaux utilisant l'IPv4 et l'IPv6.

Finalement, le dernier sujet sera les services Web. Il s'agit de tout ce qui concerne la mise à disposition de ressources via Internet. La ressource la plus commune est l'accès à un site Web, qu'il soit accessible uniquement depuis le domaine de l'entreprise ou sur Internet.

Ces différents thèmes permettront de réaliser le design et la conception du réseau que nous devrons mettre en place pour l'entreprise Fri-Thinking & Co.

2 Architectures des réseaux

L'architecture d'un réseau désigne l'organisation des équipements réseaux installés au sein d'une entreprise. C'est une notion importante, car de nos jours, les utilisateurs s'attendent à pouvoir accéder à divers types de ressources et en tout temps. Il est donc nécessaire de mettre en place des réseaux performants, sécurisés et extensibles. Afin d'atteindre ces objectifs, la première étape est l'élaboration du design de l'architecture du réseau.

Une fois le design réalisé, il sera possible d'analyser quelles technologies et quels équipements sont les plus adaptés au projet.

Il existe plusieurs designs de réseau, le *Hierarchical Network Design*, le *Mesh Network Design* et le *Flat Network Design* seront analysés.

2.1 Hierarchical Network Design

Ce modèle comprend trois couches distinctes afin que chacune se focalise sur une fonction particulière du réseau.

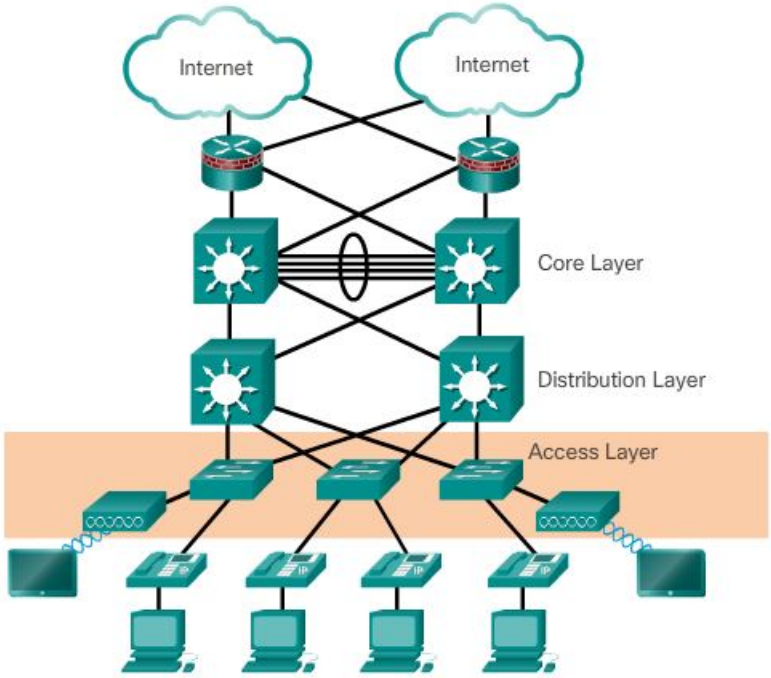

FIGURE 1 – Hierarchical Network Design

La figure ci-dessus illustre l'organisation que prennent ces couches dans un réseau d'entreprise.

2.1.1 Access Layer

Il s'agit de la couche la plus proche des utilisateurs. Celle-ci a pour rôle de leur fournir un accès au réseau. Les équipements qui la composent sont généralement des switchs et des points d'accès. Cette couche doit implémenter notamment des fonctions de sécurité et de qualité de service. Il est possible qu'elle implémente également des fonctions de couche 3, c'est-à-dire du routage.

Une notion à prendre en compte et sur laquelle se concentre cette couche est le "coût par port". C'est-à-dire l'investissement fait par l'entreprise afin de fournir un accès à Internet pour chaque port.

2.1.2 Distribution Layer

Cette couche relie les deux autres couches qui sont Access Layer et Core Layer. Il est question de la couche intelligente du réseau et fournit d'importantes fonctions dont notamment la gestion des règles d'accès, du routage ou encore la délimitation des domaines de broadcast.

Son rôle est également de décharger de certaines fonctions le Core Layer afin que celui-ci puisse fournir de meilleures performances sur les tâches qu'il est le seul à réaliser.

2.1.3 Core Layer

Le *Core Layer* est comme son nom l'indique le coeur du réseau, la couche la plus importante. Il s'agit de la couche reliant les composants de la couche *Distribution Layer* entre eux et elle relie également le réseau à Internet. Ces fonctions sont très importantes et requièrent donc une redondance, car on ne saurait se passer de cette couche. Les sous-couches ne pourraient plus communiquer entre elles et le réseau serait isolé d'Internet si celle-ci venait à être indisponible.

Cette couche nécessite également des équipements performants, car tout le trafic passera par ceux-ci. Ces équipements sont généralement les plus puissants du réseau en termes de traitement des paquets et ils peuvent gérer jusqu'à des connexions 10 Gbit/s.

2.2 Flat Network Design

Ce type de topologie requiert moins d'équipements et moins d'organisation. Il n'est cependant adapté qu'à de petites structures. En effet, ses capacités d'extension sont limitées et il devient difficile de résoudre un problème si celui-ci apparaît dans un réseau relativement important.

Ses composants ont généralement les mêmes fonctions et ne sont pas organisés d'une manière particulière, comme nous pouvons le voir sur le schéma ci-dessous.

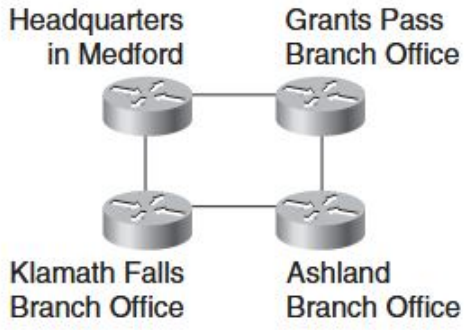

FIGURE 2 – Flat Network Design

2.3 Mesh Network Design

Ce type de réseau a comme particularité que chaque routeur et switch est connecté à tous les autres ou au moins à plusieurs autres équipements. Ce design offre plusieurs avantages comme une forte redondance et de bonnes performances. Cependant ils ont aussi de gros désavantages : ils sont chers à mettre en place et entretenir, il est difficile d'agrandir le réseau et il est également difficile de résoudre un problème.

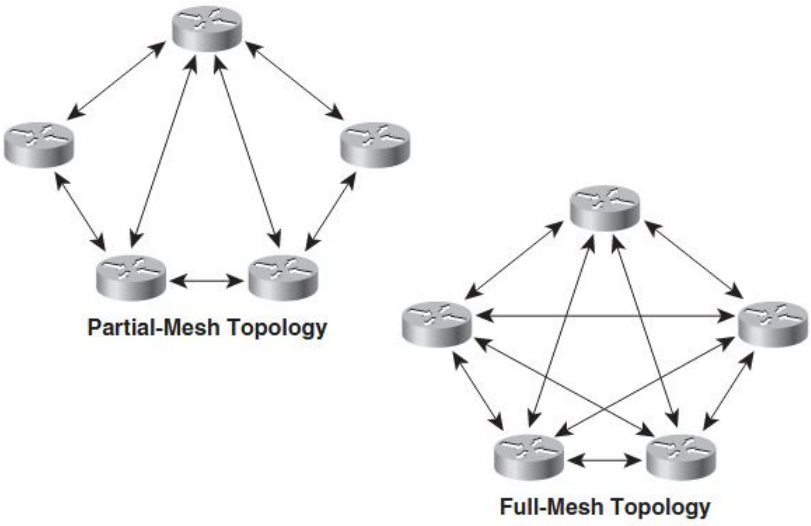

FIGURE 3 – Mesh Network Design

2.4 Comparatif de ces design

Si l'on souhaite élaborer un réseau relativement simple et de petite taille, le *Flat Network Design* peut s'avérer être le design à choisir. En effet, celui-ci sera moins cher et plus facile à installer que d'autres design. Il faudra cependant être conscient de ces limites et désavantages, surtout à l'avenir.

Le *Mesh Network Design* pourrait également s'avérer un bon choix pour un réseau de taille petite à moyenne. Il sera plus cher qu'un réseau basé sur le *Flat design* mais offrira de meilleures performances et une forte robustesse. Il aura cependant les mêmes limites concernant son évolution et la difficulté à résoudre un problème.

Lorsqu'il s'agit d'un réseau d'entreprise, le *Hierarchical Network Design* est certainement le plus adapté. Celui-ci permet de segmenter le réseau, de définir clairement les fonctions de chaque équipement et de limiter ceux-ci à ces fonctions. Sa modularité sera également un grand avantage quand il s'agira d'augmenter la taille du réseau en fonction de l'entreprise. Ses performances et sa redondance seront également un avantage pour autant que le modèle soit bien appliqué.

Quant à ses coûts, car cela reste un sujet important pour une entreprise, ceux-ci pourront être maîtrisés en investissant dans les bons équipements aux différentes couches. La facilité, surtout comparée aux autres design, de dépannage sera également une source d'économie.

3 Accès sans-fil / WiFi

Le WiFi (*Wireless Fidelity*), ou réseau sans-fil, permet de connecter différents équipements informatiques afin de permettre à ceux-ci de communiquer entre eux, ou d'accéder à Internet. Cette communication se fait grâce l'utilisation d'ondes radio, d'où son *Wireless* (de l'anglais, sans fil). Les protocoles composant cette technologie sont régis par les normes IEEE 802.11 (ISO/CEI 8802-11), et ceci depuis 1997. Cette technologie est maintenant utilisée par la plupart des particuliers et des entreprises puisqu'il est bien plus pratique de pouvoir accéder à Internet sans la contrainte d'un câble et ainsi de pouvoir se déplacer.
Cependant cette technologie n'est pas exempte d'inconvénients. En effet les débits sont plus faibles que ce que l'ont peut obtenir grâce à une liaison câblée et le médium utilisé, l'air, peut être une source de vulnérabilité au niveau de la confidentialité des données. Ce médium peut s'avérer être également une source d'instabilité.

3.1 Architectures

Un réseau local sans-fil est appelé WLAN (Wireless Local Area Netwrok) et se décline sous deux architectures différentes : Ad-Hoc et Infrastructure.

3.1.1 Architecture Ad-Hoc

Cette architecture a comme particularité de s'organiser sans infrastructure définie, ce qui est parfait pour un réseau temporaire ou simplement échanger des informations entre périphériques relativement proches. Ces réseaux n'utilisent pas les équipements réseaux habituels comme les routeurs ou les switchs. Les périphériques se connectent entre eux afin d'échanger des informations et former un *Independent Basic Service Set* (IBSS).
Le schéma ci-dessous illustre le fonctionnement de cette architecture et sa particularité qui est d'être sans point d'accès :

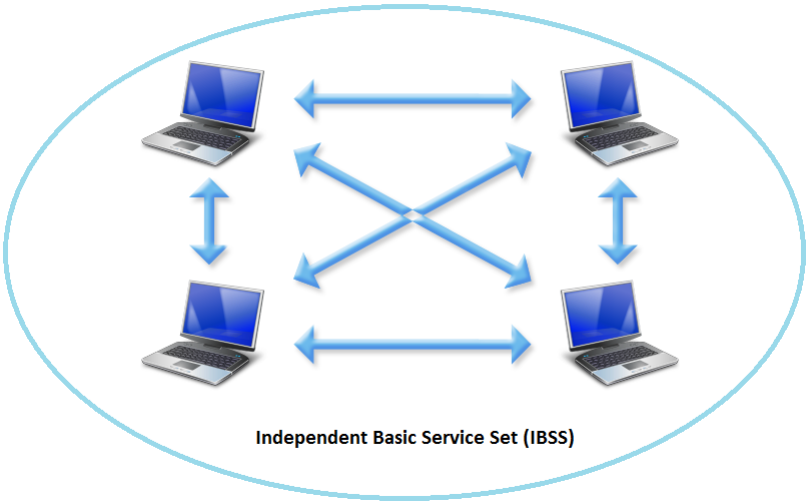

FIGURE 4 – Réseau Ad-Hoc

3.1.2 Architecture Infrastructure

Il s'agit de l'architecture la plus commune et utilisée. Elle composée de point(s) d'accès, auxquels se connectent les stations. Le réseau que forment ces stations et points d'accès (AP) se nomme *Basic Service Set* (BSS). Un ensemble de BSS forme un ESS (*Extended Service Set*).

Alors qu'avec un réseau Ad-Hoc les stations partagent des informations entre elles, l'architecture Infrastructure permet aux stations d'accéder à Internet ou d'autres périphériques câblés. Les périphériques se connectent aux AP, eux-mêmes reliés par câble au LAN, ce qui permet l'accès aux ressources LAN par les périphériques sans-fil.

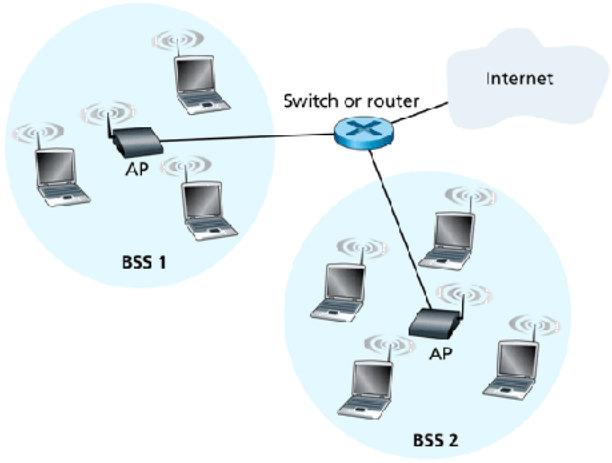

FIGURE 5 – Architecture Infrastructure

3.2 Bande de fréquences

L'une des caractéristiques d'une onde est sa fréquence et concernant le WiFi, celle-ci est réglementée et normalisée à 2.4 GHz et 5 GHz suivant la version de la norme.

3.2.1 Fréquence 2.4 GHz

Il ne s'agit pas d'une fréquence précise, mais d'une plage de fréquences qui s'étend de 2.4 GHz à 2.484 GHz, partagée en 14 canaux de 22 MHz chacun.
Voici la répartition de ces canaux sur la plage de fréquences :

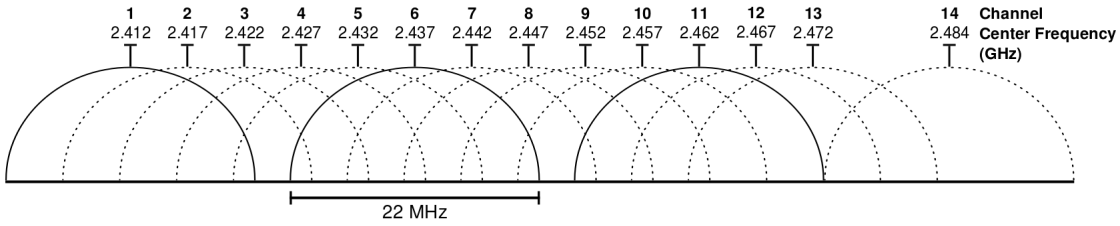

FIGURE 6 – Canaux pour la fréquence 2.4 GHz

3.2.2 Fréquence 5 GHz

Cette fréquence quant a elle est divisée en deux plages : de 5.15 GHz à 5.35 GHz et de 5.47 GHz à 5.85 GHz. Ces deux plages sont également sous-divisées en canaux de 20 MHz chacun, mais avec la particularité d'être espacés également de 20 MHz(ils ne se chevauchent pas contrairement à ceux de la bande 2.4 GHz). Contrairement aux canaux pour la fréquence 2.4 GHz, il est conseillé d'activer la sélection automatique du canal pour le point d'accès.

Cette fréquence présente un avantage au niveau du débit, mais un désavantage au niveau de la portée en comparaison avec la bande de fréquences 2.4 GHz.

3.3 Norme IEEE 802.11

IEEE 802.11 est un ensemble de normes définies par le comité de normalisation LAN/MAN de l'IEEE. La norme initiale, qui date de 1997, porte le numéro 802.11 et est également appelée 802 legacy puisqu'elle est la base des normes 802.11x.

Voici une présentation des différents standards et de leurs caractéristiques :

Norme	Date	Fréquence	Débit max	Modulation	Portée	
					Intérieur	Extérieur
802.11	1997	2.4	1.2 Mbit/s	FHSS, DSSS	20m	100m
802.11a	1999	5	54 Mbit/s	OFDM	35m	120m
802.11b	1999	2.4	11 Mbit/s	DSSS	35m	140m
802.11g	2003	2.4	54 Mbit/s	DSSS, OFDM	38m	140m
802.11n	2009	2.4 et 5	150 Mbit/s	OFDM	70m(2.4GHz)/35m(5GHz)	250m
802.11ad	2012	60	6.75 Gbit/s	OFDM	35m	
802.11ac	2013	5	866 Mbit/s	OFDM	35m	
802.11ah	2016	0.9	8 Mbit/s	OFDM	100m	

Table 1 – Liste des standards 802.11

Il existe d'autres amendements 802.11(d, h, i, j, e, r, u, y et w) qui concernent plus spécifiquement la couche MAC, la sécurité ou des mécanismes particuliers.

Le tableau 1 comporte une colonne *Modulation*. La modulation est un mécanisme permettant d'augmenter la fiabilité des WiFi. Voici une simple description de ces modulations :

- Frequency Hopping Spread Spectrum (FHSS). Il s'agit d'une vieille modulation uniquement utilisée par la norme 802.11 Legacy. Les réseaux utilisant cette modulation font sauter d'un canal à l'autre, et en même temps, l'émetteur et le récepteur afin de permettre à ceux-ci de communiquer. Plusieurs couples émetteur-récepteur sont ainsi possibles puisqu'ils n'interfèrent pas entre eux.
- Direct Sequence Spread Spectrum (DSSS). Cette modulation se sert du découpage en canaux de la bande de fréquence, comme illustré sur l'image 6, et choisit des canaux qui ne se chevauchent pas. Les canaux généralement utilisés sont le 1, 6 et 11.

- Orthogonal frequency-division multiplexing (OFDM). Cette modulation est utilisée sur les versions plus récentes de la norme 802.11, car elle permet de meilleures performances. Son principe est de multiplexer les transmissions sur un grand nombre de sous-porteuses. Aujourd'hui, cette modulation est également utilisée pour les réseaux mobiles, la radiodiffusion numérique ou encore le VDSL par exemple.

3.4 Spécifications

Les trames 802.11 sont composées comme ceci :

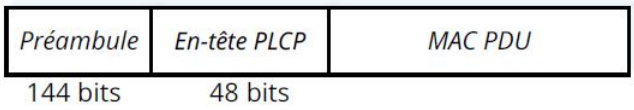

FIGURE 7 – Format des trames 802.11

Le préambule est dépendant de la couche physique et il permet de délimiter les trames. L'entête PCLP contient des informations concernant le codage de la trame. Le champ *MAC PDU* est lui-même découpé comme suit :

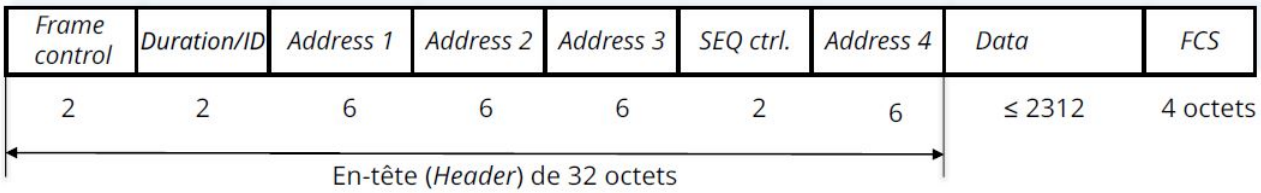

FIGURE 8 – Contenu du champ MAC PDU

Les détails de ces champs sont décrits dans le cours de M. Buntschu : "Réseaux IP : 350. Wireless LAN", 09/2015 ou dans le document disponible à l'adresse http://easytp.cnam.fr/terre/images/WiFi.pdf.

3.5 Mise en place d'un réseau sans-fil

Lorsque l'on souhaite mettre en place un réseau WiFi, il est impératif d'analyser les besoins auxquels celui-ci devra répondre. Afin de définir le nombre d'AP nécessaire, et donc la capacité du réseau, il faut définir :

- **Le nombre d'utilisateurs par AP** afin de leur garantir à chacun les performances nécessaires.
- **Le nombre de périphériques utilisés par chacun de ces utilisateurs.** Aujourd'hui, chaque utilisateur possède, en plus de son ordinateur portable, un smartphone qu'il souhaite également connecter au réseau sans-fil. De plus, les smartwatch pourraient tendent à se démocratiser et celles-ci offrant la possibilité de se connecter aux réseaux WiFi, elles sont également à prendre en compte.

- **La répartition géographique** de ces utilisateurs puisque les points d'accès ont une portée limitée. Il peut également être nécessaire d'analyser si des obstacles (par exemple : un mur) sont susceptibles de séparer l'utilisateur de l'AP auquel il se connecte, ou si le WiFi doit être accessible depuis l'extérieur du bâtiment(parking, terrasse, etc.).
- **Le type et la quantité de trafic généré.** Le débit nécessaire n'est pas le même qu'il s'agisse d'une personne consultant ses mails et faisant quelques recherches sur Internet, ou d'une autre devant fréquemment mettre en ligne des vidéos ou effectuer de gros transferts de données.

Afin de mettre en place de manière optimale un réseau sans-fil, il existe plusieurs bonnes pratiques comme le fait de préférer mettre les AP dans les bureaux plutôt que dans les couloirs, de placer les points d'accès dans des endroits dégagés afin d'éviter les obstacles, d'utiliser les deux bandes de fréquences (2.4 GHz et 5 GHz) et d'éviter le chevauchement des canaux ou encore d'installer plusieurs AP pour une même zone géographique si celle-ci est susceptible d'utiliser beaucoup de bandes passantes.
D'autres recommandations sont disponibles dans les deux documents, High Density Wi-Fi Deployment Guide et Location-Aware WLAN Design Considerations, référencés au point 8.2.

3.6 Sécurité

Il est nécessaire de sécuriser un réseau sans-fil, car celui-ci utilise l'air comme médium. Le signal peut donc être capté et lu s'il n'est pas protégé. Différentes méthodes de chiffrement ont été introduites afin de pallier à ce problème. La plus récente et conseillée est le chiffrage WPA2.

De plus, il est également nécessaire de mettre en place une authentification requise pour les utilisateurs. Le mode d'authentification, qui est l'utilisation d'une clé ou mot de passe, utilisé par les particuliers n'est pas envisageable, car il ne garantit pas une sécurité et une flexibilité suffisante. En effet, si l'on changeait la clé, il serait nécessaire d'effectuer le changement sur tous les périphériques. Il serait également problématique que le mot de passe devienne connu suite à une fuite.

Le standard IEEE 802.1X offre des moyens d'implémenter de manière adéquate la sécurité WiFi en entreprise. Ce standard prévoit l'utilisation d'un serveur d'authentification RADIUS chargé de valider l'identité de l'utilisateur. RADIUS (*Remote Authentication Dial-In User Service*) est un service client-serveur permettant de gérer des données d'authentification, que cela soit les informations de connexion des utilisateurs ou des informations comme l'adresse IP du client ou encore son temps de connexion maximal. Le standard 802.1X se base également sur l'utilisation du protocole EAP (*Extensible Authentication Protocol*). Ce protocole embarque différentes méthodes d'authentification utilisant des chiffrements.

3.7 Intérêt pour le projet

Le cahier des charges comprend la mise en place d'un réseau sans-fil pour l'entreprise Fri-Thinking & Co. Il est donc préférable de connaître les possibilités offertes par les technologies d'aujourd'hui et les bonnes pratiques afin d'installer un réseau WiFi optimal.

4 DNS, DNS64 et NAT64

4.1 DNS

Un DNS, pour *Domain Name System*, est un service permettant l'association d'un nom de domaine avec une adresse IP, et inversement. En d'autres termes, ce service traduit les noms de domaines (ou "adresse Internet") que l'Homme utilise en adresses IP, que les machines utilisent afin de communiquer. Ce service est donc utilisé et a été élaboré afin de nous simplifier l'utilisation des moyens informatiques connectés, puisqu'il est plus aisé de retenir un nom qu'une suite de 4 nombres.

4.1.1 Fonctionnement

Le système des noms de domaines est organisé de manière hiérarchique. C'est-à-dire qu'il est organisé en plusieurs niveaux, nommés *Name Space* ou espace des noms.

Pour ce qui est de la hiérarchisation, prenons l'exemple de *www.heia-fr.ch.*, nous pouvons voir que celui-ci comporte trois ".". Ceux-ci permettent de séparer les différents niveaux.
Voici la décomposition en niveau de ce nom de domaine :

Niveau 0 : "." - *Racine* ou *Root*

Niveau 1 : ".ch" - Il s'agit du domaine national (appelé *country code top level (ccTLD)* réservé à la Suisse.

Niveau 2 : ".heia-fr" - Il s'agit du sous-domaine que possède l'école. Les noms de ce niveau sont attribués par différents fournisseurs de noms, suivant le pays, aux entreprises, particuliers ou institutions gouvernementales.

Niveau 3 : "www" - Il s'agit d'un sous-domaine de *heia-fr* créé par l'école. En effet, les labels inférieurs au niveau 2 sont administrables directement par le possesseur du nom du niveau supérieur.

La hiérarchie de ce nom, ou de n'importe quel autre, suit la hiérarchie représentée par la figure ci-dessous. Cette organisation est importante, car elle permet de comprendre comment se déroule une requête DNS. Lors de la résolution d'un nom, les serveurs DNS de cette arborescence sont parcourus de haut en bas, jusqu'à définir l'adresse IP correspondant à la machine souhaitée.

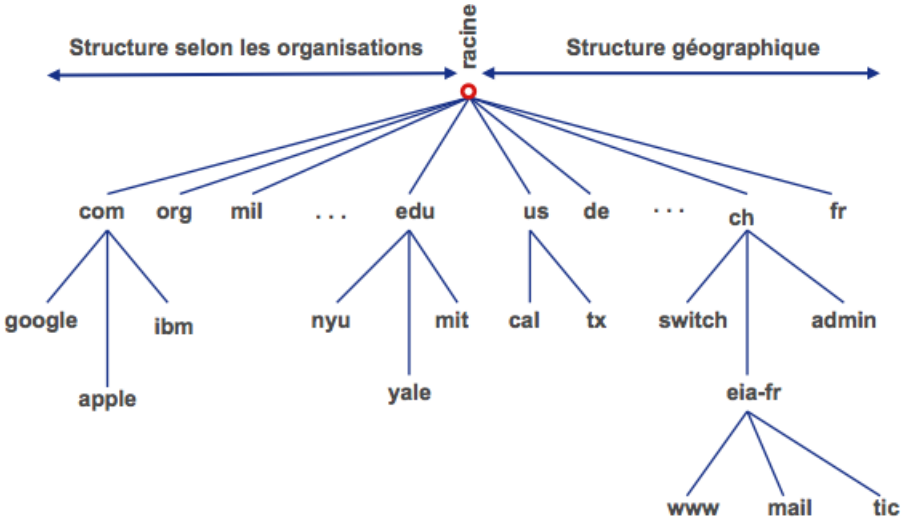

FIGURE 9 – Hiérarchie DNS

La résolution d'un nom peut se faire de deux manières différentes : par récursion et par itération. Voici un exemple de résolution par itération :

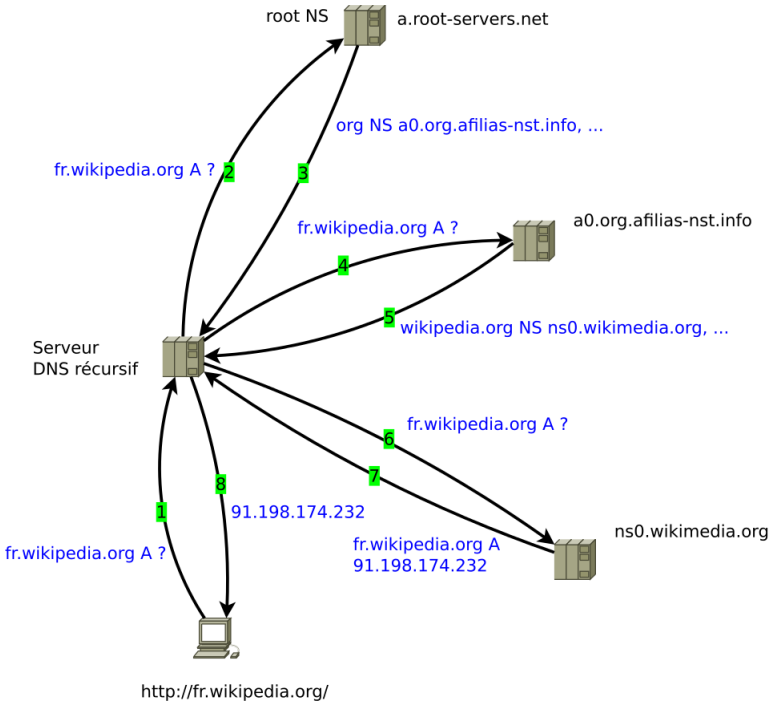

FIGURE 10 – Résolution DNS par itérations

Comme nous pouvons le voir, le client s'adresse au serveur DNS qui lui est associé dans sa configuration réseau. Ainsi ce serveur DNS se charge d'effectuer la suite de la recherche en interrogeant, suivant la hiérarchie, les autres serveurs DNS jusqu'à trouver l'adresse IP souhaitée. Il finira par retourner cette information au client.

Si nous analysons le déroulement de cette requête, nous pouvons observer que la première requête, celle du client, est récursive, alors que le serveur réalise des requêtes itératives par la suite. Il faut comprendre par *récursive* que la requête est déléguée alors que des requêtes itératives sont effectuées par la même machine en s'adressant à différents serveurs.

Il est également nécessaire de relever l'utilisation de caches afin d'accélérer les recherches et de réduire le nombre de requêtes. Lorsque la réponse arrivera au serveur effectuant la requête pour un client, celui-ci l'enregistre dans son cache, afin de répondre directement si une même requête est effectuée par la suite. Cependant, comme il n'est pas responsable de la zone pour laquelle il répondra, sa réponse sera balisée comme venant d'un serveur non autoritaire. Un serveur est appelé autoritaire lorsque celui-ci est configuré comme serveur gérant une zone DNS (qu'il soit primaire ou serveur secondaire). Généralement, plusieurs serveurs secondaires épaulent un serveur primaire afin d'offrir une redondance des informations relatives à la zone dont ils s'occupent.

4.1.2 Spécifications

Un serveur DNS utilise le protocole UDP, avec le port 53, et ne chiffre pas ses réponses. Lorsque deux serveurs DNS partagent leur base de données afin de les tenir à jour, ceux-ci utilisent TCP, afin de garantir le transfert.

Les messages DNS suivent le format suivant :

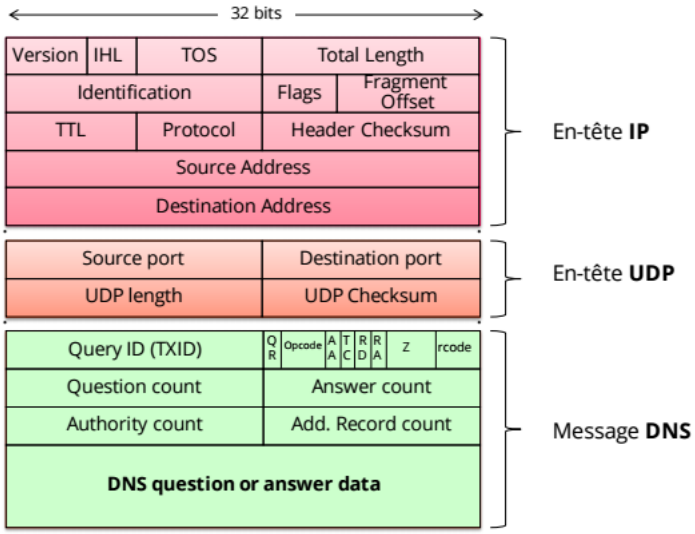

FIGURE 11 – Format des messages DNS

Concernant le champ *DNS question or answer data*, celui contient le nom de domaine à traduire et son type. Les serveurs y ajouteront ensuite les réponses qu'ils fourniront ainsi que les serveurs autoritaires. Pour ce qui est du type de la requête, il en existe plusieurs, car il est possible de demander une autre information qu'une adresse IP correspondant à un nom. Il est par exemple possible de demander quel est le serveur mail d'une zone DNS. Ces types se renseignent pour chacun des enregistrements dans la base de données d'un DNS.
Voici les types principaux :

- **SOA** (Start Of Authority) : Définit certaines informations générales sur la zone (serveur principal, adresse email de contact, différentes durées dont celle d'expiration, numéro de série de la zone)
- **A** (IPv4 Address) : Fait correspondre un nom d'hôte à une adresse IPv4
- **AAAA** (IPv6 Address) : Fait correspondre un nom d'hôte à une adresse IPv6
- **CNAME** (Canonical NAME) : Permet de faire des alias. Pour qu'un domaine pointe vers un autre.
- **MX** (Mail eXchange) : Définit le(s) serveur(s) email pour ce domaine
- **PTR** (PoinTeR record) : Associe une adresse IP à un nom. Utilisé pour les requêtes inverses
- **NS** (Name Server) : Enregistre le(s) serveur(s) DNS pour le domaine en question

Un exemple de configuration d'un serveur DNS est disponible en annexe.

4.1.3 Vulnérabilités

Il existe deux vulnérabilités principales du DNS. La première se nomme *Cache Poisonning* et consiste à fausser les informations que le serveur DNS stocke dans son cache afin que celui-ci réponde de manière erronée aux prochaines requêtes. Le but pour un pirate est de rediriger les clients vers un autre site ou serveur. Il existe une version sécurisée du DNS afin de pallier à cette faille : DNSSEC.

La deuxième vulnérabilité vient du fait de l'organisation du DNS. Comme nous l'avons vu, DNS est hiérarchique et a pour base une *racine* (composée de 13 serveurs, répartis géographiquement). Si cette racine venait à être mise hors service, DNS ne fonctionnerait progressivement plus (le temps que les informations dans les caches expirent). De nombreuses attaques ont été réalisées afin d'obtenir ce résultat. Jusque là, et heureusement, l'impact de ces attaques est resté limité.

4.1.4 Standards

Plusieurs RFC concernent le *Domain Name System*, voici les principales :

- RFC 882, Novembre 1983 - *CONCEPTS and FACILITIES*
- RFC 883, Novembre 1983 - *IMPLEMENTATION and SPECIFICATION*
- RFC 1034, Novembre 1987 - Mise à jour de *CONCEPTS AND FACILITIES*
- RFC 1035, Novembre 1987 - Mise à jour de *IMPLEMENTATION and SPECIFICATION*
- RFC 1591, Mars 1994 - *Structure and Delegation*
- RFC 6195, Mars 2011 - *IANA Considerations*
- RFC 6895, Avril 2013 - Mise à jour de *IANA Considerations*

4.2 Transition IPv4 - IPv6

L'arrivée par nécessité d'IPv6 nous amène à effectuer une transition, d'IPv4 à IPv6. Cependant, des périphériques utilisant IPv4 ne sont pas capables de communiquer avec ceux utilisant IPv6, et inversement, car les adresses ne sont pas compatibles entre-elles. Il est alors nécessaire de mettre en place certains mécanismes afin de permettre la cohabitation de ces deux protocoles durant la transition.

Les deux approches possibles sont la traduction de protocoles et l'utilisation d'une *double pile*. Cette dernière approche consiste à configurer aussi bien en IPv4 qu'en IPv6 une machine. Elle est donc capable de communiquer aussi bien avec des périphériques en IPv4 qu'en IPv6.

La première approche, qui sera décrite ici, est donc la traduction des protocoles grâce à DNS64 et NAT64. Ces deux services sont nécessaires en parallèle afin que la traduction puisse se faire.

4.3 DNS64

DNS64 est un serveur DNS ayant comme particularité de répondre à des requêtes de type AAAA (donc IPv6) même s'il ne possède qu'un enregistrement de type A (IPv4). Ce serveur se sert d'un préfixe fixe et de la représentation en hexadécimal de l'adresse IPv4.

4.3.1 Fonctionnement

Les étapes réalisées si une machine uniquement IPv6 souhaite atteindre un service uniquement IPv4 sont les suivantes :

1. Le client adresse une requête de type AAAA à son DNS.
2. Son DNS fera ensuite les démarches afin de contacter le serveur autoritaire et lui demandera une information de type AAAA.
3. Le serveur gérant la zone répondra par une réponse vide, car il ne possède pas d'enregistrement AAAA (Rappel : le domaine cherché est uniquement IPv4)
4. Le serveur DNS du client contactera à nouveau le serveur autoritaire, mais cette fois-ci avec une requête de type A.
5. Le serveur autoritaire, qui possède cette information cette fois, répondra avec une adresse IPv4.
6. Le serveur DNS du client, étant un serveur DNS64, fera ensuite la conversion de l'adresse IPv4 en une adresse IPv6.

La conversion se fera de manière algorithmique et suivant la configuration du serveur DNS64. La plupart du temps il s'agira d'utiliser un préfixe suivi de l'adresse IPv4 en hexadécimal.

Le préfixe peut être choisi soit en utilisant le préfixe réservé à la traduction d'adresse (décrit dans la RFC 6052) qui est *64 :ff9b : :/96* ou selon un préfixe réservé à un opérateur réseau.

4.4 NAT64

DNS64 n'est pas suffisant afin de permettre à deux machines configurées sur des protocoles différents de communiquer. Le protocole NAT64 est donc nécessaire en parallèle à DNS64.

NAT signifie *Network Address Translation*. Ce protocole existe dans sa version manipulant uniquement des adresses IPv4 et a pour but de d'associer des adresses IPv4 à d'autres. Ce mécanisme est utilisé afin de permettre à des machines ayant des adresses IP privées, c'est-à-dire non uniques et non routables sur Internet, de communiquer avec le reste d'Internet comme si elles utilisaient des adresses IP publiques. Un autre protocole lié à NAT et le PAT. Le *Port Address Translation* réalise la même opération que le NAT, mais celui-ci associe une adresse IP privée à un port combiné à l'adresse IP publique du routeur. Il permet ainsi une économie d'adresses, puisque l'on peut traduire une grande quantité d'adresses privées en une seule adresse publique. Cet avantage n'en est pas un lorsqu'il s'agit d'IPv6, puisque nous ne risquons pas d'être en pénurie d'adresses IPv6. Cependant, une évolution de NAT, qui est NAT64, est actuellement nécessaire à la cohabitation des adresses IPv4 et IPv6.
NAT64 se chargera de lier une adresse IPv6 à une adresse IPv4 afin de permettre le bon acheminement des paquets.

4.4.1 Stateless NAT64 vs Stateful NAT64

Le *Stateless NAT64* fonctionne comme le NAT décrit précédemment. Il associe une adresse IPv4 à une adresse IPv6, ou inversement. Il n'y a donc aucune économie d'adresse réalisée.

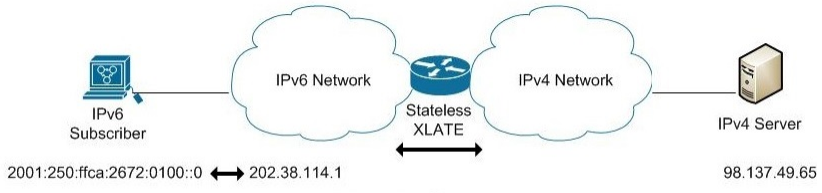

Figure 12 – Stateless NAT64

Concernant le *Stateful NAT64*, celui-ci correspond, en quelque sorte, au PAT. Il traduit une adresse IPv6 en une adresse IPv4 combinée à un port. L'adresse IPv4 reste la même lorsque plusieurs adresses IPv6 sont traduites, mais le port change. C'est ce port qui différencie ensuite quelle adresse IPv6 doit être adressée.

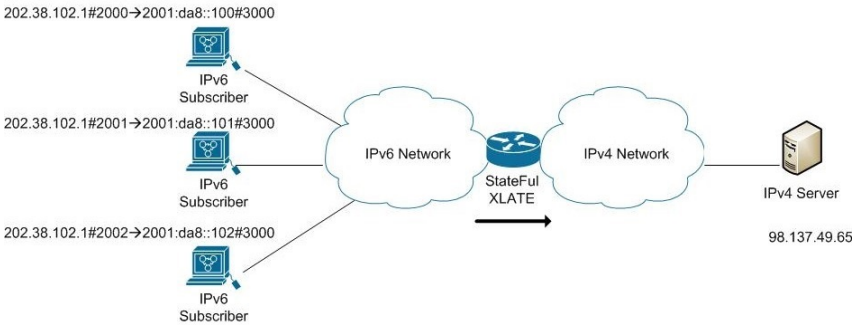

Figure 13 – Stateful NAT64

4.5 DNS64 et NAT64

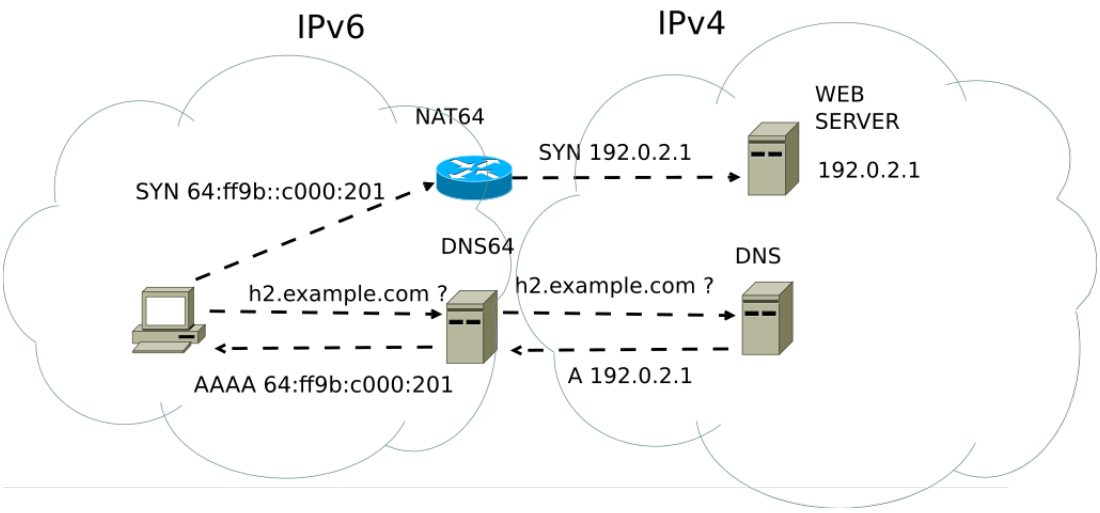

FIGURE 14 – Stateful NAT64

Voici la combinaison des deux protocoles présentés. Comme nous pouvons le voir, la communication entre un réseau IPv4 et un réseau IPv6 requiert ces deux protocoles. Si nous analysons le déroulement du dialogue entre le client et le serveur Web, voici les étapes :

1. Le client demande à son serveur DNS l'adresse IP de h2.example.com (une demande d'adresse IPv6)
2. Le serveur DNS du client ira questionner le serveur DNS responsable de la zone example.com
3. Le serveur DNS d'example.com répondra premièrement par une réponse vide à la requête IPv6
4. Le serveur du client renverra une requête, mais cette fois-ci, il demandera un enregistrement IPv4
5. Le serveur DNS d'example répondra avec un enregistrement IPv4
6. Le serveur DNS du client convertira cette réponse en une adresse IPv6 grâce à un préfixe
7. Le client connaît enfin l'adresse qu'il souhaite atteindre. Il commencera donc l'ouverture d'une session avec le serveur Web
8. Le service NAT64, du routeur, entre en fonction, car il doit connecter son réseau interne en IPv6 à un réseau IPv4. Il associera l'adresse IPv6 à une adresse de son pool d'adresses IPv4 ou plutôt, il enregistrera le port associé à l'adresse IPv6, combiné à l'adresse IPv4 publique de son réseau
9. La réponse du serveur Web h2.example.com sera également traduite par le NAT64 pour être adressée au client en IPv6

4.6 Utilité dans le projet

Nous aurons besoin de mettre en place DNS64 et NAT64, car le réseau à mettre en place pour Fri-Thinking & Co est composé d'une partie adressée en IPv4 et d'une autre en IPv4/IPv6, comme nous pouvons le voir sur l'image ci-dessous :

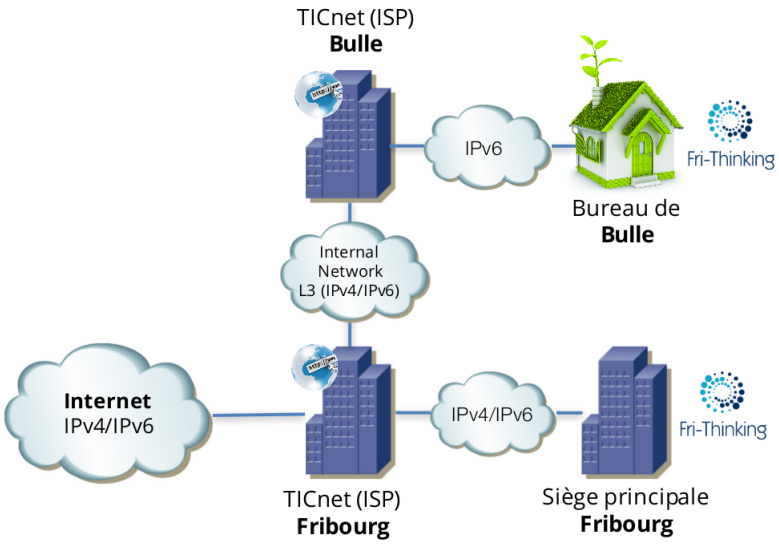

FIGURE 15 – Schéma réseau Fri-Thinking & Co

Nous devrons également disposer d'un serveur DNS afin d'administrer la zone DNS *fri-thinking.ch* comme spécifié dans le cahier des charges.

5 Service Web

5.1 Présentation

Un service web consiste à rendre accessibles certaines ressources ou fonctionnalités sur Internet ou sur un intranet. Ce service doit se faire de manière automatique, c'est à dire sans intervention humaine, et être accessible en tout temps. Afin de remplir ce dernier critère, il est nécessaire de disposer d'un serveur web, c'est à dire d'une machine remplissant le rôle de répondre en tout temps aux demandes des utilisateurs.

Les demandes sont en majorité des requêtes de pages HTML, mais elles pourraient également être des téléchargements de fichier ou du streaming vidéo. Du côté utilisateur, ces requêtes se font généralement grâce à un navigateur Web, qui est le client HTTP le plus courant.

5.2 Fonctionnement

L'échange entre le client et le serveur se fait grâce au protocole HTTP, ou dans sa version sécurisée (HTTPS). Le protocole HTTP (*Hypertext Transfer Protocol*) est un protocole de couche 7 (Application) du modèle OSI, utilisant le protocole TCP comme couche de transport et utilise le port 80 par défaut (443 pour HTTPS).

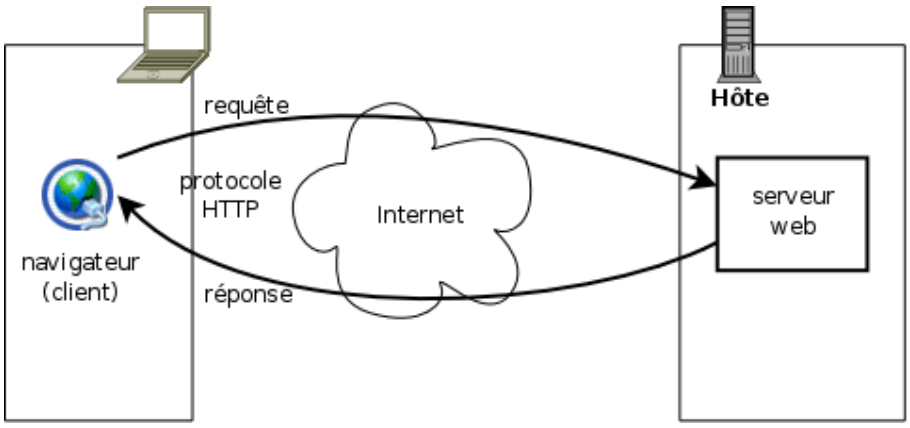

FIGURE 16 – Schéma d'un échange client-serveur

Le serveur quant à lui a besoin d'une application afin de répondre aux requêtes. Il existe de nombreuses plateformes permettant ceci, dont voici les principales :

- **Apache HTTP Server** : Créé en 1995, il est actuellement le serveur HTTP le plus répandu. Il s'agit d'un logiciel libre et multiplateforme.
- **Nginx** : Plus récent qu'Apache, celui-ci est apparu en 2002. Il s'agit également d'un logiciel libre. Celui-ci est spécialisé dans les connexions simultanées.
- **Internet Information Service** (IIS) : Logiciel développé par Microsoft, supportant le langage ASP.NET. Ce serveur Web ne peut être mis en place que sur un Windows.
- **Lighttpd** : Développé initialement par Jan Kneschke depuis 2003, ce serveur Web est connu pour sa faible consommation de ressources, autant au niveau mémoire que charge CPU.

Ces services se partagent le marché selon le graphique ci-contre.

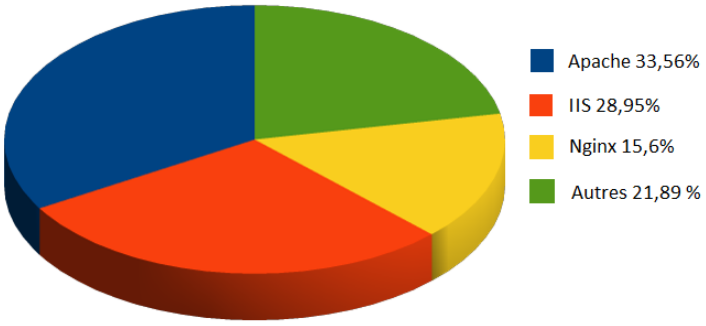

FIGURE 17 – Parts de marché des services Web

Le fait de connaître les parts de marché d'un produit reste une information utile puisqu'elle nous informe du succès du produit et spécialement de la quantité potentielle d'informations que l'on pourrait trouver en cas de besoin.

5.3 Intégration dans le projet

Afin de remplir le cahier des charges, il nous sera nécessaire de mettre en place un serveur Web pour l'entreprise Fri-Thinking & Co. Puisque le site sera statique et peu gourmand, Lighttpd peut s'avérer une bonne solution.

6 Conclusion

Les recherches et l'écriture de cette analyse m'ont permis d'en apprendre plus sur certains sujets et d'en découvrir de nouveaux. J'ai pu découvrir par exemple différentes architectures réseaux ainsi que leurs avantages et inconvénients. J'ai également pu approfondir certaines de mes connaissances sur le WiFi et en apprendre davantage sur ce sujet.

Les thèmes traités devraient nous aider pour la suite du projet, notamment pour la partie conception et design, mais également pour la partie réalisation.

J'ai pu me rendre compte que la recherche d'informations et la compréhension de celles-ci prennent une grande partie de la réalisation de ce genre de rapport. Ce fut cependant intéressant de pouvoir rechercher différentes sources, de découvrir réellement les RFC et de comparer les informations entre elles. Certains sujets se sont avérés plus compliqués que prévu, car les sources disponibles étaient en moins grande quantité.

Fribourg, le 24 mars 2017

Pascal Roulin

7 Glossaire

Terme	Définition
IIS	Internet Information Service
DNS	Domain Name System
HTTP(S)	Hypertext Transfer Protocol (Secure)
Modèle OSI	Open Systems Interconnection, standard de communication
NAT	Network address translation
PAT	Port Address Translation
WiFi	Wireless Fidelity
IP	Internet Protocol
DHCP	Dynamic Host Configuration Protocol
IEEE	Institute of Electrical and Electronics Engineers
ISO	Organisation internationale de normalisation
WLAN	Wireless Local Area Network
LAN	Local Area Network
IBSS	Independent Basic Service Set
BSS	Basic Service Set
ESS	Extended Service Set
AP	Access Point
MAN	Metropolitan Area Network
FHSS	Frequency Hopping Spread Spectrum
OFDM	Orthogonal Frequency-Division Multiplexing
DSSS	Direct Sequence Spread Spectrum
MAC	Media Access Control
VDSL	Very-high-bit-rate Digital Subscriber Line
PCLP	Physical Layer Convergence Protocol
PDU	Protocol Data Unit
WPA2	Wi-Fi Protected Access
RADIUS	Remote Authentication Dial-In User Service
EAP	Extensible Authentication Protocol
TLD	Top-Level Domain
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
HTML	HyperText Markup Language
CPU	Central Processing Unit

Table des figures

8 Références

8.1 Architecture des réseaux

1. Priscilla Oppenheimer ; Top-Down Network Design - Third Edition
   www.teraits.com/pitagoras/marcio/gpi/bPOppenheimerTopDownNetworkDesign3rde d

2. Intronet-2 2016 - CCNA Routing and Switching : Routing and Switching Essentials
   netacad.com

8.2 WiFi

1. Wikipedia : Wi-Fi
   fr.wikipedia.org/wiki/Wi-Fi

2. IEEE 802.11
   fr.wikipedia.org/wiki/IEEE_802.11

3. Le Standard 802.11
   easytp.cnam.fr/terre/images/WiFi.pdf

4. High Density Wi-Fi Deployment Guide (CVD)
   documentation.meraki.com/MR/Deployment_Guides

5. Location-Aware WLAN Design Considerations
   www.cisco.com

6. IEEE 802.1X
   fr.wikipedia.org/wiki/IEEE_802.1X

7. RADIUS
   fr.wikipedia.org/wiki/Remote_Authentication_Dial-In_User_Service
8. EAP
   fr.wikipedia.org/wiki/Extensible_Authentication_Protocol

8.3 DNS, DNS64 et NAT64

1. Wikipedia - Domain Name System
   fr.wikipedia.org/wiki/Domain_Name_System
2. OpenClassRooms - Service DNS
   openclassrooms.com
3. Commentcamarche.net - Système de nom de domaine
   www.commentcamarche.net
4. Wikipedia - Transition d'IPv4 vers IPv6
   $fr.wikipedia.org/wiki/Transition\_d'IPv4\_vers\_IPv6$
5. Stateful and Stateless NAT64
   www.mplsvpn.info/2011/10/stateful-and-stateless-nat64
6. "Stateless NAT64 is useless"
   blog.ipspace.net/2011/05/stateless-nat64-is-useless
7. Wikipedia - NAT64
   en.wikipedia.org/wiki/NAT64
8. DNSSEC
   http://www-igm.univ-mlv.fr/dr/XPOSE2014/DNSSEC/dns
9. RFC 6147 - DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers
   https://tools.ietf.org/html/rfc6147
10. RFC 6146 - Stateful NAT64 : Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
    http://www.bortzmeyer.org/6146

8.4 Service Web

1. Wikipedia - Service Web
   fr.wikipedia.org/wiki/Service_web
2. Wikipedia - Hypertext Transfer Protocol
   https://fr.wikipedia.org/wiki/Hypertext_Transfer_Protocol