

# Réalisation d'une API de configuration automatique de réseau WiFi maillé sous Linux

BUGNOT Thibaut

22 février 2018

# Table des matières

Introduction	2
<b>1 Objectifs, définitions, contraintes</b>	<b>3</b>
1.1 Introduction aux réseaux wifi . . . . .	3
1.2 La norme 802.11s . . . . .	4
1.3 Adressage et routage . . . . .	6
<b>2 Réseaux sans fils sous Linux</b>	<b>7</b>
2.1 Gestion du réseau sous Linux . . . . .	7
2.2 Création de réseaux 802.11s . . . . .	8
2.3 Détection de réseaux existants et sélection de canal . . . . .	8
<b>3 Adressage et routage</b>	<b>11</b>
3.1 Adressage dans un réseau maillé . . . . .	11
3.2 Routage . . . . .	11
<b>4 Implémentation et architecture logicielle</b>	<b>12</b>

# Introduction

# Chapitre 1

## Objectifs, définitions, contraintes

### 1.1 Introduction aux réseaux wifi

Le wifi, abréviation de wireless fidelity, est un ensemble de protocoles permettant la communication sans fil entre deux appareils en utilisant des ondes radios. Ces protocoles se situent au niveau de la couche d'accès du modèle tcp/ip. La standardisation de cette norme a été initiée l'IEEE<sup>1</sup> en 1990. Cela à aboutit, en 1997, au standart IEEE 802.11 définissant les réseaux locaux sans fils [1]. La norme d'origine prévoyait l'utilisation d'ondes radios dans la bande de fréquences libre entre 2401 et 2495 MHz[2], courramment appelée bande à 2,4 GHz, ou d'infra rouges. Cependant, pour suivre l'évolution des technologies, le standart IEEE 802.11 s'est enrichi afin d'augmenter le débit et d'utiliser la bande de fréquences libre entre 5170 et 5710 MHz. Les standarts IEEE 802.11a et IEEE 802.11b ont donc été définis en 1999, le standart 802.11g et 2003 et le standart 802.11n en 2009.

Depuis sa création, la norme IEEE 802.11 définit 14 cannaux dans la bande 2,4 GHz. Chaque canal à une largeur de 22 MHz et l'écart entre les centres de deux canaux successifs est de 5 MHz<sup>2</sup>. Il en résulte donc un fort recouvrement entre les différents cannaux comme le montre la figure 1.1.

Un réseau wifi est un réseau local découpé en "cellules" appelées BSS<sup>3</sup>. Deux appareils doivent se trouver dans le même BSS pour communiquer entre eux.

---

1. Institute of Electrical and Electronics Engineers

2. Sauf les centres des cannaux 13 et 14 qui sont espacés de 12 MHz

3. Basic Service Set

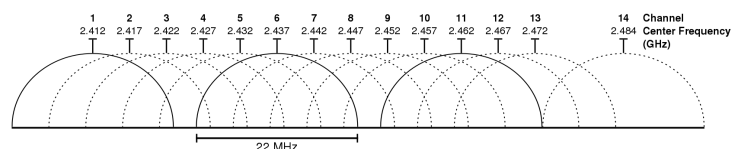


FIGURE 1.1 – Répartition des cannaux dans la bande 2,4 GHz

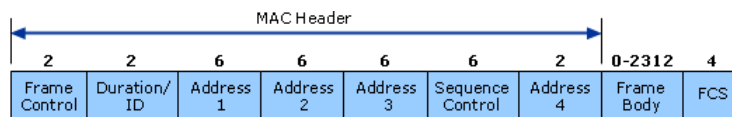


FIGURE 1.2 – Format des trames 802.11

Il existe deux modes de BSS : Le mode Infrastructure et le mode ad-hoc[3]. La plupart des réseaux wifi de particuliers ou d'entreprises sont des réseaux en mode Infrastructure.

Le mode infrastructure est une topologie centralisée. Il se caractérise par le fait que chaque BSS possède une station de base, appelée aussi point d'accès, et que toutes les communications passent nécessairement par le point d'accès de la BSS, et ce même si l'émetteur et le récepteur du message se trouvent dans le même BSS. Un point d'accès peut être relié par un réseau câblé à un ou plusieurs autres points d'accès, étendant ainsi le LAN<sup>4</sup> [4], ou à un routeur pour accéder à un réseau WAN<sup>5</sup>. Le mode ad-hoc, au contraire, est un mode "d'égal à égal". Deux entités au sein du même BSS peuvent communiquer directement.

Comme le montre la figure 1.2[5], le premier champ de l'en-tête wifi est le FCF<sup>6</sup>, permettant d'identifier les trames en fonction de leur rôle. Ainsi, les trames peuvent être de trois types, identifiées par les deux bits en position 3 et 4 du FCF : Management, Contrôle ou Donnée.[6]. Les 4 bits suivants identifient le sous type, et les 8 derniers bits sont des flags. Les trames de données sont utilisées pour transporter des données de plus haut niveau, les trames de contrôles sont utilisées pour les acquittements et les réservations, et les trames de management servent à organiser et maintenir le réseau[7].

Les Beacons frames sont des trames de management particulières qui permettent à un point d'accès de déclarer sa présence aux appareils à proximité. Ils transportent différentes informations comme le SSID<sup>7</sup> du réseau, qui est une chaîne de 2 à 32 caractères, un timestamp permettant de se synchroniser, le canal sur lequel il émet, et d'autres informations.[3].

## 1.2 La norme 802.11s

Comme dit précédemment, le mode infrastructure est actuellement le plus utilisé. Cependant, une de ces limites est que, dans certaines situations, il n'est pas toujours possible de connecter un point d'accès à un switch[8]. En effet, la longueur des câbles ethernet est limitée, ce qui rend difficile le déploiement de points d'accès dans des environnements ouverts.

C'est ce qui fait la force du mode ad-hoc. Chaque appareil peut communiquer avec tous les autres appareils qui sont à portée. De plus, chaque appareil peut relayer le message si le destinataire final n'est pas à portée. Ainsi, dans l'exemple de la figure 1.3, chaque noeud peut communiquer avec n'importe quel autre, à la condition qu'un algorithme de routage s'exécute sur le réseau et que chaque noeud sache quel est le suivant pour atteindre la destination. Ce genre de réseau

4. Local Area Network, ou Réseau local

5. Wide Area Network, ou Réseau étendu

6. Frame Control Field, ou Champ de contrôle de trame

7. Service Set Identifier

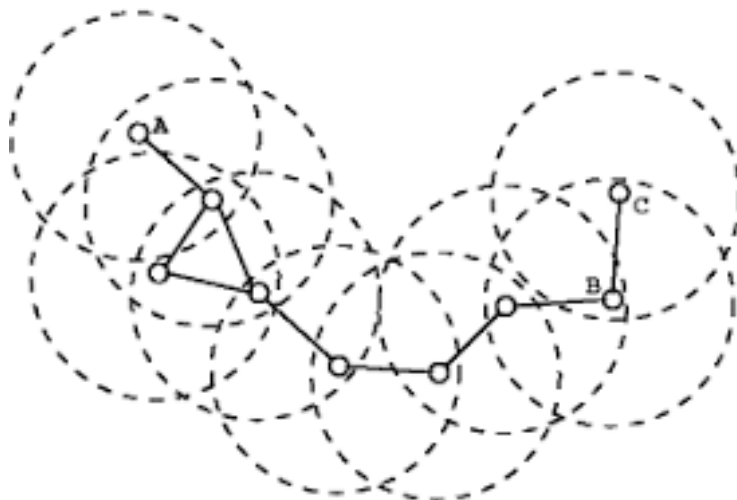


FIGURE 1.3 – Exemple de réseau ad-hoc

est appelé réseau maillé<sup>8</sup>. Le principal avantage de ces réseaux est qu'ils sont très flexibles. On peut les étendre sans avoir à tirer de nouveaux câbles ou à ajouter de nouveaux équipements intermédiaires[8]. De plus, le retrait d'un petit nombre de noeuds ne doit pas empêcher le réseau de fonctionner s'il est possible de trouver des routes alternatives pour les trames.

Le standard 802.11s est un amendement de la norme 802.11, définissant la manière dont les appareils disposant d'une carte réseau sans fils peuvent s'interconnecter pour former un réseau sans fil maillé. L'IEEE a commencé à travailler sur ce standard en 2003 et celui-ci a été adopté en 2006. Pour faciliter l'interopérabilité, un réseau 802.11s est vu de l'extérieur comme un unique segment ethernet. Pour permettre la retransmission des informations d'un noeud à l'autre, la norme 802.11s étend l'en-tête 802.11 classique avec un en-tête mesh comme montré dans la figure 1.4[7].

Les 4 champs d'adresses de l'en-tête 802.11 sont utilisés, puisqu'il faut à chaque transmission du message donner l'adresse du noeud qui a effectué la transmission, celle du prochain noeud, celle du destinataire final et celle de l'expéditeur originel. Dans certains cas plus complexes, il est nécessaire d'ajouter des adresses supplémentaires, ce qui explique que l'en-tête mesh comporte un champ optionel d'extention d'adresses. C'est le cas par exemple si l'émetteur et/ou le destinataire, ne se trouvent pas dans le réseau mesh, mais que la trame va traverser un réseau mesh. Parmi les autres valeurs ajoutées, le TTL<sup>9</sup> et le Mesh sequence number<sup>10</sup> permettent d'éviter les boucles infinies qui risqueraient de saturer le réseau.

8. Mesh Network en anglais

9. Nombre de fois maximal que peut être relayée une trame avant d'être abandonnée, cette valeur est décrétementée à chaque saut

10. nombre identifiant de manière unique une trame

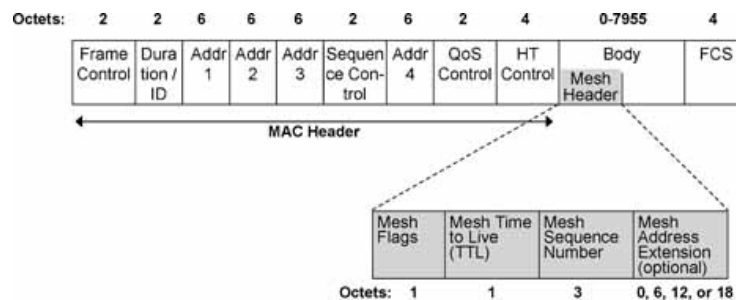


FIGURE 1.4 – Format des trames 802.11s

### 1.3 Adressage et routage

Dans un réseau TCP/IP, chaque noeud doit disposer de deux adresses. Chacune d'elles permet de l'identifier, en théorie, de manière unique. La première est l'adresse MAC, une adresse sur 48 bits, utilisée pour identifier les noeuds dans les protocoles de la couche d'accès du modèle TCP/IP. Cette adresse permet à une trame de voyager sur un LAN jusqu'à sa destination, mais sera changée à chaque fois que le paquet passe par un routeur. La deuxième est l'adresse IP, une adresse sur 32 bits qui est utilisée par le protocole IP, qui est un protocole de la couche réseau du modèle TCP/IP. Cette adresse est inchangée d'un bout de la transmission à l'autre <sup>11</sup>.

L'adresse MAC est attribuée à une carte réseau par le constructeur. Ainsi, nous avons la garantie que chaque appareil possède une adresse MAC unique. L'adresse IP doit également être unique mais, contrairement à l'adresse MAC, elle n'est pas enregistrée dans la carte réseau par le constructeur car toutes les adresses IP identifiant les appareils d'un même LAN doivent avoir le même préfixe. Il existe des protocoles permettant d'affecter automatiquement des adresses IP à des appareils sans avoir besoin de recourir à une intervention humaine. Le protocole majoritairement utilisé est DHCP <sup>12</sup>. Ce protocole nécessite qu'un serveur dispose d'une liste d'adresses IP disponibles qu'il va affecter à chaque noeuds du réseau sur demande de ces derniers[9]. Néanmoins, le recours à un serveur central d'adresses IP amoindrit les avantages à l'utilisation d'une infrastructure décentralisée tel qu'un un réseau maillé.

Dans un réseau maillé, il est aussi nécessaire de prévoir le routage des trames. La norme 802.11s définit également le protocole HWMP <sup>13</sup> comme protocole de routage pour les réseaux wifi maillés. Contrairement à la majorité des protocoles de routages, HWMP ne se base pas sur les adresses IP, mais sur les adresses MAC, puisque le but est d'aiguiller les trames au sein d'un même LAN. Il s'agit d'un protocole de routage à vecteur distance puisque les noeuds n'ont pas connaissance de l'intégralité de la topologie du réseau mais uniquement des noeuds qui le constituent et de la "distance" de chacun d'eux [10].

11. en l'absence de mécanismes de traduction d'adresse (NAT)

12. Dynamic Host Configuration Protocol

13. Hybrid Wireless Mesh Protocol

## Chapitre 2

# Réseaux sans fils sous Linux

### 2.1 Gestion du réseau sous Linux

Une importante partie du projet consiste à pouvoir communiquer avec les interfaces sans fils dont disposent les appareils. En effet, il est nécessaire d’une part, de récupérer des informations à propos de ces dernières et d’autre part, de les configurer pour arriver à les utiliser de la manière que nous le souhaitons. Pour gérer les interfaces sans fils, il est important de bien distinguer deux niveaux : Les cartes réseaux<sup>1</sup>, qui existent physiquement, et les interfaces qui pourraient être qualifiées de “logiques” qui utilisent ces cartes réseaux et sont utilisées pour envoyer et recevoir des données. C’est aux interfaces que l’on associe un type (Point d’accès, client, noeud mesh, monitor, ...) déterminant son mode de fonctionnement. Une seule carte réseau peut être utilisée par plusieurs interfaces.

Historiquement, sous linux, la communication avec les interfaces se faisait avec des appels systèmes `ioctl`<sup>2</sup>. Des outils permettant de manipuler les interfaces en utilisant cette méthode sont depuis longtemps fournis avec les distributions linux. C’est le cas par exemple du package `net-tools`, incluant le programme `ifconfig`, et permettant de manipuler les interfaces (état, informations d’adressages) ou de `wireless-tools`, incluant le programme `iwconfig`, permettant de manipuler plus précisément les interfaces sans fils.

Cependant, depuis 2007, il existe un autre moyen de manipuler les interfaces. En effet, se développe **netlink**, une famille de socket ayant pour but de faire communiquer les processus entre eux. Cela permet, entre autre, de faire communiquer un processus utilisateur avec un processus du noyau linux. La librairie `libnl` implémente les pré-requis fondamentaux pour utiliser le protocole `netlink`. Cependant, celle-ci se veut minimaliste. C’est pourquoi elle est complétée par 3 API : `libnl-route`, `libnl-genl` et `libnl-nf`[11]. Des outils de configuration d’interfaces utilisent ces nouveaux moyens. C’est le cas de la suite d’outils `iproute` pour contrôler les interfaces et de `iw` pour contrôler plus précisément les interfaces sans fils. Nous utiliserons `netlink` dans notre code.

L’API que nous utiliserons principalement pour gérer les interfaces est `libnl-`

---

1. généralement abrégées **wiphy**, pour Wireless PHYsical device

2. Abréviation de Input Output ConTroL, il s’agit d’une fonction permettant de manipuler des fichiers spéciaux



genl. Celle ci permet, grace à nl80211, un en-tête netlink, d'envoyer des messages permettant de contrôler les interfaces wifi. Les commandes qu'il est possible d'envoyer sont définies dans l'énumération nl80211\_commands dans le fichier nl80211.h. En créant des messages netlink avec ces commandes, il nous est possible, entre autre, de récupérer les informations sur les cartes réseaux connectés (NL80211\_CMD\_GET\_WIPHY), celles sur les différentes interfaces (NL80211\_CMD\_GET\_INTERFACE), de choisir la fréquence d'émission de de réception de la carte réseau (NL80211\_CMD\_SET\_WIPHY), de créer une interface sur une carte réseau (NL80211\_CMD\_NEW\_INTERFACE) ou de changer le type d'une interface (NL80211\_CMD\_SET\_INTERFACE)

Les commandes transmissent dans un message netlink peuvent avoir besoin d'un ou plusieurs attributs. La liste de tous les attributs existants dans le cadre de la gestion des interfaces sans fils est défini dans l'énumération nl80211\_attrs dans le fichier nl80211.h.

L'API libnl-genl dispose déjà de fonction permettant de créer des socket netlink, des messages netlink, d'y ajouter des attributs et de l'envoyer sur le socket. Selon la commande donnée, il se peut que le noyau réponde en renvoyant un ou plusieurs messages netlink contenant des informations. C'est le cas lorsque l'on utilise par exemple la commande NL80211\_CMD\_GET\_INTERFACE. Le message renvoyé contiendra alors les informations sur les interfaces. Il est alors nécessaire d'analyser le message pour en extraire les informations souhaitée. Dans tous les cas, Le dernier message renvoyé par le noyau sera un message d'acquiescement ou, en cas de problème, un message d'erreur. Après avoir envoyer un message netlink, il est donc nécessaire d'écouter sur le socket jusqu'à la réception d'un de ces deux messages.

## 2.2 Création de réseaux 802.11s

## 2.3 Détection de réseaux existants et sélection de canal

Un des objectif du projet consiste à détecter les réseaux wifi mesh déjà existant et, si il n'en existe aucun, à choisir le meilleur canal, c'est à dire le moins encombré, pour en créer un nouveau. Pour cela, il est nécessaire d'être en mesure de scanner les réseaux déjà existants. A cette fin, les beacons frames décrites chapitre 1, partie 1 sont particulièrement utiles. En effet, elles sont envoyées à intervalles réguliers par les points d'accès, mais aussi par tous les noeuds d'un réseau mesh. Ces trames contiennent en effet de nombreuses informations à propos du réseau. Ces informations n'étant pas toujours les mêmes en fonction du contexte, elle se présentent, pour la plupart, sous la forme tag-longueur-valeurs. C'est à dire qu'une fois les différents en-têtes enlevées et les informations fixes (dont la longueur est connue) écartées, le premier octet est un tag, c'est à dire un nombre identifiant l'information qui suit, le deuxième octet nous donne la longueur de l'information, nottons la n, et les n octets suivants sont l'information. L'octet suivant est à nouveau un tag, suivi d'une longueur, ect.

Prenons comme exemple la figure 2.1, qui est un exemple de beacon frame obtenu avec wireshark. Les octets surlignées et ceux qui les précèdent constituent l'en-tête et ne nous intéressent pas. Les octets encadré en jaune sont des

```

00 00 80 00 00 00 ff ff ff ff ff ff 68 a3 78 d2
07 ec 68 a3 78 d2 07 ec 10 ea 5f 81 3c 59 dd 00
00 00 60 00 11 04 00 0b 66 72 65 65 62 6f 78 48
44 63 63 01 08 82 84 8b 96 2c 0c 12 18 03 01 01
05 04 00 02 00 00 2a 01 04 32 05 24 30 48 60 6c
30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00
00 0f ac 02 0c 00 2d 1a ac 00 03 ff ff ff 00 01

```

FIGURE 2.1 – Un exemple de beacon frame

informations “fixes”, dans le sens où elles sont toujours présentes dans une beacon frame. Il s’agit d’un time stamp, du beacon interval<sup>3</sup> et quelques flags. Le reste du message illustre le fonctionnement décrit plus haut. Ainsi, le premier octet dans le cadre rouge est 00, ce qui indique que l’information qui va suivre est le SSID<sup>4</sup>. L’octet suivant est 0b<sup>5</sup> indiquant que le SSID est donné sur 11 octets. Les 11 octets suivants donnent le SSID au format ASCII. Le tag dans le cadre vert est 01, indiquant que l’information à suivre est les débits supportés, et la longueur de ce champ est de 8 octets. Les 8 octets suivants indiquent donc chacun un débit. Dernier exemple, dans le cadre bleu, le tag est 03, indiquant que l’information à venir est le canal utilisé, la longueur de cet information est de 01 octet et l’information est 01, indiquant que ce point d’accès fonctionne sur le canal 1, à la fréquence 1412<sup>6</sup>.

Encore une fois, l’API libnl-genl nous fournit les outils pour demander au noyau linux de faire un scan, via les commandes NL80211\_CMD\_GET\_SCAN et NL80211\_CMD\_TRIGGER\_SCAN à envoyer dans un message netlink. Cela nous permet de récupérer toutes les informations sur les différents réseaux contenus dans les beacon frames. Cependant, après une phase de tests, la conclusion empirique a été que ce scan ne détectait pas toujours tous les réseaux wifi mesh. Nous avons donc pris la décision, dans le but d’avoir les résultats les plus complets possibles, d’implémenter notre propre scanner pour exploiter nous même les beacon frames.

TCPdump est un programme généralement inclus dans les distributions linux permettant de “sniffer” des paquets sur une interface réseau. Ce programme se base sur libpcap[12], une bibliothèque permettant de capturer des paquets. C’est cette bibliothèque que nous utiliserons. Elle permet de récupérer les messages tels qu’ils ont été capturés par l’interface. Il est ensuite possible d’effectuer toutes les opérations souhaitées sur eux.

Pour être en mesure de capter les beacon frames, il est nécessaire de régler une interface en mode monitor. De plus, puisqu’il existe 14 canaux, il est nécessaire de passer de l’un à l’autre pour tous les scanner. Ces deux opérations sont possibles avec la bibliothèque libnl décrite chapitre 2, partie 1. La méthode que nous utiliserons est donc la suivante : nous paramétrons la carte réseau associée à une interface en mode monitor sur une fréquence, puis nous utilisons les fonctions de libpcap pour écouter sur l’interface pendant 3 secondes. Pendant ce temps, à chaque réception d’une trame, nous vérifions qu’il s’agit d’une beacon frame en analysant son type. Si c’est le cas, on analyse chaque information qu’elle

3. L’intervalle de temps entre l’envoi de deux beacon frames

4. nom du réseau wifi

5. Il s’agit d’une valeur en hexadécimal valant 11 en décimal

6. voir figure 1.1

contient en recherchant les tags 0, 3, 113 et 114 indiquant respectivement le SSID, le canal de fonctionnement, la configuration mesh et le MeshId. Bien sur, seuls les beacon frames indiquant un réseau mesh possèdent les deux derniers tags. En outre, le tag 00 est toujours présent mais dans le cas d'une beacon frame indiquant un réseau mesh, sa longueur est de 0 bits, due au fait qu'un réseau mesh n'as pas de SSID.

Une fois le scan répété sur chacun des 14 canaux, nous avons donc deux listes : Une liste des réseaux "normaux" et une liste des réseaux mesh. De plus, nous pouvons calculer simplement l'occupation de chaque fréquence, et si besoin trouver la moins encombrée. Cependant, comme évoqué précédemment, et comme le montre bien la figure 1.1, les canaux se superposent. Il n'est pas rare qu'en écoutant sur un canal, on reçoive un message envoyé sur un autre canal voisin. Ainsi, lors de la sélection de canal, il peut être judicieux d'exclure non seulement le dit canal, mais aussi ses voisins.

## Chapitre 3

# Adressage et routage

### 3.1 Adressage dans un réseau maillé

### 3.2 Routage

Plus précisément, le protocole HWMP dispose de deux modes de fonctionnement : “on demand” et “proactive tree building”. Le second nécessite qu’un noeud soit désigné comme noeud racine[10].

Avec le mode “on demand”, chaque fois qu’un noeud a besoin de connaître le chemin vers un autre noeud, il envoie un paquet “route request (RREQ)” en broadcast, en identifiant le noeud de destination. Le paquet RREQ contient aussi un champ métrique initialisé à 0. Chaque noeud intermédiaire va recevoir le paquet RREQ, éventuellement en plusieurs exemplaires. Si le paquet RREQ a une métrique plus faible que celle déjà connue, le noeud intermédiaire met à jour sa table de routage et le retransmet après avoir augmenté la métrique. Lorsque le paquet atteint le noeud de destination, ce dernier répond avec un paquet “Route Reply (RREP)” en unicast vers la source. Ainsi, tous les noeuds entre la destination et la source connaissent une route vers ces deux points [10].

## Chapitre 4

# Implémentation et architecture logicielle

# Bibliographie

- [1] Michel Terré. Wifi, mars 2007.  
<http://easytp.cnam.fr/terre/images/WiFi.pdf>.
- [2] Canaux et fréquences wifi 2.4 ghz et 5 ghz, janvier 2015.  
<https://infos-reseau.com/canaux-et-frequences-wifi-2-4-ghz-et-5-ghz/>.
- [3] F.Nolot. Les réseaux sans-fil : Ieee 802.11.  
<http://www.nolot.eu/Download/Cours/reseaux/m1info/ProtoAv-Cours7-Wifi.pdf>.
- [4] James F. Kurose ; Keith W. Ross. Ieee 802.11 lans, 1999.  
[https://www.net.t-labs.tu-berlin.de/teaching/computer\\_networking/05.07.htm](https://www.net.t-labs.tu-berlin.de/teaching/computer_networking/05.07.htm).
- [5] How 802.11 wireless works, Mars 2003.  
[https://technet.microsoft.com/en-us/library/cc757419\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc757419(v=ws.10).aspx).
- [6] Nicolas Darchis. 802.11 frames : A starter guide to learn wireless sniffer traces, octobre 2010.  
<http://www.nolot.eu/Download/Cours/reseaux/m1info/ProtoAv-Cours7-Wifi.pdf>.
- [7] Guido Hiertz ; Dee Denteneer ; Sebastian Max ; Rakesh Taori ; Javier Cardona ; Lars Berlemann ; Bernhard Walke. Ieee 802.11s : The wlan mesh standard, fevrier 2010.  
<http://ieeexplore.ieee.org/document/5416357/>.
- [8] Jerome Henry. 802.11s mesh networking, novembre 2011.  
[https://www.cwnp.com/uploads/802-11s\\_mesh\\_networking\\_v1-0.pdf](https://www.cwnp.com/uploads/802-11s_mesh_networking_v1-0.pdf).
- [9] R. Droms. Dynamic host configuration protocol, mars 1997.  
<https://tools.ietf.org/html/rfc2131>.
- [10] Avinash Joshi ; Hrishikesh Gossain ; Jorjeta Jetcheva ; Malik Audeh ; Michael Bahr ; Jan Kruys ; Azman-Osman Lim ; Shah Rahman ; Joseph Kim ; Steve Conner ; Guenael Strutt ; Hang Liu ; Susan Hares. Hwmp protocol specification, novembre 2006.  
doc. : IEEE 802.11-06/1778r1.
- [11] Netlink protocol library suite (libnl).  
<http://www.infradead.org/~tgr/libnl/>.
- [12] Tcpdump et libpcap.  
<http://www.tcpdump.org/>.