**Réseaux IP**

Project Intégré

# Etude Préliminaire


Ecrit par

Bryan Perdrizat

Groupe 4

Sous la direction de

**François Buntschu**



Haute école d'ingénierie et d'architecture Fribourg

Hochschule für Technik und Architektur Freiburg

Télécommunication, filière réseaux et sécurité

HAUTE ÉCOLE D'INGÉNIÉRIE ET D'ARCHITECTURE

Fribourg, Suisse


23 mars, Semestre de printemps 2018

# Table des matières

# 1 Introduction

Pour réaliser l'objectif pour lequel nous avons été mandaté, à savoir fournir un accès internet à haut débit à l'entreprise **Fri-Learning & Co**, il nous a été demandé d'étudier les technologies et les thématiques qui seront utilisé pour mettre en place le cahier des charges suivant :

a. Utilisation native de IPv4 et IPv6.
b. Attribution dynamique des adresses IPv4 et IPv6.
c. Connexion à Internet à haut débit avec les deux protocoles cités en (a) pour le client (Attention Berlin n'est qu'en IPv6 et doit pouvoir se connecter sur des sites IPv4 à NAT64/DNS64).
d. Routage dynamique entre les sites de Fribourg et Berlin (fournisseur d'accès).
e. Routage dynamique "privé" entre les sites de Fribourg et Berlin (client).
f. Mise en place d'un cloud de type OpenStack dans les datacenters du fournisseur d'accès, réparti entre le site de Fribourg et celui de Berlin, avec liaison de couche 2 entre les datacenters au travers du nuage L3.
g. Gestion du domaine DNS fri-learning.ch sur une machine virtuelle dans le cloud.
h. Mise en place d'un serveur web www.fri-learning.ch comme vitrine de l'entreprise sur une machine virtuelle dans le cloud (une page d'accueil statique pour démontrer qu'il est accessible est suffisante).
i. Spécification de la structure du LAN et de l'accès sans fil au sein des bâtiments du siège principal du client.
j. Spécification de l'architecture réseau de l'ISP sur son site de Berlin & Fribourg (datacenter, sécurité et connexion à Internet).

Ce document présentera les points suivant, en donnant les spécifications et les références associées, le contexte et un exemple d'utilisation.

— Architecture réseau
— Communication sans-fils / Wireless (WiFi)
— Serveur Web, DHCP

# 2 Architecture de réseau

L'architecture réseau représente une topologie logique, selon laquel les équipements réseaux seront interconnecté. Afin qu'une architecture sois le plus optimal possible, la liste des points — non-exhaustifs — suivants sont à considérer.

## 2.1 Besoin d'un réseau

**Redondance :** Pour que l'architecture résiste au mieux aux imprévus, avoir des connexions et des équipements redondants permet d'éviter des pannes de plusieurs minutes à plusieurs heures en fonctions de la gravité du problème.

**Connectivité/Sécurité :** Aujourd'hui de plus en plus d'appareils sont connectés via une connexion sans-fil, tout en voulant accéder à tout types de services et ce, depuis n'importe où. Plus le nombre d'accès à un réseau est grand, plus les restrictions doivent être maitrisées ; quel informations ? Par qui ? Par quels appareils ?

**Scalable :** Il n'est pas toujours possible de prévoir la charge que devra supporter un réseau des années après l'avoir implémenté, un réseau bien optimisé devrait pouvoir être mis à niveau en changeant le minimum d'éléments possible, et surtout sans affecter le fonctionnement des autres parties de l'architecture.

**Résilient :** Malgré la redondance de plusieurs équipements et connexions, une architecture n'est pas résiliente pour autant. Un réseau correctement configuré doit être capable de détecter une panne, et réagir le plus rapidement possible en conséquence, jusqu'à pouvoir remettre les points défectueux sur pied.

Bien que cette étude préliminaire doit être exempte d'objectivité, seul quelques architectures de réseau seront présentée, en particulier le *Hierarchical Network Design* qui s'impose comme le modèle le plus utilisé en étant un véritable fer de lance des technologies *Cisco*.

## 2.2 Hierarchical Network Design

C'est l'architecture que promeut *Cisco*, elle peut autant être utilisée pour des réseaux LAN que WAN.L'architecture se compose de 3 couches distinctes qui rendent le modèle à la fois robuste et modulable.

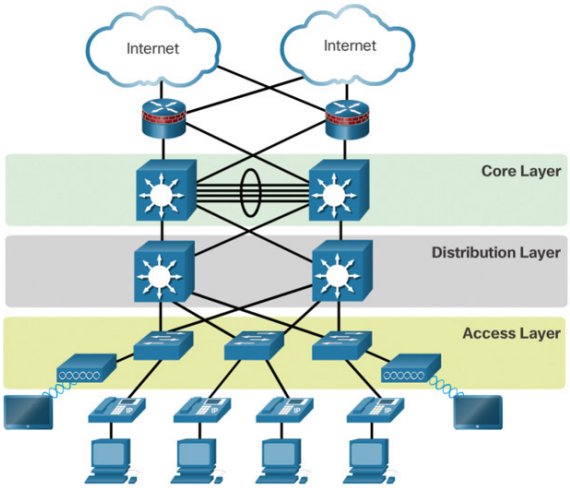


*FIGURE 1 – Architecture hiérarchique*

### 2.2.1 Access Layer

La "couche d'accès" est la plus proches des stations des utlisateurs, elle est principalement conçue d'équipements réseaux de couche 2 qui offrent une liaison aux couches supérieurs. Les stations des utilisateurs, les "hot spots" Wifi, ou n'importe quels autres appareils auxquels les utilisateurs doivent avoir acccès, y sont connectés.

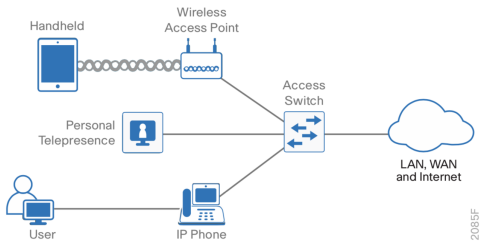


*FIGURE 2 – Représentation de la couche d'accès*

C'est une couche cruciale qui doit avant tout supporter des pics de traffic d'un grand nombre d'appareils connectés simultanément. C'est aussi sa responsabilité de séparer les groupes de terminaux en réseaux logiques. Comme précédemment mentionné dans le points **Connectivité/Sécurité** de la Section 2.1, l'architecture se doit de restreindre l'accès uniquement aux appareils autorisés, c'est aussi une des missions de cette couche.

### 2.2.2 Distribution Layer

La "couche de distribution" est la couche de routage directement reliée à la couche d'accès grâce à des équipements réseaux de couche 3 (du modèle OSI).

En tant que couche intermédiaire, les routeurs doivent fournir une interconnection entre les différents protocoles de routages et protocoles routés qui traversent l'architecture, de plus pour améliorer les performances de routage, les noeuds de la couche sous-jacente peuvent être routés statiquement, tandis que le routage dynamique n'est uniquement utilisé qu'entre équipement du *Distribution Layer*. Enfin, elle doit pouvoir fournir un haut niveau d'abstraction au *Core Layer* en dissimulant la topologie du *Access Layer* afin que le routage ne soit exécuter que sur le *Distribution Layer*.

### 2.2.3 Core Layer

Le *Core Layer* est la couche supérieure du *Hierarchical Network Design*, cette couche est principalement responsable de l'interconnectivité entre le réseau LAN et internet ou à d'autre site d'une même entité.

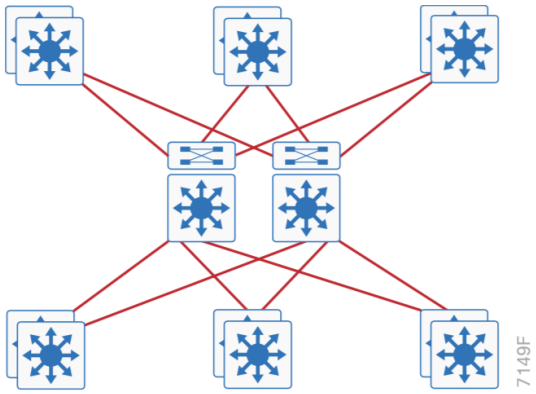


*FIGURE 3 – Le Core Layer centralise les flux*

De ce fait, les routeurs du *Core Layer* doivent être configurés et optimisés pour maximiser le nombre de paquets traités à la seconde, en utilisant le mode de routage *Cut-Through* par exemple ou encore en évitant de configurer des systèmes de filtrage sur ces routeurs.

Comme il s'agit d'un point sensible de l'architecture, les routeurs se doivent d'être redondant pour assurer la stabilité de ce noeud du réseau.

### 2.2.4 Two-Tier Design (Collapsed Core)

Sur des réseaux de petite voir moyenne taille, la séparation en 3 parties distinctes de l'architecture peut être superflue, il existe pour ça un modèle qui regroupe le *Distribution Layer* et *Core Layer* en une couche appelée *Collapsed Core Layer*.

Ce regroupement permet le plus souvent d'économiser des coûts mais aussi du temps de maintenances; c'est pariculièrment adapté à des réseaux qui vont peu ou pas s'agrandir.

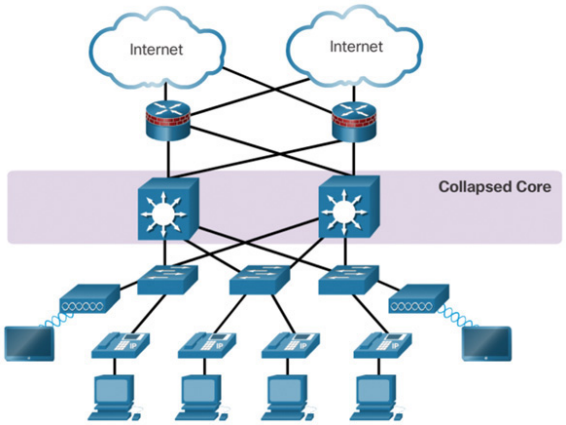


*FIGURE 4 – L'architecture hiérarchique à 2 couches*

## 2.3 Flat Network Design

Le *Flat Network* contrairement au *Hierarchical Network* ne comporte qu'une seule couche qui assume l'entière responsabilité des 3 couches d'une architecture hiérarchique. Ce qui rend le réseau facile à administrer, tant que la taille du réseau reste modeste, mais limite l'expansion de ce dernier. De manière générale les équipements qui composent le réseau sont arrangés en boucle.

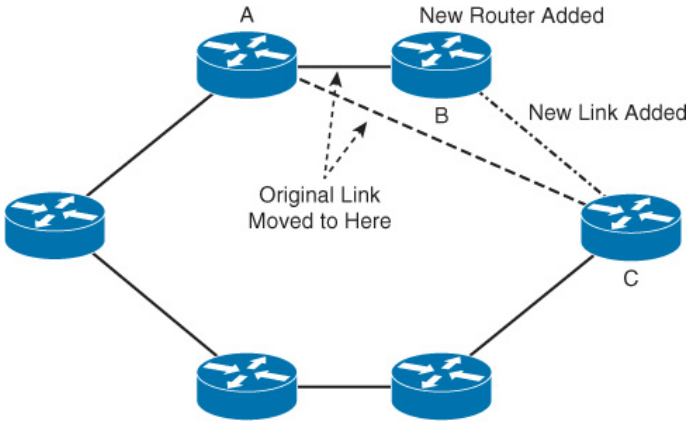


*FIGURE 5 – Une exemple d'architecture en boucle et les répercussions de l'ajout d'un noeud*

## 2.4 Mesh Network Design

Le réseau maillé ou *Mesh Network* tient plus d'une version alternative du *Flat Network* que d'une architecture à part entière. Ici, chaque routeur est connecté à tout les autres dans ça version complète — on parle alors de *Full-Mesh* — ou seulement à quelqu'uns (*Partial-Mesh*).

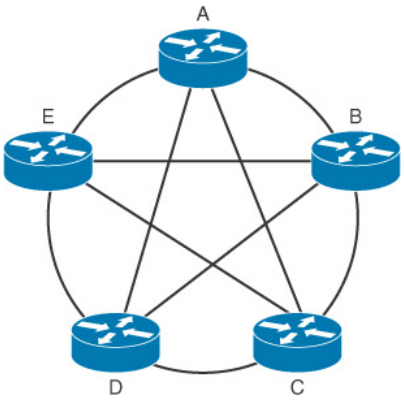


*FIGURE 6 – Un réseau maillé complet (Full-Mesh)*

La redondance des connexions procurent une grande stabilitée à ce type d'architec-

ture mais une fois de plus rend l'évolution et l'agrandissement compliqué. A ajouter que plus le nombre de routeurs augmentent plus la quantité de bande passante utilisée par les protocoles de routage est grande, ce qui fait concorder le type de connexion filaire et le *Throught-put* des équipements avec la taille du réseau.

# 3 Communication sans-fil / Wireless (WiFi)

## 3.1 Généralité

Apparu au début des années 2000, le "WiFi" désigne l'ensemble des protocoles et standards contenus dans la norme **IEEE 802.11**, qui définit les moyens d'accès aux couches 1 et 2 du modèle OSI, pour des équipements réseaux sans-fils. Cette technologie utilise les ondes électro-magnétiques — utilisant l'air comme médium — afin de transmettre des données. Dés lors, les connexions à un points d'accès sans-fil sont devenus légion chez les particuliers ainsi que sur les lieux de travail du monde entier.

## 3.2 Méthode d'accès

Comme mentionné précédemment, on retrouve cette technologie pricipalement sur des équipements réseaux utilisés comme "hot spots" ou sur des appareils mobiles tel que des ordinateurs portables. Les "hot spots" servent de points d'accès un réseau filiaire LAN ou WAN on parle dés lors d'*Access Points (AP)*.

Afin de couvir une plus grande zone, un équipements peut être utilisé en mode *Repeter* afin de propager les données. Enfin, il existe un mode *Ad-Hoc*, qui permet de relier des équipements qui sont à portée radio, ce qui serait semblable d'une certaine manière à relier les stations entre elles au moyen d'un câble.

## 3.3 IEEE 802.11

Le standards **IEEE 802.11** est apparu à la fin des années 1990 pour définir les couches PHY, LLC et MAC du modèle IEEE — qui représentent les couches 1 et

2 du modèle OSI — d'un réseau sans-fils. La particulartié de cette norme est qu'elle offre un modèle standardisé pour la couche de liaison ce qui permet de redéfinir les standards pour la couche physique sans impliquer les couches suppérieurs. Par exemple, la révision **IEEE 802.11a** fait état d'une modification de la couche physique de la norme **IEEE 802.11**.

### 3.3.1 Performance

Il existe à ce jour de nombreuses révisions de la norme originelle, certaine d'entre elles ne concernent que la couche 2 d'autres au contraire sont des améliorations de la couche physique. Le tableau récapitualif (Tableau 1) présente les dernières normes en terme de performance ainsi que les prochaines révisions attenduent.

| Norme | Date | Fréquence (GHz) | Bande Passante (MHz) | Débit max. (Mbps) | Modulation | Portée Ext./Int. (m) |
|---|---|---|---|---|---|---|
| 802.11 | 1997 | 2.4 | 22 | 2 | FHSS | 20/100 |
| a | 1999 | 5 | 20 | 54 | OFDM | 35/120 |
| b | 1999 | 2.4 | 20 | 11 | DSSS | 35/140 |
| g | 2003 | 2.4 | 20 | 54 | DSSS | 38/140 |
| n | 2009 | 2.4/5 | 20/40 | 150 | OFDM | 70/250 |
| ad | 2012 | 60 | 2160 | 6750 | OFDM | 35/ |
| ac | 2013 | 5 | 20/40/80/160 | 8667 | OFDM | 35/ |
| ah | 2017 | 0.9 | 1–16 | 8 | OFDM | 100/ |
| ax | 2019 | 2.4/5 | 20/40/80/160 | 1200 | OFDM | 35/ |
| ay | 2019 | 60 | 2160 | 20000–40000 | OFDM | 35/300–500 |

*TABLE 1 – Tableau récapitulatif des versions de la norme IEEE 802.11*

### 3.3.2 Modulation

Parmis les méthodes de modulation, celle qui a su s'imposer au fil des années est le OFDM, l'un de ces plus grands avantages est le fait de pouvoir créer plusieurs sous-canaux et ainsi pouvoir exploiter d'avantage la taille de la bande passante. L'OFDM désigne une vaste famille schéma de modulation numérique tel que le BPSK, QPSK ou encore le QAM.

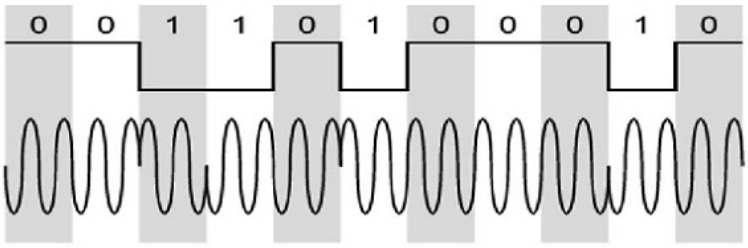


*FIGURE 7 – Un signal modulé grâce au mécanisme BPSK*

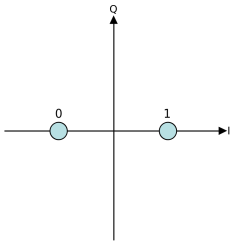


*FIGURE 8 – BPSK*

**BPSK :** Dans le *Binary Phase Shift Keying*, la phase d'un signal à amplitude constante est alternée entre deux valeurs, qui représentent le 1 et le 0. De manière générale les deux phases sont inversées de 180°.

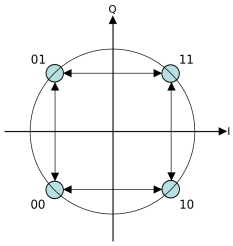


*FIGURE 9 – QPSK*

**QPSK :** Avec deux fois l'efficience du BPSK pour la même bande passante, le *Quadrature Phase Shift Keying* permet de transmettre 2 bits grâce à une seule modulation, car la phase du signal peut prendre une des quatre phases disponibles correspondant à une paire unique de bits (00, 01, 10, 11).

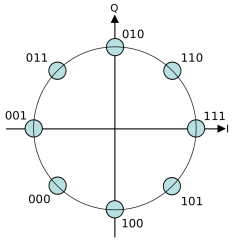


*FIGURE 10 – MPSK*

**MPSK :** Successeur du QPSK, le *M-ary Phase Shift Keying* exploite au mieux le changement de phase, il est utilisé de manière générale avec 8 différentes phases ; un nombre de phase supérieur 8 est rarement exploité car çela demande trop de puissance.

**QAM :** Dans les points précédents, l'amplitude du signal est toujours resté constante. En permetant à l'amplitude de varier avec la phase, le *Quadrature Amplitude Modulation* est devenu le schéma de modulation le plus performant. Il existe différente version du QAM, allant d'une constellation de 8 points à 1024.

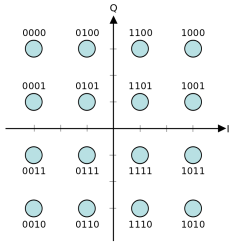


*FIGURE 11 – 16-QAM*

## 3.4 Wireless LAN Design (WLAN)

Toujours dans un souci de planification et de conception, une réseau sans-fils doit pouvoir répondre aux mêmes besoins qu'un réseau filaire comme exposé à la Section 2.1.

### 3.4.1 WLAN Classic Network

Dans sa forme traditionnelle, un WLAN est composé d'un ou plusieurs APs qui sont directement connectés à internet au travers d'une connexion filaire.

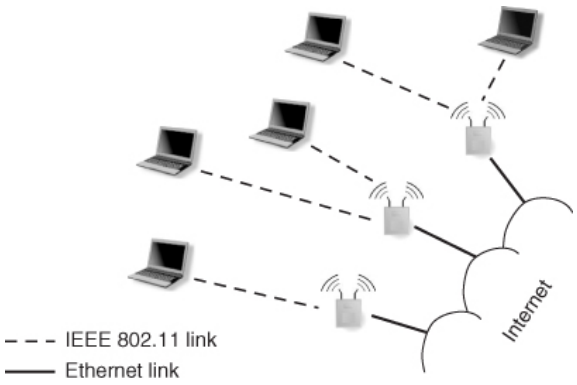


*FIGURE 12 – Une réseau WLAN typique*

Comme la portée des APs est limitée à plusieurs centaines de mètres en extérieur et beaucoup moins en intérieurs, la couverture d'une grande zone peut devenir coûteuses en matériel et en câblage. C'est là qu'intervient une architecture maillée dîtes *Mesh Network*.

### 3.4.2 Mesh Network

Le *Mesh Network* à la particulartié d'être composé de *Mesh Stations* qui peuvent établir des connexions inter-routeurs en plus des connexions aux stations clientes. Ceci permet augmenter la robustesse grâce aux nombreuses liaisons redondantes et d'étendre la couverture du réseau considérablement tout en conservant un nombre raisonnable de d'équipements cablés au réseau LAN.

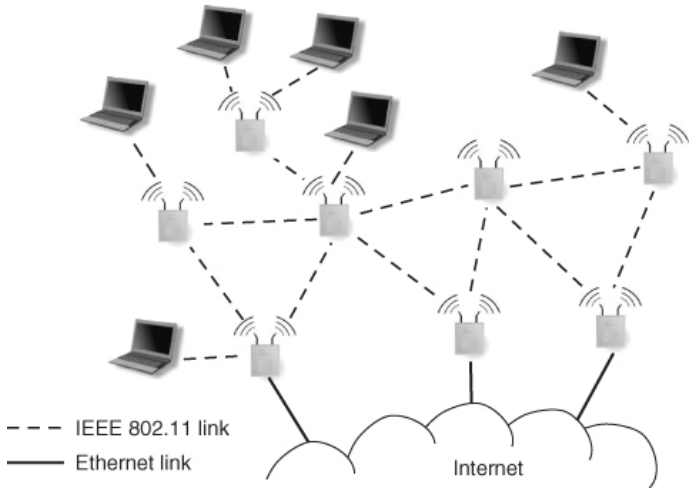


*FIGURE 13 – Un exemple de WLAN maillé*

## 3.5 Sécurité

La mobilité qu'offre un réseau WLAN est sans limite mais cette liberté est à double tranchant. Un réseau sans-fils n'offre aucune protection physique en comparaison à un réseau cablé.

### 3.5.1 Problématique

Comme les données sont transmises au moyen d'ondes à hautes fréquences — entre 1 GHz et 5 GHz — il est difficile de contenir les ondes au sein d'un périmètre, ce qui peut exposer les réseaux et les transmissions aux attaques d'un terminal situé en dehors des limites d'un bâtiment.

L'une des solutions est d'assumer que ces informations sont accessibles à tous et d'essayer de le chiffrer afin que personne ne puisse déchiffrer les données transmises. Depuis lors des mécanismes de protections ont été mise en place : WEP, WPA puis WPA2 et bientôt WPA3, chaque protocole patche les failles de securités du précédent. Néanmoins, Il existe des protocoles — propriétaires pour certain — visant à augmenter la sécurité.

### 3.5.2 EAP

L'*Extension Authentification Protocole* est un protocoles ratifié dans les **RFC 3748/5247**, qui permet à une station de négocier une authentification avec un serveur mandataire au travers d'un AP. L'EAP existe sous plusieurs versions comme par exemple : EAP-TLS ou encore EAP-TTLS ; ce dernier incorpore une authentification par nom d'utilsateur/mots de passe.

# 4 Serveur & services

Le principe même d'un serveur (informatique) est de répondre à des requêtes normalisées provenant d'autres terminaux informatiques. On parle de relation client-serveur.

## 4.1 Serveur DHCP

Le *Dynamic Host Configuration Protocol* (DHCP) défini en 1993 pour la première fois dans la **RFC 1531**, supplante le protocole BOOTP (*Bootstrap Protocol*) défini dans la RFC 951.

Le BOOTP permet de fournir à une station en démarrage, des informations — tel qu'une adresse IP, un masque de sous-réseau, la passerelle par défaut, etc…, pour se connecter à un serveur de démarrage afin de pouvoir charger un système d'exploitation — on parle ici d'une époque où terminaux ne disposait pas d'un disque dur.

### 4.1.1 Pourquoi le DHCP

Le DHCP partage beaucoup de points communs avec son prédécesseur ainsi il garde les mêmes numéros de port UDP à savoir 67 et 68, mais il a aussi pour vocation de combler le vide son prédécesseur en permettant :

— d'avoir plusieurs serveurs sur le même réseau

— de pouvoir configurer plus d'un sous-réseau avec l'aide des relais DHCP

— aux administrateurs de contrôler et configurer les paramètres du réseau

### 4.1.2 Relais DHCP

Les relais DHCP sont particulièrement pratique dans de grands réseau où le serveur DHCP est n'est pas directement accessible par tous les sous-réseaux, les relais permettent de transmettre au(x) serveur(s) les requêtes qui leurs parviennent. De cette manière les relais jouent le rôle d'interface de communication entre le client et le serveur.

### 4.1.3 Fonctionnement

Pour aquérir une adresse IP, la station agit ainsi :

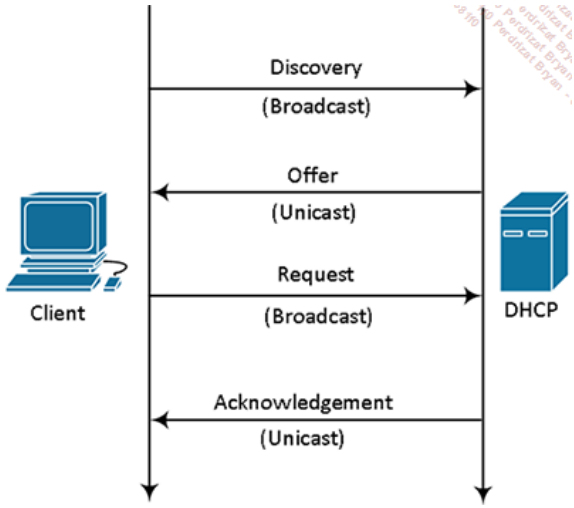


*FIGURE 14 – Echange entre un client et un serveur DHCP*

**Discovery :** Une station que nous appelerons le client ici, envoie un message de type *DHCP Discover* y en *broadcast*, afin de découvrir si un serveur DHCP est présent sur le réseau, comme le client ne possède aucune adresse IP pour l'instant, l'adresse source du message est 0.0.0.0.

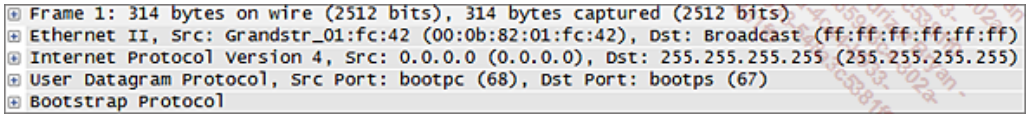


*FIGURE 15 – Message DHCP Discovery*

**Offer :** Si un serveur reçois la demande du client, celui lui renvoie une des adresses disponible. Le message DHCP Offers sera délivrer avec l'adresse fourni par le serveur au client, mais comme le client ne dispose toujours pas de son adresse IP, c'est l'adresse MAC qui va permettre au réseau de router correctement le paquet. Le paquet peut aussi transmettre d'autres informations comme le nom de domaine à utiliser, la passerelle par défaut ou le masque de sous-réseau pour ne citer que les plus utilisés.

**Request :** Une fois la proposition d'adresse reçue, le client doit confirmer qu'il désir utiliser l'adresse fournie. Comme l'adresse ne lui est toujours pas officiellement attribuée, une nouvelle fois le message est envoyé en broadcast.

**Acknowledgement :** Le serveur confirme que l'adresse est reservé pour le client et qu'il peut désormais l'utiliser.

### 4.1.4 DHCPv6

Pour les adresses IPv6, il existe trois manières d'obtenir une adresse IP.

**SLAAC :** C'est le choix par défaut, le client obtient sa configuration via un routeur IPv6 qui utilise le SLAAC (*Stateless Address Autoconfiguration*). Depuis ces informations, le client génère ça propre adresse IPv6 ; un serveur DHCPv6 est donc optionnel.

**Stateless DHCPv6 :** Le client n'obtient pas la totalité de sa configuration via un routeur IPv6 et des informations supplémentaires sont récupérer d'un serveur DHCPv6 *stateless* — soit un serveur qui ne maintient auncune information des stations présentent sur le réseau. Le client génère donc ça propre adresse IPv6.

**Stateful DHCPv6 :** Le client obtient uniquement la passerelle par défaut via le SLAAC et récupère le reste de sa configuration au moyen d'un serveur DHCPv6 *stateful* — qui agit comme un serveur DHCP IPv4 en gardant les informations concernant les stations du réseau. Le client reçoit une adresse IPv6 du serveur.

## 4.2 Serveur HTTP

Le serveur HTTP inventé dans la foulée par les ingénieurs qui ont mis au point le *World Wide Web* (WWW) — puis démocratisé et redeveloppé par la fondation Apache ou encore Microsoft, — est à la base même des serveurs web.

Ces derniers permettent à un usager d'internet d'accéder à des ressources stockées physiquement sur un terminal informatique n'importe où dans le monde. Les données accédées sont le plus souvent des fichiers HTML (*Hypertext Markup Language*) qui disposent des informations nécessaires afin d'afficher un site web sur la station du client.

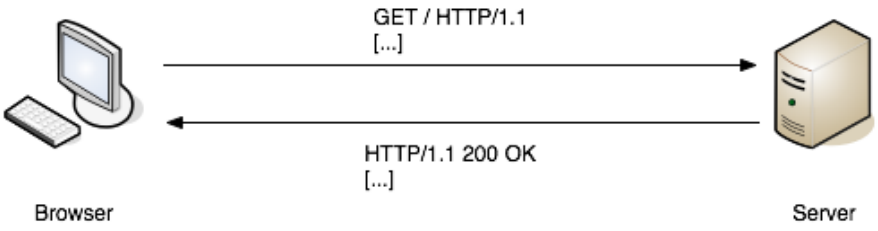


*Figure 16 – le flux d'une requête HTTP*

Pour requêter une page web, une station va émettre une requête HTTP à destination d'un serveur sur le port 80. Une fois que la requête est en main du serveur, celui va générer la réponse après avoir vérifié que la ressources est disponible et autorisée à l'accès.

Une fois que le serveur est prêt, ce dernier va renvoyé la réponse, qui se compose majoritairement des données de la ressource accédées, en plus de l'entête du protocole HTTP. L'entête contient un code permettant au client de déterminer le résultat de la requête ; sur la Figure 16, le code retourné est 200, çela signifie que la requête est un succès.

# 5 Conclusion

## 5.1 Synthèse

Pour synthétiser l'ensemble de l'étude, les points traités sont purement subjectifs, il se peut que certain élément n'ai pas été abordé ou peu car l'intérêt personnel, la do-

cumentation ou tout simplement le relation avec le travail pratique était manquant. Néanmoins, cette étude devrait pouvoir apporter une réponse quant aux principales questions de mes camarades.

## 5.2 Postface

Après consultation d'une quantité de références et de ressources sur les sujets abordés dans cette étude, il apparaît que ce document effleure seulement en surface les sujets traité, tant des sujets comme l'architecture réseau peuvent être vaste et les communication sans-fil, mathématiquement très technique.

D'une certaine manière, ce document n'a pas pour vocation de renseigner complètement les lecteurs mais de pouvoir leur transmettre les connaissances nécessaires afin de pouvoir aborder de la documentation plus technique sur les éléments présentés tout au long de cette étude.

Bryan Perdrizat
Fribourg, le 23 mars 2018

# Table des figures



# Liste des tableaux

# Références


[1] R. B. M. Abdelrahman, A. B. A. Mustafa, and A. A. Osman. A comparison between ieee 802.11a, b, g, n and ac standards. http://www.iosrjournals.org/iosr-jce/papers/Vol17-issue5/Version-3/D017532629.pdf.

[2] C. N. Academy. Campus lan and wireless lan design guide. https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Campus-LAN-WLAN-Design-Guide-2018JAN.pdf.

[3] C. N. Academy. *Scaling Networks v6 Companion Guide*. Cisco Press, Août 2017.

[4] D. Donohue and B. Stewart. *CCNP Routing and Switching Quick Reference Library : ROUTE 300-101, SWITCH 300-115, and TSHOOT 300-135 Quick References*. Cisco Press, Décembre 2014.

[5] IEEE. Official ieee 802.11 working group project timelines. http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm.

[6] H. Liu and G. Li. *OFDM-Based Broadband Wireless Networks : Design and Optimization*. Wiley-Interscience, 2005.

[7] M. Nakhjiri and M. Nakhjiri. *AAA and Network Security for Mobile Access : Radius, Diameter, EAP, PKI and IP Mobility*. John Wiley & Sons, 2005.

[8] P. Oppenheimer. *Top-Down Network Design, 3rd Edition*. Cisco Press, Août 2010.

[9] T. S. Rappaport. *Wireless Communiction : Principles and Practice*. Prentice Hall PTR Upper Saddle River, 1996.

[10] P. Santi. *Mobility Models for Next Generation Wireless Networks : Ad Hoc, Vehicular and Mesh Networks*. John Wiley & Sons, Août 2013.

[11] T. Slattery. Network redundancy or resilience ? https://www.nojitter.com/post/240151667/network-redundancy-or-resilience.

[12] D. Teare and C. Paquet. *Campus Network Design Fundamentals*. Cisco Press, Décembre 2005.

[13] D. Weedmark. Five things to be considered in designing a network. http://smallbusiness.chron.com/five-things-considered-designing-network-35911.html.

[14] R. White and D. Donohue. *The Art of Network Architecture : Business-Driven Design*. Cisco Press, avril 2014.