Table des matières :

Table des figures :

SIGLES ET ACRONYME

3GPP	3rd Generation Partnership Project
AAA	Authentication Authorization Accounting
AKA	Authentication and Key Agreement
ATM	Asynchronous Transfer Mode
BTS	Base Transceiver Station
BSC	Base Station Controller
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
CDMA	Code Division Multiple Access
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
ESS	Extended Service Set
EDGE	Enhanced Data GSM Environment
GGSN	Gateway GPRS Support Node
GPRS	Global Packet Radio Service
GSM	Global System for Mobile communications
HLR	Home Location Register
HSPDA	High Speed Downlink Packet Access
IEEE	Institute of Electrical and Electronics Engineers
IMS IP	Multimedia Subsystem
LTE	Long Term Evolution
MAC	Media Access Control
MSC	Mobile Switching Center
NAS	Network Access Server
NGH	Next Generation Hotspot
OFDMA	Orthogonal Frequency Division Multiple Access
PCC	Policy Control and Charging
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
PDN	Public Data Network
RADIUS	Remote Authentication Dial-In User Service
RAN	Radio Access Network
RNC	Radio Network Controller
RNIS	Réseau Numérique à Intégration de Service
SIM	Subscriber Identity Module
SGSN	Serving GPRS Support Node
SSID	Service Set Identifier
TLS	Transport Level Security
UMTS	Universal Mobile Telecommunications System
UTRAN	Universal Terrestrial Radio Access Network
VLR	Visitor Location Register
VRRP	Virtual Router Redundancy Protocol
WAG	Wireless Access Gateway
Wi-Fi	Wireless Fidelity
WiMax	Worldwide Interoperability for Microwave Access
WISP	Wireless Internet Service Provider

W-LAN	Wireless Local Area Network
WLC	Wireless Lan Controller
LOS	Line of sight
NLOS	Non line of sight
CPE	Client Product Equipment

INTRODUCTION GÉNÉRALE

Les nouvelles technologies évoluent exponentiellement de nos jours. De l'émergence des réseaux et du réseau Internet, à la conception de nouveaux équipements, ordinateurs et mobiles, au développement de nouvelles applications ; les réseaux cellulaires se saturent. Les utilisateurs ont vécu l'évolution technologique et ont vu leur besoin grandir. En effet, ils ont utilisé le GSM et étaient capable de communiquer avec leur proche ; ensuite, ils pouvaient envoyer des données avec l'apparition du GPRS et ensuite le EDGE qui proposait une bande passante plus importante. Et de génération en génération, le besoin des utilisateurs ne cessant d'accroître, apparaît finalement la 3ème et maintenant la 4ème génération des réseaux mobiles, offrant encore plus de débit. Cependant, le trafic des données est en expansion considérable. La constante hausse du visionnage de vidéos en ligne et l'utilisation d'applications connectées causent aujourd'hui l'explosion du trafic de données sur les réseaux mobiles :

- Entre 2009 et 2014, la consommation mobile de données a été multipliée par 39 et le nombre de mobinautes utilisant la Data passera de 12,8 millions à 635,8 millions.

- En 2014, 66% du trafic mobile mondial est monopolisé par les consultations vidéo. [1]

Un des plus grands défis des opérateurs téléphoniques est de faire face à l'insatiable appétit de leurs clients pour les connexions 3G/4G. À cause de la saturation de ceux-ci, les opérateurs comptent répondre à la demande à travers plusieurs axes :

- Le développement des infrastructures de réseaux mobiles.
- La réalisation de nouveaux réseaux, avec les technologies LTE et WiMax.
- Les petites cellules ou Femtocells.
- Le basculement automatique vers le Wi-Fi quand cela est possible (Wi-Fi Offload)

La solution la plus communément envisagée est celle du basculement automatique de la connexion d'un réseau cellulaire mobile vers un réseau Wi-Fi disponible, de façon complètement transparente pour l'utilisateur. Cette dernière sera probablement privilégiée

puisqu'elle est moins chère à développer. Conçue sous l'appellation du 3G/4G offload, cette technique se base sur l'emplacement d'un nombre de hotspots, diffusant un réseau Wi-Fi aux clients se trouvant dans la zone de couverture et leur donnant accès à Internet. Un utilisateur pourrait alors accéder à Internet via un reseai Wi-Fi. Tout le trafic qui transitait auparavant par les réseaux mobiles 3G/4G passerait par le Wi-Fi.

Le présent document est le fruit d'un travail réalisé pendant mon stage de fin d'études au sein de Sigmatel à Casablanca. Le sujet principal est celui de l'étude et de l'implémentation d'une solution 3G/4G offload. Il introduit dans le première et le deuxième chapitre, l'environnement de travail tout en situant le projet. Le troisième et le quatrième chapitre présente une étude des architectures existantes, notamment celle des réseaux UMTS, LTE et Wi-Fi ainsi que la technologie offload. Le cinquième chapitre est une étude de projet Wi-Fi Outdoor de la ville ELJADIDA. Finalement le dernier chapitre vient pour décrire le travail réalisé dans ce contexte, et qui consiste à réaliser des tests sur une plateforme du Wi-Fi offload.

Chapitre 1

Présentation de l'organisme d'accueil

INTRODUCTION

Le stage de fin d'études, que nous avons effectué lors de la dernière année cycle ingénieur au sein de la faculté de sciences et technique de Fès, est une opportunité pour les élèves ingénieurs de mettre en valeur leurs acquis durant leur formation. Mon choix s'est posé sur la société Sigmatel à Casablanca pour son poids considérable dans le domaine des télécommunications au Maroc. Ce chapitre donnera un aperçu sur cette dernière.
Sigmatel est l'interlocuteur de référence dans l'intégration d'infrastructures de communication sécurisées au Maroc. Créée en 1991, Sigmatel s'est vite forgé une place dans la conception, l'intégration et l'exploitation de solutions de communication au Maroc. Ceci revient à ses valeurs qui la rendent aujourd'hui leader dans le marché marocain. Elle a choisi comme valeurs, l'innovation, la performance, l'engagement, l'audace et l'intégrité. Sigmatel suit une politique dont le capital humain est mis au premier plan. Tout en innovant, elle s'acharne à diversifier ses offres afin de mieux répondre aux besoins croissants de ses clients.

I. NAISSANCE ET EVOLUTION DE SIGMATEL

Créée en 1991, Sigmatel est devenue la référence au Maroc pour les terminaux d'accès analogiques, RNIS et xDSL une année plus tard. Quatre ans passé, Sigmatel est devenue Gold Partner de 3Com en interconnectant 40 bâtiments en ATM par de la fibre optique. En 1997, Sigmatel a gagné deux grandes références de câblage par la certification *Network Design Installator*. Elle a également lancé plusieurs projets, notamment le fournisseur de services Internet Dounia Net, les sociétés, d'ingénierie Réseaux et Télécom au Maroc ExperTeam et d'intégration de solutions software en communication OpenSoft. Elle a ensuite signé un partenariat en exclusivité de LG et est devenue leader sur le marché des PABX numériques. En 2006, après avoir représenté Avaya, leader mondial de la ToIP et des centres d'appels, elle s'est focalisée sur l'infrastructure télécom pour opérateurs, et elle a réalisé le réseau CDMA de WANA. Deux années plus tard, elle a déployé le réseau 3G de WANA. Parmi les récents projets de Sigmatel, le déploiement réseau Wi-Fi pour opérateur INWI à El Jadida en 2014 et à casablanca en 2015, projet intitulé « Wifi 7dak ». A ce jour, la société compte environ 300 employés, un capital de 20 000 000 Dhs et quatre agences à Rabat, Agadir, marrakech et Tanger. Sigmatel s'occupe aussi de la maintenance et l'opération des sites INWI dans le milieu et le sud du royaume avec plus de 5000 sites à gérer. [2]

II. SOLUTIONS PROPOSEES

La notoriété qu'a connue Sigmatel à travers les années lui a permis d'élargir son centre d'activité. La structure efficace qu'elle a adoptée lui a permis d'encourir le dynamisme des nouvelles technologies dans le domaine des télécommunications. Sigmatel est présente dans les installations, notamment dans le pré-câblage informatique, l'aménagement de site, les

infrastructures télécom et systèmes, les centres de contact et l'installation des visioconférences. Elle actionne également dans les réseaux sécurisés multiservices, la téléphonie et la sécurité des systèmes d'information.

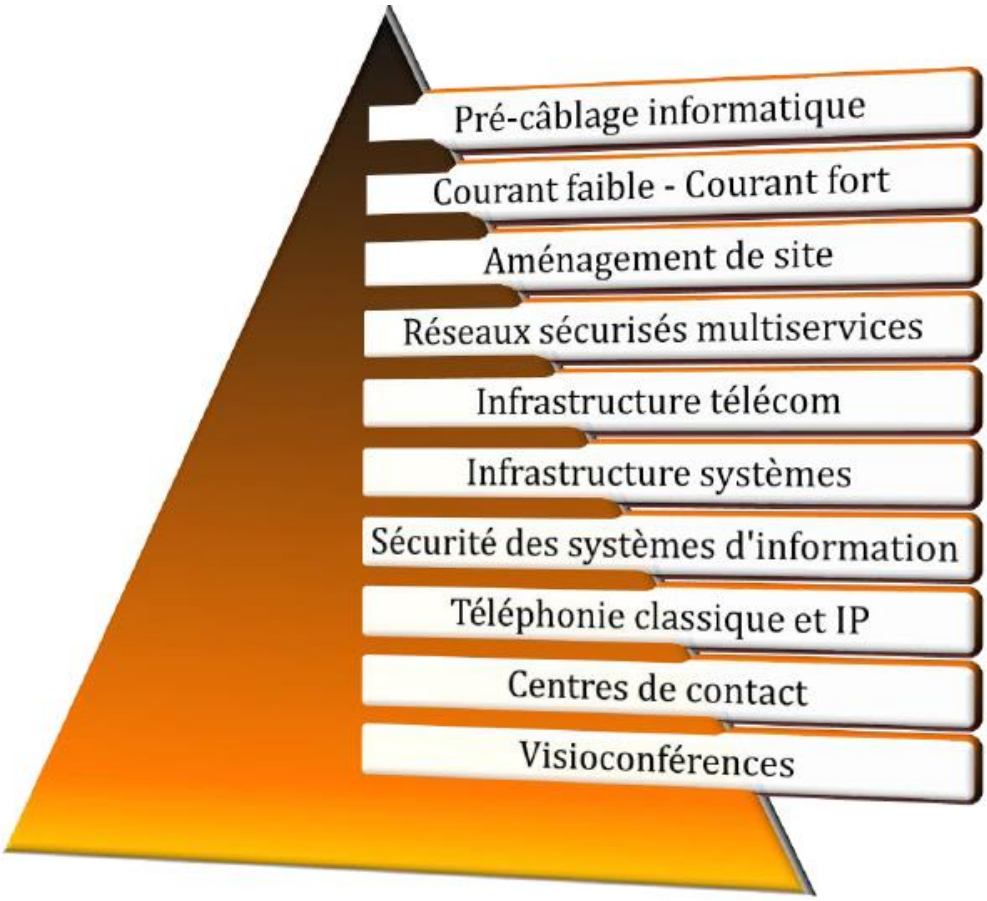


Figure 1 : SOLUTIONS SIGMATEL

III. SERVICES

Parmi les principaux objectifs de Sigmatel, l'accompagnement des clients tout au long du processus de la solution. Elle catégorise ses services en trois volets : les services professionnels, les services d'exploitation et les services d'intégration.

Figure 2 : SERVICES SIGMATEL

Par ses services professionnels, Sigmatel a la responsabilité de proposer à ses clients les meilleurs offres et solutions en adéquation avec leur besoin. Elle s'engage à les accompagner tout le long de l'appel d'offre en apportant le meilleur de son expertise. Elle

se charge de l'audit, du design, du maquettage, de la veille technologique et de l'expertise constructrice.

Les services d'exploitation englobent les supports techniques et les locations de ressources. Sigmatel s'engage par ses services à superviser, exploiter et améliorer les réseaux et les applications de ses clients.

Les services d'intégration se placent en seconde phase, après le choix de l'architecture et des solutions technologiques. Ils concernent directement l'intégration, le déploiement des solutions. Sigmatel se soucie également de l'accompagnement au changement et des formations afin de faciliter la prise en main des outils mis en place.

IV. PARTENAIRES

Aujourd'hui, Sigmatel a dans son compte un nombre considérable de partenaires. Nous en citons :

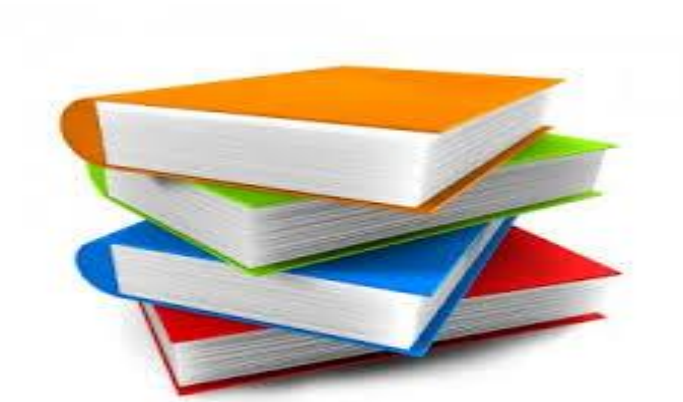
- Avaya - Gold Business Partner
- 3Com - Gold Partner
- ZyXEL - Official Partner
- Trend Micro - Premium Partner
- Cisco - Select Certified Partner
- Altai - Exclusive Partner
- IBM - Business Partner
- Microsoft - Sales Specialist…
- partenaire exclusif d'ALTAI au Maroc

CONCLUSION

La structure Sigmatel est une société leader en solutions de réseaux et de télécommunications au Maroc. Elle n'existe que depuis une vingtaine d'années, cependant, elle a su se marquer sur le marché marocain en se positionnant en première place sur l'intégration et la maintenance de solutions innovantes et qui se dotent d'un avenir prometteur.

CHAPITRE 2

PRESENTATION DU CAHIER DE CHARGE



INTRODUCTION

Ce présent chapitre aura pour but d'introduire le sujet de stage de fin d'études en annonçant le besoin qui a conduit à la naissance du projet et de la solution de l'offload. Quand la problématique de la congestion a été relevée, les ingénieurs ont annoncé une série de solutions que nous détaillerons en seconde partie dans ce chapitre. La solution qui marque plus d'intérêt est celle de l'offload, nous verrons alors les différents fournisseurs qui ont déployé la solution d'une part, et d'autre part, la position de ce projet pour l'entreprise qui nous a accueilli pour ce stage de fin d'études. Plusieurs taches nous ont été confiées dès notre arrivée, nous avons donc procédé à une planification de celles-ci afin de répondre au cahier de charges dans les temps fixés.

I. PROBLEMATIQUE:

Le nombre des terminaux mobiles augmente exponentiellement. La combinaison de ceux-ci et des réseaux mobiles 3G/4G provoque une véritable explosion de la consommation de Datas. Les utilisateurs sont donc connectés à plein temps et ont accès à la vidéo et la TV en streaming. Ces services nécessitent une bande passante importante et un grand débit, ce qui cause une utilisation permanente du réseau et donc sa congestion. De celle-ci résultent une médiocre performance et des interruptions de service. Le client se retrouve avec une bande passante constamment utilisée et congestionnée. Sans oublier que les équipements qui assurent la connexion 3G/4G tombent souvent en panne, ce qui cause des coupures du service de l'internet et nécessite des efforts colossaux au niveau de la maintenance.

Parmi les solutions proposées figure une nouvelle technologie, faisant l'objet du présent document. La 3G offload consiste à répondre au besoin du client qui souhaite avoir un bon débit et une connexion fluide. Cette solution dirige de flux de données qui transite normalement par ces réseaux mobiles vers une infrastructure d'un réseau puissant et existant qu'est le Wifi. Le déploiement et la mise en place de la solution résout le problème et le client dispose maintenant d'une connexion à travers le Wifi, lui permettant d'accéder à Internet comme il le souhaite. Sauf que cette solution, bien adaptée à la congestion des réseaux mobile nécessite une maintenance permanente.

En effet, tout équipement informatique est exposé aux défaillances. De tous types, ces défaillances peuvent être causées subitement, et ainsi provoquer un arrêt de connexion soudain chez l'utilisateur. Si le routeur auquel est connecté l'utilisateur, qui lui fournissant l'accès à Internet est arrêté, la connexion chez le client est interrompue. De ce risque, un mécanisme de sécurité devrait être mis en place afin de gérer les éventuelles défaillances que le réseau pourrait subir. Le routeur en risque, devrait être protégé et assurer sa fonction sans interruptions.

II. PISTES DE SOLUTION

Afin de rendre le réseau 3G moins congestionné aux heures de pointe, les opérateurs ont procédé à une limitation de la bande passante aux utilisateurs. Tous les forfaits 3G sont plafonnés à 500Mo par mois en général dans le but d'éviter qu'un utilisateur occupe toute la bande passante fournie.

Une première solution serait de doubler le nombre des antennes et donc diminuer la taille des zones de couverture. Ceci offre une bande passante uniforme certes, mais n'assure pas un trafic identique entre les zones d'une part, et d'autre part, l'implantation des stations de base peut s'avérer compliquée. La capacité de données est limitée et l'efficacité spectrale est très pauvre. Le développement des infrastructures est également limité par l'aspect coût de l'investissement.

Les opérateurs ont donc opté pour le déploiement de nouveaux réseaux plus performants au niveau de la bande passante et donc du débit. Au Maroc, les utilisateurs mobiles ont commencé cette année a utilisé la 4ème génération des réseaux mobiles (LTE) successeur à la 3G, qui vient pour répondre à leur besoin gourmande de l'internet. Le débit et la bande passante seront alors aux alentours de 300 Mbit/s [3]. Cette solution pourrait donc alléger le trafic circulant sur le réseau 3G, cependant, ce nouveau réseau risque d'être congestionné également.

Une deuxième solution est les femtocells ou Home Node B, qui sont des éléments de base d'un réseau cellulaire de téléphonie mobile, de faible puissance, prévu pour offrir une couverture radio limitée et souvent dédiée à un usage résidentiel ou en entreprise. Grâce au femtocells on aura une couverture meilleure pour les zones dont le signal est faible et une capacité data mobile importante pour les usagers qui utilisent l'accès internet sur leur téléphone, mais elles présentent des inconvénients tel que des grandes risque concernant la confidentialité des communications privées. De plus le Wifi possède une place déjà bien ancrée dans notre vie de tous les jours donc les femtocells sont en face d'un concurrent difficile à détrôner.

La dernière solution proposée par les ingénieurs de télécommunications consiste à exploiter la puissance des réseaux connus afin de remédier au problème de congestion. La 3G/4G offload est une solution qui se base sur la technologie du Wi-Fi pour désengorger les réseaux mobiles. En effet, l'idée de base serait de faire basculer le trafic de ces réseaux vers le Wi-Fi. Un utilisateur connecté à Internet par son réseau 3G, il verra son flux passer par le Wi-Fi sans qu'il s'en rende compte, le basculement est automatique. Cette technique nécessite la mise en place de hotspots, auprès desquels le client se connecte. Chaque utilisateur devrait ensuite s'authentifier auprès d'un serveur Radius, qui contiendrait une base de données des clients autorisés à se connecter. Cette nouvelle technologie de hotspots

ne nécessite pas un budget important pour leur déploiement, encore moins en ce qui concerne la configuration et la maintenance.

III. CONTEXTE REEL.

Aptilo, Aruba networks, Ruckus Wireless, Alepo, Runcom technologies sont des sociétés qui proposent des solutions d'offloading à travers le monde. En 2011, les solutions Wi-Fi étaient principalement apportées par Cisco, Ruckus Wireless et Ericsson/Belair [4].

Boingo Wireless a récemment lancé le premier réseau commercial NGH (pour Next Generation Hotspot Wi-Fi dans le monde) à l'aéroport O'Hare de Chicago. En outre, une démonstration de cette technologie a été lancée en direct lors de la connexion Wi-Fi Congrès mondial à Beijing le 21 novembre 2013. Le réseau est organisé par Cisco et China Mobile. Durant cette démonstration, un total de 13 fournisseurs de services fera la démonstration des capacités NGH en utilisant le réseau au cours du Congrès [5].

Au Maroc, l'opérateur Inwi en collaboration avec Sigmatel, a lancé le projet Wi-Fi outdoor permettant de couvrir de larges zones urbaines avec du haut début non filaire. Ce service lancé à Casablanca et à El Jadida en avant-première entre juillet 2013 et juillet 2014, sous le nom de « Wifi 7dak », a connu une grande appréciation par les habitants des deux villes. Ce projet connaitra une expansion dans les autres villes du Maroc dans les années prochaines. En effet, le projet « Wifi 7dak » devrait couvrir 22 villes avant le deuxième semestre 2016 ambitionnant de démocratiser l'accès à Internet.[6]

IV. LE PROJET POUR L'ENTREPRISE

Le Wi-Fi pour opérateur ou le Wi-Fi outdoor représente pour Sigmatel un projet de taille. Elle a collaboré avec l'opérateur Inwi et l'équipementier Altai technologies dans l'élaboration et le déploiement de la solution à El-Jadida et à Casablanca. Mais, consciente de l'aspect innovation dans le domaine des télécommunications, Sigmatel ne s'est pas contentée de déployer la solution, mais s'oriente aujourd'hui à la réalisation de fonctionnalités plus élaborées afin de répondre aux exigences du marché. La solution pouvant être déployée également chez des organismes tels que les grandes surfaces, les malls, ou même les hôtels, la société reste à l'écoute du marché et des appels d'offre.

V. TACHES DEMANDEES ET OBJECTIFS

Le Wi-Fi opérateur est une idée innovante, qui répond à la fois à la problématique de la congestion des réseaux mobiles et aux exigences des clients en terme de performance de connexion. Sigmatel a travaillé sur cette solution en collaboration avec l'opérateur Inwi, ce qui la positionne parmi les autres intégrateurs. La solution ainsi déployée, suscitera l'attention des autres concurrents sur le marché marocain, ce qui rend la solution, un projet d'avenir et de grande taille. La présentation du Wi-Fi opérateur nous a amené à fixer comme objectif pour notre stage de fin d'études, l'étude de projets WIFI 7DAK de INWI et la réalisation d'une série de tests qui s'inscrit dans la politique de développement de la

solution. Ces tests se feront sur une plateforme virtuelle dans l'objectif de tester de nouvelles fonctionnalités à proposer aux clients, notamment l'aspect redondance pour assurer la haute disponibilité de la solution.

L'aboutissement et la réalisation du projet nous a mené à entreprendre une approche basée sur des tâches. Nous avons donc procédé à une répartition comme suit :

- Documentation sur les réseaux cellulaires 3G / 4G

- Documentation sur le Wi-Fi

-Documentation de 3G Offload

-Visite des sites wifi outdoor de INWI & Etude de projet « Wifi 7dak »

- Prise en main du routeur Mikrotik et de ses configurations

- Etude de l'architecture de test

- Prise en main de la maquette à base de la technologie Ruckus Wireless, des interfaces de configuration et de la plateforme Cloud4wi pour le Wi-Fi outdoor

- Configuration d'un portail captif relatif à un exemple d'hôtellerie et test de connectivité

- Réalisation de la maquette de test

- Installation de l'outil VMware
- Installation d'une machine Windows, Ubuntu et du routeur
- Configuration des adresses IP sur les trois machines virtuelles
- Test de communication entre les machines et de l'authentification locale
- Installation et configuration de Freeradius et des bases de données MySQL
- Implémentation des tests d'authentification, de comptabilité et de redondance

- Rédaction du rapport et présentation

VI. PLANIFICATION:

La planification d'un projet est parmi les phases d'avant-projet les plus importante. Elle consiste à déterminer et ordonnancer les tâches du projet et à estimer leurs charges respectives.

Parmi les logiciels de planification des projets, nous avons choisi MS PROJECT 2007 qui est l'un des outils professionnels les plus répandus en termes de planification.

1. PRESENTATION DU DIAGRAMME DE GANT :

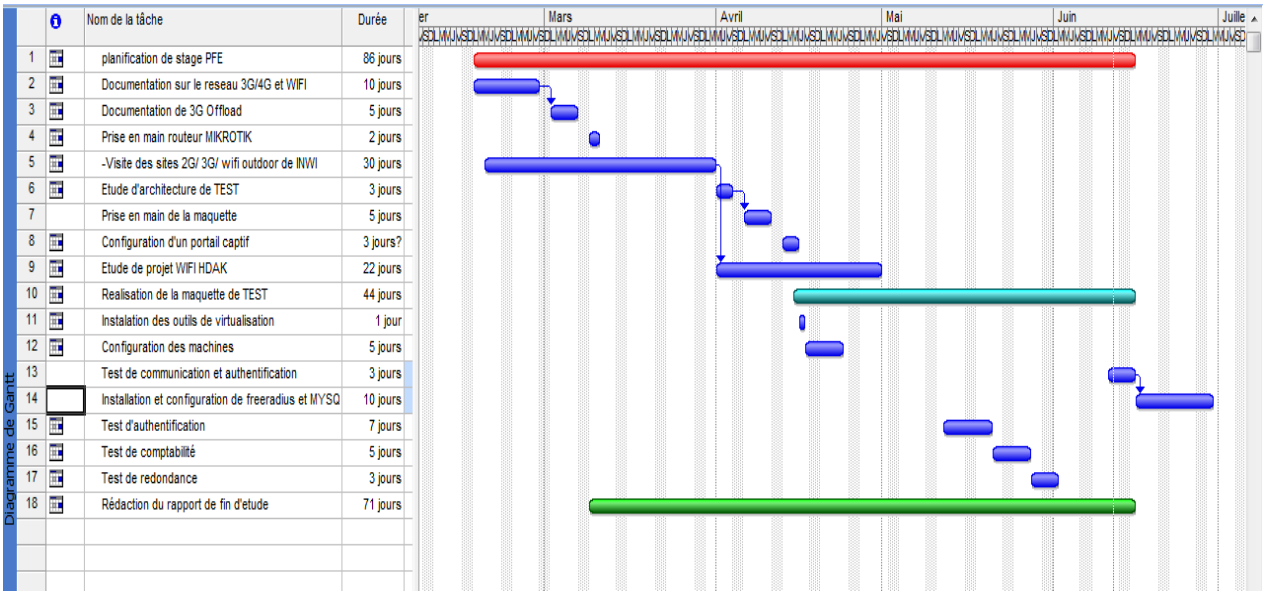


Figure 3 : Présentation de diagramme de gant

2. ORDONNANCEMENT DES TACHES :

		Nom de la tâche	Durée
1		planification de stage PFE	86 jours
2		Documentation sur le reseau 3G/4G et WIFI	10 jours
3		Documentation de 3G Offload	5 jours
4		Prise en main routeur MIKROTIK	2 jours
5		-Visite des sites 2G/ 3G/ wifi outdoor de INWI	30 jours
6		Etude d'architecture de TEST	3 jours
7		Prise en main de la maquette	5 jours
8		Configuration d'un portail captif	3 jours?
9		Etude de projet WIFI HDAK	22 jours
10		Realisation de la maquette de TEST	44 jours
11		Instalation des outils de virtualisation	1 jour
12		Configuration des machines	5 jours
13		Test de communication et authentification	3 jours
14		Installation et configuration de freeradius et MYSQ	10 jours
15		Test d'authentification	7 jours
16		Test de comptabilité	5 jours
17		Test de redondance	3 jours
18		Rédaction du rapport de fin d'etude	71 jours

Diagramme de Gantt

Figure 4 : Ordonnancement des taches

CONCLUSION

Ce chapitre a mis l'accent sur les problèmes existants des réseaux mobiles, ainsi que la méthodologie suivie pour l'élaboration de ce projet de fin d'étude, et sa planification tenant compte des délais à respecter.

Avant d'entamer les différentes phases qui nous ont permis de mener à bien le projet, il serait judicieux de commencer tout d'abord par une étude des aspects théoriques des réseaux mobiles et de wifi, dont la connaissance semble indispensable à la maitrise du projet et à sa réalisation.

CHAPITRE 3

APERÇU SUR LES RESEAUX MOBILES

INTRODUCTION

Le but de ce chapitre est d'introduire et de décrire de manière générale les réseaux Wi-Fi, 3G et 4G. Nous verrons dans un premier temps l'architecture des trois réseaux, et les éléments essentiels qui la constituent. En second lieu, nous nous focaliserons sur les problèmes qui peuvent causer la congestion des deux derniers. Cette partie s'inscrit dans l'objectif de la compréhension de la nouvelle technologie du Wi-Fi Offload.

I. LE WI-FI

Le Wi-Fi (pour *Wireless Fidelity)* est un réseau local, de type Ethernet à accès sans fil permettant d'atteindre des débits de 11 Mbit/s théorique dans une bande de fréquence de 2,4 Ghz. Ce réseau apparut après la concrétisation de la norme IEEE 802.11 qui lui a assurée un essor remarquable. La portée radio du réseau Wi-Fi pouvant atteindre 25 mètres dans un environnement dense et 60 mètres en absence d'obstacles, il est considéré comme la solution la plus adéquate aux milieux indoor. La mise en place d'une solution Wi-Fi sans fil nécessite un point d'accès Wi-Fi et un terminal doté d'une carte Ethernet Wi-Fi ou d'un adaptateur USB Wi-Fi

1. APPLICATIONS DU WI-FI[7]

Les applications du Wi-Fi sont diverses et nombreuses. Il répond aux besoins d'un réseau d'entreprise Ethernet sans fil. La première application était donc d'étendre le réseau filaire existant.

Le Wi-Fi s'est ensuite introduit dans les foyers chez le grand public. L'objectif derrière l'installation d'un réseau sans fil est de pouvoir se connecter à l'internet depuis n'importe quel endroit du domicile. Ce réseau semble adéquat parce qu'une seule borne Wi-Fi suffit à couvrir un domicile de moins de 100 m².

La troisième utilisation concerne les hotspots. En effet, un hotspot est un point d'accès sans fil à Internet. D'un terminal mobile personnel, les utilisateurs peuvent se connecter et accéder à internet qu'ils soient dans un café, un hôtel, un aéroport, ou même une salle d'attente. Cette technologie qui date de 14 ans, a connu un essor remarquable dès son apparition. De ceci sont créés les WISP (Wireless Internet Service Providers) ou fournisseurs d'accès à internet sans fil.

2. MODES DE FONCTIONNEMENT

Mode infrastructure :

Le mode infrastructure se base sur une station spéciale appelée Point d'Accès (PA). L'ensemble des stations à portée radio du PA forme un BSS *(Basic Service Set)*. Chaque BSS est identifié par un BSSID *(BSS Identifier)* de 6 octets qui correspond à l'adresse MAC

du PA. Cette architecture permet d'étendre les réseaux parce qu'elle permet à des terminaux de se connecter à n'importe quel réseau via un point d'accès.

C'est une architecture centralisée où toute communication doit passer par le PA même s'il s'agit d'une communication entre deux stations du même BSS. Il est possible de relier plusieurs points d'accès entre eux (ou plus exactement plusieurs BSS) par une liaison appelée système de distribution (notée DS pour Distribution System) afin de constituer un ensemble de services étendu (extended service set ou ESS). Le système de distribution (DS) peut être aussi bien un réseau filaire, qu'un câble entre deux points d'accès ou bien même un réseau sans fil. Le figure ci-dessous présente deux point d'accès en mode infrastructure.

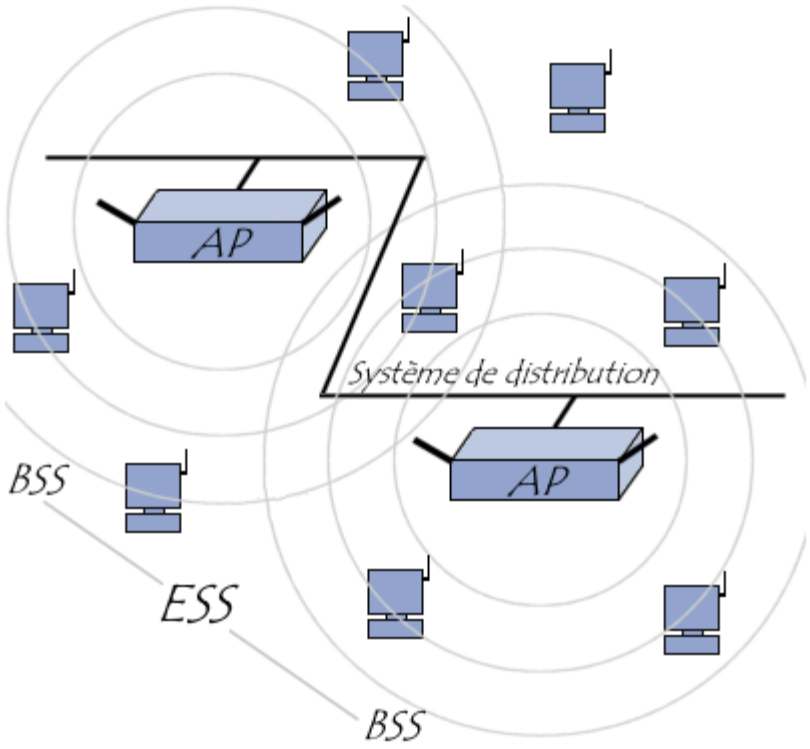


Figure 5 : mode infrastructure

Un ESS est repéré par un ESSID (Service Set Identifier), c'est-à-dire un identifiant de 32 caractères de long (au format ASCII) servant de nom pour le réseau. L'ESSID, souvent abrégé en SSID, représente le nom du réseau et représente en quelque sort un premier niveau de sécurité dans la mesure où la connaissance du SSID est nécessaire pour qu'une station se connecte au réseau étendu.

Lorsqu'un utilisateur nomade passe d'un BSS à un autre lors de son déplacement au sein de l'ESS, l'adaptateur réseau sans fil de sa machine est capable de changer de point d'accès selon la qualité de réception des signaux provenant des différents points d'accès. Les points d'accès communiquent entre eux grâce au système de distribution afin d'échanger des informations sur les stations et permettre le cas échéant de transmettre

les données des stations mobiles. Cette caractéristique permettant aux stations de "passer de façon transparente" d'un point d'accès à un autre est appelé itinérance (en anglais roaming).

Mode AD-HOC :

En mode ad hoc les machines sans fils clientes se connectent les unes aux autres afin de constituer un réseau point à point (peer to peer en anglais), c'est-à-dire un réseau dans lequel chaque machine joue en même temps le rôle de client et le rôle de point d'accès.

L'ensemble formé par les différentes stations est appelé ensemble de services de base indépendants (en anglais independant basic service set, abrégé en IBSS).

Un IBSS est ainsi un réseau sans fil, qui est constitué au minimum de deux stations et n'utilisant pas de point d'accès. L'IBSS constitue donc un réseau éphémère permettant à des personnes situées dans une même salle d'échanger des données. Il est identifié par un SSID, comme l'est un ESS en mode infrastructure.

Dans un réseau ad hoc, la portée du BSS indépendant est déterminée par la portée de chaque station. Cela signifie que si deux des stations du réseau sont hors de portée l'une de l'autre, elles ne pourront pas communiquer, même si elles "voient" d'autres stations. En effet, contrairement au mode infrastructure, le mode ad hoc ne propose pas de système de distribution capable de transmettre les trames d'une station à une autre. Ainsi un IBSS est par définition un réseau sans fil restreint.

3. TYPES D'ARCHITECTURE [8].

ARCHITECTURE AUTONOME :

Cette architecture représente la solution classique et largement déployée au monde. Elle est constituée par un ensemble de points d'accès autonomes, agissant comme des éléments indépendants. En fait, chaque PA dispose de sa propre version de configuration et prend en charge un certain nombre de tâches telles que la gestion des associations 802.11, la gestion des radiofréquences et la gestion de la sécurité. Toutefois, cette architecture présente des limitations au niveau de la configuration des points d'accès qui est individuelle et au niveau de la gestion de mobilité.

ARCHITECTURE CENTRALISEE :

Contrairement à l'architecture autonome, celle-ci concentre l'intelligence en un point unique. En effet, elle est constituée par des points d'accès légers, des contrôleurs, et des serveurs d'administration. Le point central de cette architecture sont les contrôleurs ou

les WLC (Wireless Lan Controller) qui ont la charge de piloter les bornes et gérer des fonctionnalités avancées telles que la mobilité, la détection des intrusions, et le cache DHCP/RADIUS. Le deuxième composant est le point d'accès léger qui renvoie toutes les fonctions avancées de la couche liaison au contrôleur, ce qui facilite leur gestion. Cette architecture est clairement schématisée dans la figure suivante :

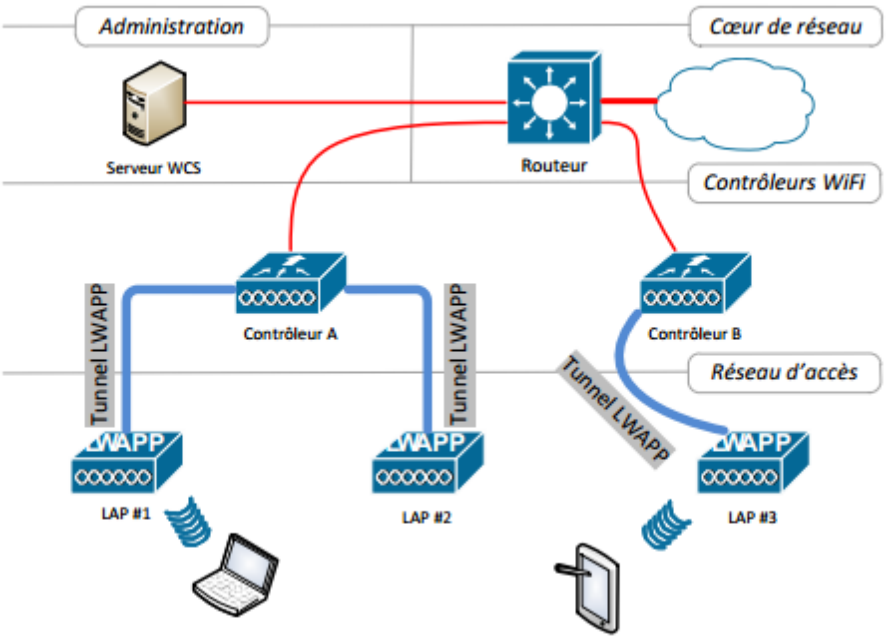


Figure 6 ; ARCHITECTURE CENTRALISEE WI-FI – JEAN-CHRISTOPHE RIOS

Parmi les fonctionnalités supplémentaires qu'offrent les contrôleurs, nous trouvons la mobilité entre points d'accès au niveau 2 et entre contrôleurs au niveau 2 et 3. Le handover et le roaming sont mieux supportés du fait que le contrôleur dispose d'une vue globale sur les points d'accès d'une part, et d'autre part, les données utilisateurs sont transférées. Ceci dit, le contrôleur représente donc un point central et critique de l'architecture, dont la défaillance est intolérable.

Le serveur de gestion WCS (pour Wireless Control System) est placé au-dessus des contrôleurs. Il permet de gérer les contrôleurs joignables par leur adresse IP via une interface web. Parmi les différentes fonctionnalités à configurer, le SSID diffusé, les normes du réseau wifi, et éventuellement la disponibilité des serveurs DHCP et RADIUS.

4. GESTION DE LA MOBILITE

Le roaming ou le handover représente l'action qui consiste pour une station à changer de point d'accès sans perdre sa connectivité réseau.

Cette fonctionnalité pour les réseaux Wi-Fi est classée selon deux catégories :

- Roaming intra-ESS (Internal Roaming) qui est manifesté quand un mobile passe d'un point d'accès à un autre au sein du même réseau sans fil.

- Roaming inter-ESS (External Roaming) traduit le déplacement d'un autre fournisseur de service Internet sans fil WISP dans le WLAN.

5. AUTHENTIFICATION :

La norme 802.1X :

802.1x est un standard d'authentification mis en place par l'IEEE et permettant de contrôler l'accès au réseau et à ses équipements. Il est basé sur le protocole EAP dont le rôle est de transporter les informations d'identifications des utilisateurs. Ce standard est utilisé principalement pour sa facilité d'utilisation et de gestion.

Ce standard se compose de trois parties importantes : le point d'accès, le serveur d'identification (notamment Radius) et le terminal. En effet, le terminal essaie de se connecter via le point d'accès. Ce dernier lui demande un identifiant qui le transmet au serveur d'identification. Le serveur redemande à l'utilisateur de confirmer son identité, et vérifie les informations reçues en fonction desquelles l'utilisateur est autorisé ou non.

D'un point de vue compatibilité, les serveurs Radius gèrent le standard de sécurité 802.1x. Cependant, il est à noter qu'il y a une variation sur les protocoles EAP acceptés.

Extensible Authentification Protocole EAP :

L'EAP est un protocole d'identification, basé sur un échange de trames et des méthodes d'authentification. Ce protocole peut être utilisé avec un point d'accès compatible avec 802.1x, autorisant ainsi une négociation des clés de chiffrement. Le protocole EAP et cette méthode d'authentification peuvent prendre en charge d'autres mécanismes tels que AKA (Authentification and Key Agreement), SIM (Subscriber Identity Module) ou MD5, le vérificateur d'intégrité :

- EAP-SIM : permet l'authentification des utilisateurs à travers leur carte SIM. En effet, chaque terminal mobile dispose d'une carte SIM spécifiant l'identité de l'utilisateur et contenant une clé secrète. Ce processus se déroule par un échange de requêtes et de réponses à travers le serveur Radius. Ce processus de communication entre le terminal, le point d'accès, le serveur Radius et la base de donnée HLR est bien décrit dans la figure ci-contre :

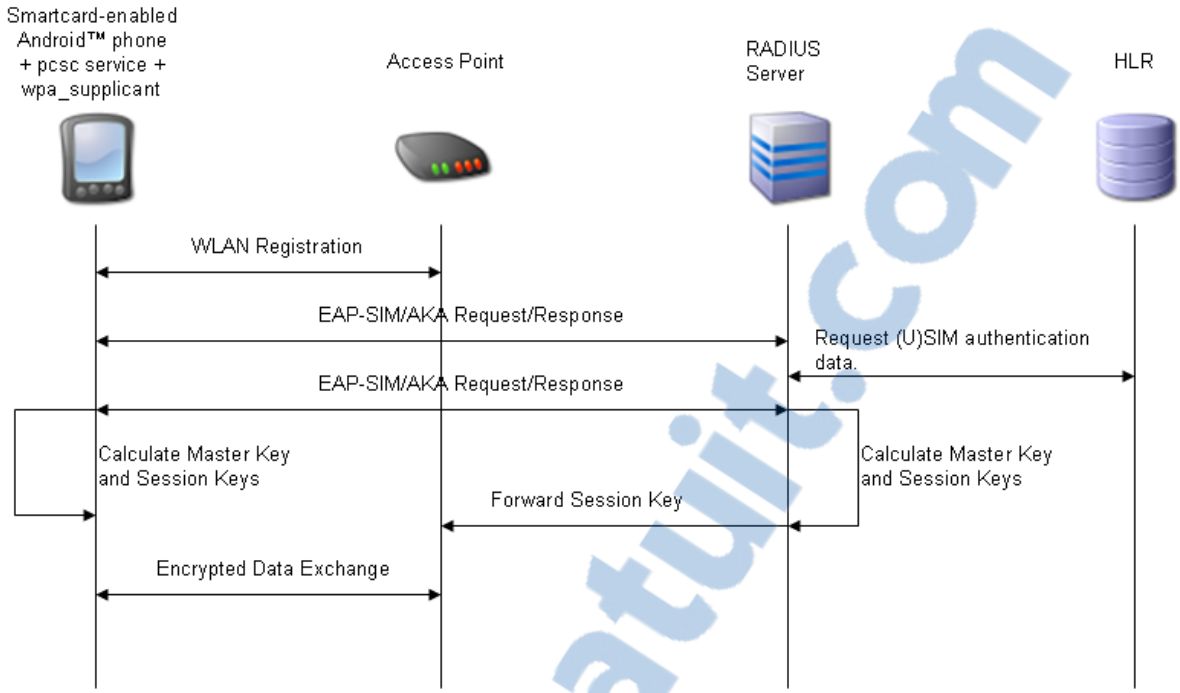


Figure 7 : COMMUNICATION EAP SIM [9]

- EAP-TLS (*Transport Level Security*) : permet l'authentification à la base des certificats du serveur et du client. Il permet la création d'un tunnel sécurisé pour l'identification entre l'utilisateur et le serveur Radius. A la différence de l'EAP SIM, le TLS dispose d'une partie contrôlant les certificats. La figure ci-dessous spécifie les échanges entre les différentes parties :

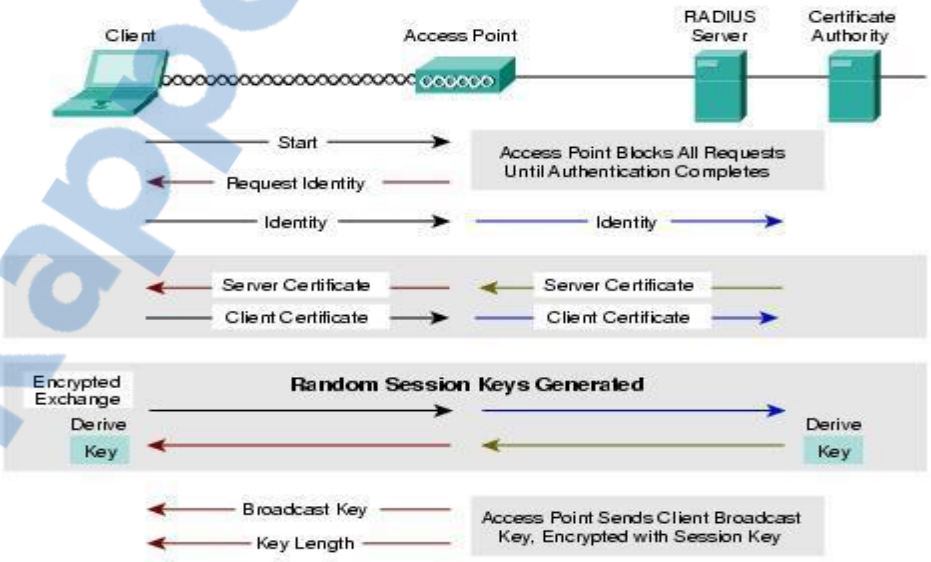


Figure 8 : COMMUNICATION EAP TLS [10]

II. LA 3EME GENERATION / UNIVERSAL MOBILE TELECOMMUNICATIONS SYSTEM

Le réseau de la troisième génération radio peut être représenté par l'UMTS. Cette génération a apporté des améliorations par rapport à la deuxième génération -2G- avec toutes ses évolutions. Ces améliorations peuvent être résumées par :

- Un accès plus rapide à internet depuis les équipements mobiles à savoir les téléphones portables, les tablettes ou les clés 3G.
- Une qualité de communication plus proche de la téléphonie fixe.
- Une solution pour la congestion vécue par les réseaux 2G essentiellement dans les grandes villes.

Pour profiter de ces avantages avec le minimum de coût, nous avons eu recours à l'exploitation de l'architecture du réseau 2G et nous avons introduit des modifications pour mettre en place les réseaux 3G. Cette coexistence des deux générations en termes d'architecture complémente les deux réseaux et optimise la qualité de services. Elle peut être illustrée par la figure suivante :

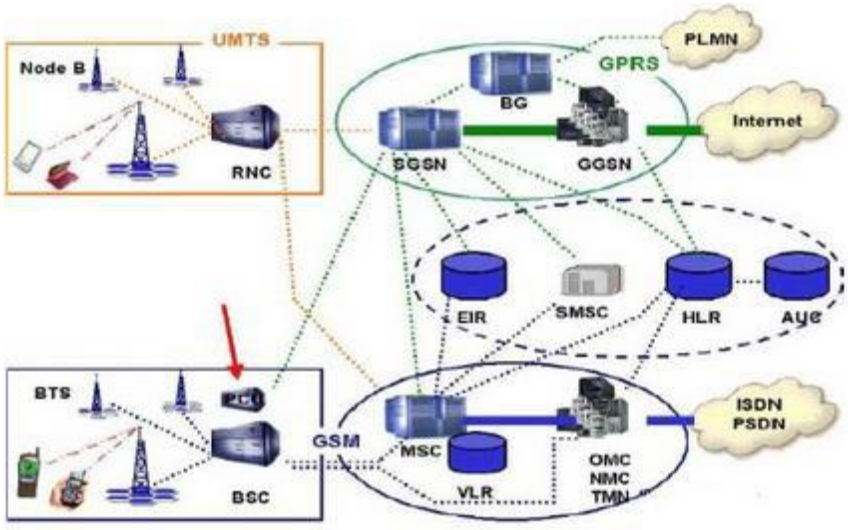


Figure 9 : COEXISTENCE DES RESEAUX GSM ET UMTS [11]

Sur la figure ci-dessus, il y a quatre grandes parties. Une partie consacrée au réseau GSM constituée par des stations de base ou des BTS, et des BSC (pour Base Station Controller) qui a la charge de commander plusieurs BTS. Ce bloc est ensuite lié au MSC qui gère un certain nombre de BSC, et à des bases de données VLR et HLR.

La seconde partie est relative au réseau UMTS et elle dispose des mêmes éléments avec des nominations différentes. Dans les réseaux de troisième génération, les stations de base sont nommées des Node B et le RNC joue le rôle du BSC.
Ces deux derniers sont liés ensuite au coeur du GPRS constitué lui-même du SGSN (pour Serving GPRS Support Node) qui est une passerelle permettant l'acheminement des données et GGSN (pour Gateway GPRS Support Node) une passerelle également, mais destinée à l'interconnexion entre le réseau paquet mobile et les réseaux IP externes.
La figure ci-dessus introduit même le réseau GPRS, nommée également la génération 2,5 ou la 2,5G. Celui-ci dérive du réseau GSM et introduit la transmission par paquets permettant l'envoi de données. Ce réseau à la spécificité également d'établir un circuit au besoin, qu'au moment de l'échange de données. Au niveau architectural, la GPRS permet de fournir une connectivité IP permanente à une station mobile en introduisant les équipements SGSN et GGSN.

1. ARCHITECTURE DU RESEAU 3G

L'architecture du réseau UMTS est constituée de trois volets importants :

- Les stations mobiles.
- Le domaine radio ou réseau d'accès appelé RAN *(Radio Access Network)* ou UTRAN.
- Le domaine réseau cœur intitulé CN *(Core Network)*

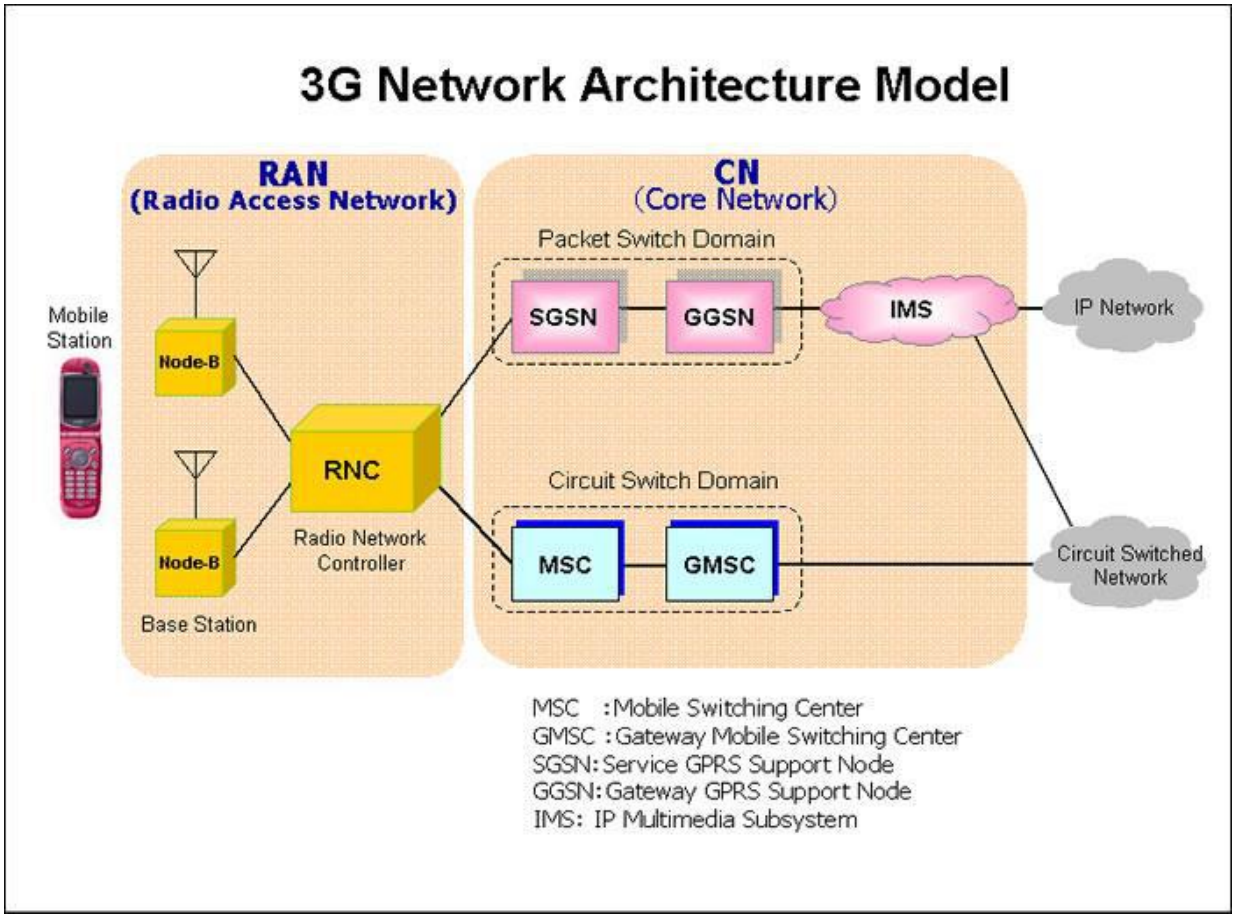


Figure 10 : ARCHITECTURE RESEAU UMTS [12]

Domaine réseau d'accès :

Ce domaine est composé principalement de deux unités à savoir le Node B et le RNC ou le contrôleur du réseau radio formant ensemble l'UTRAN. Le Node B est équivalent à la BTS du réseau GSM. Il permet l'émission et la réception des signaux sur l'interface radio en utilisant des récepteurs et des transmetteurs CDMA. Pour les récepteurs, ils convertissent les signaux pour les acheminer au RNC sur l'interface Iub. Et dans le sens inverse, les transmetteurs CDMA convertissent les signaux reçus du RNC pour les envoyer sur l'interface Uu (interface aire entre RNC et téléphone mobile).

Pour le RNC, comme son nom indique, il assure les fonctions de contrôle des ressources radio allouées aux Nodes B auxquels il est connecté. Il est aussi le point d'accès aux différents services offerts par l'UTRAN (UMTS Terrestrial RNC Radio Access Network). Il est responsable du HandOver pour maintenir la connexion de l'abonné en passant d'une cellule à une autre et de la macro-diversité qui est la phase pendant laquelle une station mobile est connectée simultanément à différentes cellules radio pour assurer une meilleure qualité de communication et éviter la coupure de la communication lors du passage d'une cellule à une autre.

Domaine réseau cœur :

Le réseau cœur d'UMTS est composé de deux parties :

- Une partie de commutation de circuits pour la transmission de la voix qui se base sur l'architecture GSM existante.

- Une partie de commutation de paquets pour la transmission des données composée du SGSN et du GGSN qui sont similaires à ceux utilisés pour le réseau GPRS mais avec quelques modifications logiques.

Pour la mise en place du réseau cœur UMTS, un opérateur a le choix entre adapter le réseau GSM/GPRS existant en apportant quelques modifications aux SGSN et GGSN existant pour supporter de nouvelles caractéristiques à savoir les nouveaux protocoles de signalisation ou mettre en place un autre réseau de base composé de 3G SGSN et 3G MSC pour supporter l'interface UTRAN avec ses spécificités et par suite profiter d'un réseau UMTS en parallèle sans aucun impact sur le réseau GSM/GPRS. Cette dernière solution peut être adoptée afin d'éviter les risques d'instabilité et les problèmes de capacité que peut poser la première solution.

2. CLASSES DE SERVICES UMTS

Il existe quatre classes de services, définies par le 3GPP (the 3rd Generation Partnership Project). Toute classe est adaptée aux besoins des applications de transport multimédias dans l'UMTS.
- Conversationnelle. Cette classe offre une bande passante contrôlée pour le flux voix avec un minimum de délai entre les paquets.

- Streaming. Cette classe permet aux services de streaming d'offrir une bande passante continue et contrôlée dans le but de transférer la vidéo et l'audio.
- Interactive. Elle est consacrée à des échanges entre le client et le réseau sous forme de requête et de réponse.
- Background. Cette dernière classe requiert un minimum d'interactivité et tolère des transferts par lots sans transmission en temps réel.

3. INDICATEURS CLE DE PERFORMANCE.

Afin de pouvoir étudier, gérer et maintenir un réseau, un certain nombre de paramètres relatifs à celui-ci sont vérifiés. Les performances d'un réseau UMTS se mesurent en prenant en compte les cinq piliers suivant :

- L'accessibilité
- L'intégrité
- La maintenabilité
- La disponibilité
- La mobilité

En effet, il existe des outils de gestion de performances, dont la responsabilité est de collecter automatiquement les statistiques de performances générées par les différents éléments des réseaux mobiles 3G/4G. Ce travail est fourni en temps quasi-réel et il est basé sur un concept de compteurs tels que le nombre de connexions simultanées, la puissance consommée ou même la valeur des interférences.

4. LIMITATION DE LA 3G :

Dès le lancement de la technologie UMTS, celle-ci est devenue obsolète. Les limitations du réseau UMTS proviennent de plusieurs sources et en premier lieu, le débit se révèle insuffisant pour transporter des données lourdes. D'un débit réel de 384 kbit/s, les applications sur la 3G restent limitées. De plus, à la commercialisation de cette technologie et pour éviter les problèmes de congestion, les opérateurs ont opté à des limitations de la bande passante allouée à chaque utilisateur à une centaine de méga par mois.

La 3G est maintenant presque partout présente au monde à ce jour, même si l'investissement pour son déploiement et son infrastructure a coûté cher. A noter également que le client était contraint à changer son téléphone portable par un compatible et prenant en charge la nouvelle technologie.

L'insatisfaction des utilisateurs, et leur besoin insatiable en un réseau de haut débit a poussé les opérateurs à concevoir un autre réseau plus performant au niveau du débit. De ce fait, la technologie HSPDA est créée avec un débit de l'ordre de 1,8 Mbit/s en première version. Toutefois, les évolutions ne cessent de prendre part à notre quotidien et ainsi apparaît la quatrième génération.

III. LA 4EME GENERATION / LONG TERM EVOLUTION

LTE (Long Terme Evolution), connue sous le nom de la 4G, est la dernière technologie sans fil apparu. Elle est basée sur des techniques radios telles que l'OFDMA et le MIMO, permettant le transfert de données à très haut débit, avec une portée plus importante, un nombre d'appels par cellule supérieur et une latence plus faible.
Les réseaux LTE sont des réseaux cellulaires constitués de milliers de cellules radio qui utilisent les mêmes fréquences hertziennes. Ceci permet d'affecter à chaque cellule une largeur spectrale plus importante, variant de 3 à 20 MHz, et donc d'avoir une bande passante plus importante et plus de débit dans chaque cellule.

1. ARCHITECTURE DU RESEAU LTE

L'architecture du réseau LTE, comme elle est montrée dans la figure suivante, est constituée de 2 parties :

- Une partie radio e-UTRAN

- Un réseau de cœur EPC (Evolved Packet Core)

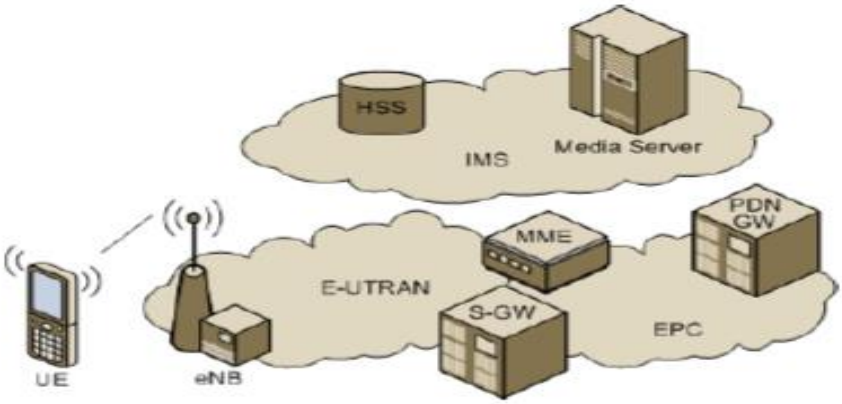


Figure 11 : ARCHITECTURE LTE [13]

Réseau d'accès E-Utran :

La seule entité présente dans l'E-UTRAN est l'eNodeB qui peut être assimilé à un Node B plus un RNC. L'eNodeB est le responsable de la transmission et de la réception radio avec l'UE. Les fonctions supportées par le RNC ont été réparties entre l'eNodeB et les entités du réseau cœur MME/SGW.

Réseau cœur EPC :

Ce domaine est constitué de plusieurs entités :

- MME (*Mobility Management Entity*), représente le nœud principal de contrôle du réseau d'accès LTE/SAE. Cette entité manipule un certain nombre de fonctionnalités telles que:
  - Le suivi des UE en Mode Inactif
  - L'activation / désactivation du Bearer
  - Le choix du SGW pour un UE
  - Le handover Intra-LTE impliquant la location du noeud du réseau d'accès
  - L'interaction avec le HSS pour authentifier un utilisateur en attachement et implémentation des restrictions d'itinérance
  - Elle fournit des identités temporaires pour les utilisateurs
- SGW (*Serving Gateway*) est la passerelle de service SGW dont l'objectif principal est de gérer la mobilité du plan utilisateur, elle agit également comme une frontière principale entre le Radio Access Network (RAN) et le réseau cœur. La SGW maintient également les chemins de données entre les eNodeBs et les passerelles PDN. De cette façon le

SGW forme une interface pour le réseau de données par paquets à l'E-UTRAN. Aussi quand les UEs se déplacent dans les régions desservies par des eNodeBs, la SGW sert de point d'ancrage de mobilité veillant à ce que le chemin de données soit maintenu.

- PGW (*PDN Gateway*) De même que le service GW, la passerelle PDN est le point d'ancrage des sessions vers les réseaux de données externes, la PDN GW soutient également des fonctions d'application de la politique (qui appliquent des règles définis par l'opérateur pour l'allocation des ressources et de l'utilisation), ainsi que le filtrage de paquets (comme l'inspection approfondie des paquets pour la détection de signatures de virus) et support de charge évolué (comme par URL charge).

2. QUALITÉ DE SERVICE ET PCRF :

PCRF (*Policy and Charging Rules Function)* est une entité importante dans le domaine de réseau de base LTE, initialement introduite dans 3GPP. Elle est principalement responsable de la politique de décision et de contrôle des décisions. En d'autre terme, si un utilisateur a besoin d'une meilleure qualité de service, alors il est de la responsabilité de PCRF de lancer la QoS avec des instructions d'IMS. Ses principales fonctionnalités sont listées ci-dessous :

- Fournir des informations de qualité de service au paquet de la passerelle
- Dynamiquement gérer et contrôler les sessions de données.
- Appliquer les paramètres de qualité de service minimum.
- Déterminer la politique de tarification pour les paquets.

3. LIMITATIONS DE LA 4G

La quatrième génération, bien que pas encore commercialisée partout dans le monde, elle se fait une place parmi les autres technologies existantes. En effet, la première offre mobile en 4G utilisant le standard LTE a été lancée dans les villes de Stockholm (Suède) et Oslo (Norvège) le 15 décembre 2009. Cependant, les téléphones mobiles compatibles n'ont apparu qu'une année plus tard par le constructeur Samsung.

Les limitations de la 4G sont rares à ce jour, du fait que la technologie n'est pas encore bien lancée. Cependant, les chercheurs estiment que pour des raisons de coût, elle sera difficilement acceptée par le consommateur, qui cherche à avoir un réseau de très haut débit à moindre coût.

Techniquement, pour des contraintes de batterie, les noeuds mobiles seront limités à un petit nombre de radios d'adaptation qui doivent être capables de fonctionner dans un certain nombre de modes de communication pris en charge et sur une gamme de fréquences.

CONCLUSION :

A travers l'aperçu général sur les réseaux 3G, 4G et Wi-Fi. Nous avons essayé de relever les différentes limitations des réseaux de troisième et de quatrième génération afin de voir l'apport de la nouvelle technologie de l'offload. La partie du Wi-Fi liste les caractéristiques de celui-ci et les atouts qui font de lui un réseau puissant.

CHAPITRE 4

TECHNOLOGIE 3G OFFLOAD

INTRODUCTION

Le réseau 3G rencontre de nos jours un problème de congestion au quotidien. Les opérateurs ont donc adopté une solution selon leurs propres critères : coût, efficacité, qualité de service.

Parmi ces solutions se présente l'Offload 3G qui consiste principalement à décharger le réseau 3G sur un autre réseau. Celui-ci est soit formé par des Femtocells qui sont de minuscules systèmes radio 3G à faible consommation, ou un réseau d'autre nature à savoir le Wi-Fi.

Le « Wi-Fi Offload » est amené à se développer ces prochaines années pour ce qu'il offre comme solution et pour ces différents avantages. Il consiste à mutualiser les réseaux disponibles, autrement dit, profiter de toute l'infrastructure actuelle afin d'en créer des réseaux plus performants. Ceci dit, elle est basée principalement sur le basculement de la connexion Internet mobile (3G/4G) vers un réseau Wi-Fi à portée, pour désengorger les réseaux des opérateurs. Etant donné leur saturation et le nombre de points d'accès Wi-Fi à travers les territoires, le basculement Wi-Fi semble être une démarche de bon sens. Ce basculement tendra à devenir automatique, et complètement transparent, sans que la moindre coupure de connexion soit occasionnée.

Actuellement, cette nouvelle technologie n'a pas encore connu un lancement remarquable. Nous remarquons que le trafic des Data passe toujours à travers les réseaux mobiles. Cependant, elle prendra un essor remarquable à partir de 2016 où les trafics à travers ces réseaux et l'offload commenceront à s'égaliser (***Mark Poletti, CableLabs).***

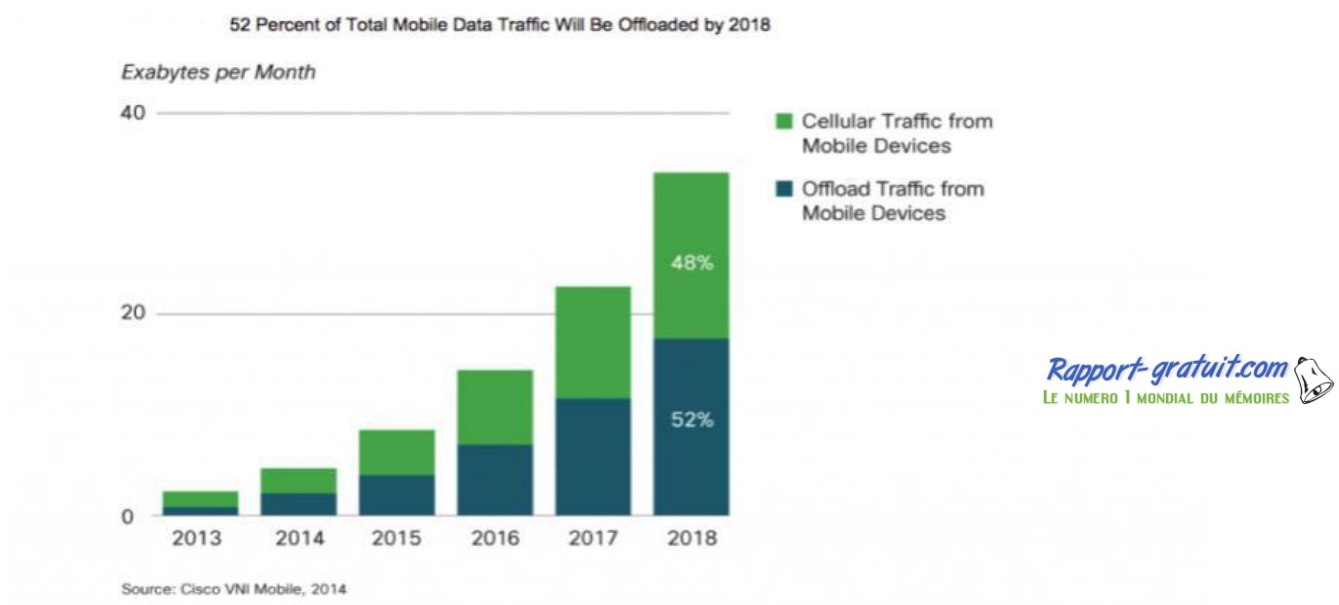


Figure 12 : EVOLUTION DE LA TECHNOLOGIE 3G OFFLOAD [14]

I. HISTORIQUE

La technologie 3G offload est toute récente, répondant ainsi à la congestion des réseaux 3G. Elle a connu un essor considérable les deux dernières années vu le taux de congestion que connaissent les réseaux 3G. Cette technologie a été déployée au monde entier. Plusieurs intégrateurs se sont mis à l'étude de cette technologie et à son déploiement. Parmi ces intégrateurs :

- Aptilo networks est un fournisseur mondial de télécommunications basé à Stockholm. Ils ont la charge de produire et commercialiser des systèmes et des solutions réseaux télécoms, notamment les réseaux mobiles 3G, LTE, WiMAX, Wi-Fi. Parmi les produits de la société, les serveurs Radius, les serveurs AAA, les Hotspots Wi-Fi et les solutions PCRF.

- Runcomest la raison derrière de la technologie OFDMA. Elle développe, fabrique et commercialise une large gamme d'équipements et de systèmes fonctionnant le réseau 4G à travers le monde. Le pionnier reconnu dans le développement de la technologie Orthogonal Frequency Division Multiple Access (OFDMA). Fondée en 1997 par le Dr Zion Hadad, et basée à Rishon Le Zion à Israël, la société possède un portefeuille important et une liste considérable de solutions. Elle emploie quelques-uns des plus grands experts mondiaux de la technologie sans fil à large bande. Entre 2008 et 2010, Runcom a déployé plus de 3000 stations de base et plus de 300 000 terminaux à travers le monde.

- Ruckus Wireless a développé une architecture de référence et a construit à cet effet des systèmes Wi-Fi pour les fournisseurs qui abordent un grand nombre des préoccupations face à l'intégration du Wi-Fi dans la grande infrastructure de l'opérateur mobile. Ils sont leader sur le marché des infrastructures réseau et proposent une large gamme de produit.

II. CONTEXTE REGLEMENTAIRE DU WI-FI OFFLOAD AU MAROC

L'Agence Nationale de Réglementation des Télécommunication (ANRT) a été créée pour réguler le secteur des télécommunications, en veillant au respect des règles d'une concurrence saine et loyale. Par ses actions, telles l'analyse des marchés, la fixation des prix d'interconnexion, la prévention des pratiques anticoncurrentielles, le pilotage des projets du Service Universel, l'Agence œuvre à universaliser l'accès aux télécommunications, à préserver les droits des usagers et à réduire la fracture numérique [16].

Une décision concernant l'installation et l'exploitation de réseaux Wi-Fi outdoor a été prise par le directeur général de l'ANRT M. Azdine EL MOUNTASSIR BILLAH le 5 avril 2013. La décision comporte 9 articles et M. le directeur :

- A autorisé un déploiement libre des réseaux Wi-Fi outdoor au Maroc (sans assignation de fréquences, ni paiement de redevances de fréquences) par les exploitants de réseaux publics de télécommunications terrestres autorisées à fournir des services de télécommunications fixes et mobiles.

- A charger l'ANRT de lancer le processus de réaménagement du spectre des fréquences nécessaires à l'exploitation des technologies Wi-Fi outdoor avec les utilisateurs actuels de cette bande et à fixer les conditions techniques d'exploitation de la bande de fréquences Wi-Fi outdoor [17].

III. POURQUOI CHOISIR LE WI-FI

Pour faire face au problème de congestion des réseaux 3G, les opérateurs ont eu le choix entre plusieurs approches : élargir le réseau, basculer sur des Femtocells qui doivent être mis en place avec le réseau existant ou encore basculer sur le réseau WiMax ou le Wi-Fi. Le dernier choix était le plus favorisé pour plusieurs raisons.

Pour commencer, le Wi-Fi offload est la solution la moins couteuse à appliquer. En effet, la transmission de DATA sur le réseau Wi-Fi est 90% moins couteuse que la transmission de DATA sur un réseau 3G. D'après GreenPacket, l'offloading de DATA sur un autre réseau comme le Wi-Fi peut potentiellement engendrer des économies. D'où l'avantage du Wi-Fi par rapport aux Femtocells. D'autre part, le réseau WiMax n'est pas encore déployé par plusieurs opérateurs dans le monde, ce qui pose un problème de disponibilité limitant les chances de ce choix par rapport au Wi-Fi. De plus, la majorité des équipements vendus actuellement comme les Smartphones et les tablettes disposent de la fonctionnalité Wi-Fi. En contrepartie, le WiMax souffre encore d'un problème de compatibilité avec un grand nombre d'équipements utilisés actuellement par les abonnés mobile. D'où l'utilisation du Wi-Fi semble plus facile et pose moins de contraintes que l'utilisation du réseau WiMax ou des Femtocells.

Le Wi-Fi utilise une bande de fréquences (bande ISM) autre que celle utilisée par les réseaux radio des opérateurs ce qui permet de réduire les chances d'interférences entre les deux réseaux. Enfin, un autre avantage du Wi-Fi, est la stabilité de la connexion qu'il peut offrir, soit à l'intérieur ou à l'extérieur des bâtiments si nous utilisons une architecture maillée formée par les points d'accès (réseau Mesh). Pour tous ces avantages, plusieurs opérateurs tel que Free, l'opérateur le plus préféré en France, ont déjà commencé à utiliser le wifi offload 3G comme solution pour la congestion à laquelle fait face leur réseau 3G. Cependant, il existe toujours des contraintes de passage du réseau 3G au réseau Wi-Fi qui concernent surtout la sécurité des données échangées sur le Wi-Fi, vu sa vulnérabilité aux attaques extérieurs et au piratage.

IV. PRINCIPE DE FONCTIONNEMENT

L'opération de DATA offload du 3G vers le Wi-Fi peut être assurée par une simple application au niveau de l'équipement mobile qui commute entre les deux réseaux radio. Cette méthode se caractérise par sa simplicité, mais en contrepartie, elle présente quelques limites. Pour cela, la 3GPP a introduit la mobilité Wi-Fi (Wi-Fi mobility) au niveau de la release 8, pour assurer un Handover transparent ou Seamless Handover entre le réseau 3G et le réseau WLAN, comme amélioration du concept d'I-WLAN déjà introduit au niveau de la release 6.

Et toujours dans la recherche d'une meilleure qualité de service et de basculement entre les deux réseaux, la 3GPP a introduit l'IP Flow mobility qui permet aux opérateurs de contrôler le passage d'un réseau à un autre, selon la nature des applications et les flux de données en question.

V. AVANTAGES ET INCONVENIENTS

En plus du coût attractif du basculement, bien moins élevé que les autres solutions de désengorgement des réseaux mobiles, le recours aux réseaux Wi-Fi présentent de nombreux intérêts pour les opérateurs :

- La totalité des équipements mobiles vendus actuellement disposent de la fonctionnalité Wi-Fi (ordinateurs portables, smartphones, tablettes, etc.)
- Le Wi-Fi utilise des spectres de fréquence autres que ceux détenus par les opérateurs
- Les points d'accès Wi-Fi proposent une connexion stable non seulement en intérieur, mais également à l'extérieur des bâtiments. Ils proposent un maillage particulièrement dense dans les centres villes.
- En revanche, lorsque l'opérateur fait basculer une connexion d'un réseau mobile vers un hotspot Wi-Fi public, sans que l'utilisateur puisse réellement s'en apercevoir, cela peut s'avérer dangereux pour lui et ses données personnelles.

Contrairement aux Femtocells, qui demandent à l'opérateur de sensibiliser ses clients à leur installation et leur utilisation, l'usage du Wi-Fi est plus facile, et requiert moins l'attention des souscripteurs.

VI. ARCHITECTURE GLOBALE [18]

La plupart des réseaux actuels sont basés sur le réseau 3G/4G. L'enjeu de la technologie nouvelle est de profiter de l'infrastructure déployée afin d'alléger la charge sur ces réseaux cellulaires. De plus, le projet de partenariat de la troisième génération (3GPP) définit deux types d'accès Wi-Fi différents : un accès sûr ou approuvé et un accès pas sûr. Ce dernier regroupe tous les types d'accès non sécurisés (sans authentification et sans chiffrement), ou

qui ne sont pas contrôlés par l'opérateur. Le second type réfère aux accès sécurisés et contrôlés.

Quand le réseau Wi-Fi est utilisé pour la décharge des données mobiles, celui-ci devrait prendre en compte les trois points suivants :

- L'authentification pour assurer que l'accès ne s'effectue pas que pour les clients autorisés
- Policy and Charging Control (**PCC)** rassemblant toute les politiques concernant le trafic généré à travers l'accès Wi-Fi.
- La mobilité d'un réseau à un autre : de la 3G au Wi-Fi, ou inversement.

L'architecture du réseau Wi-Fi est composée de plusieurs parties :

- Le client voulant se connecter à Internet.
- La partie accès au réseau : à partir du réseau LTE ou Wi-Fi.
- La partie serveurs d'authentification AAA connectés à la base de données HLR, et serveur RADIUS.
- La partie passerelle et accès à Internet.

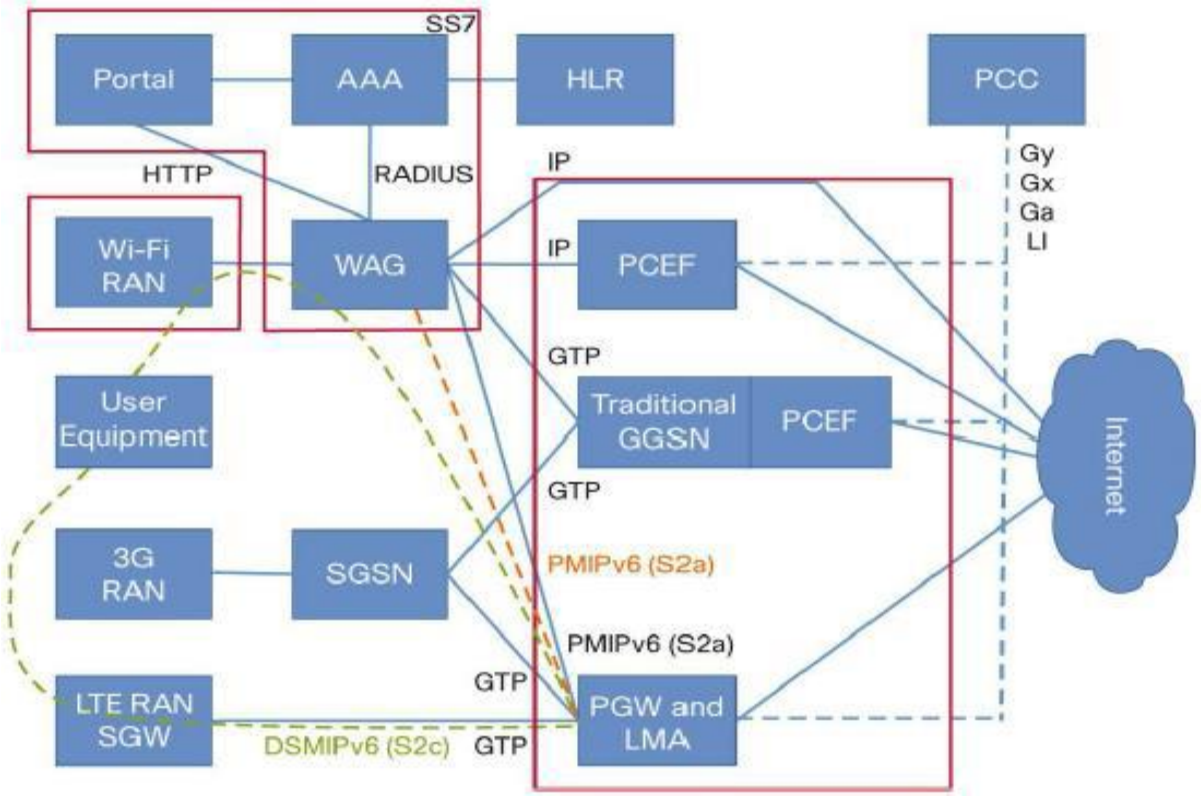


Figure 13: ARCHITECTURE GLOBALE WI-FI CISCO [18]

VII. FONCTIONNEMENT GLOBAL DE LA SOLUTION :

Prenons l'exemple d'un client voulant se connecter à Internet. Il détecte le SSID de la zone Wi-Fi dans laquelle il se trouve. En accédant à une page web, il est redirigé vers une page sur laquelle il s'authentifie. Une requête Radius est envoyée aux serveurs d'authentification qui vérifie sur leur base de données si le client est autorisé. Le retour de la requête permet au client d'accéder à la page qu'il souhaite dans le cas d'une réponse favorable.

1. TECHNIQUES D'AUTHENTIFICATION

Il existe plusieurs méthodes d'authentification qui pourront être implémentées fréquemment, deux types d'authentification sont utilisés parce qu'ils ont la caractéristique d'être destinés à plusieurs abonnés d'une part, et d'autre part, parce qu'ils permettent un accès facile au réseau Wi-Fi pour des utilisations fréquentes selon l'environnement :

- Portal-Based Authentification : pour des utilisateurs sans abonnement permanent avec l'opérateur
- EAP BASED authentification : pour les abonnés d'opérateur avec carte SIM ou certificat

EAP-BASED Authentification :

Ce type d'authentification se base sur EAP et IEEE 802.1x afin de garantir l'accès au réseau. Il se fait au niveau 2 permettant ainsi une négociation des clés de chiffrement dans le message EAP pour garantir plus de sécurité radio. En effet, les équipements avec cartes SIM encapsulent l'information dans ce message. Celui-ci transite vers le serveur AAA et par la base de données HLR, ce qui nécessite une interconnexion.

Dans ce cas de figure, la communication suit une autre envergure : L'utilisateur détecte le SSID du point d'accès de la zone où il se trouve. Celui-ci essaie de s'authentifier sur le serveur AAA en envoyant une requête EAP. Ce message contiendra son IMSI. Au niveau du serveur AAA, la session d'encapsulation démarre ; le message EAP est envoyé à la base de données HLR qui se charge du chiffrement de ce message. Une fois le message chiffré, il est ensuite envoyé au serveur AAA, qui renvoie à l'utilisateur la fin de l'étape de l'encapsulation, avec l'adresse MAC chiffrée. La carte SIM calcules et vérifie les nouvelles valeurs et transmet un message au serveur AAA. Ce dernier accuse l'utilisateur du succès de l'opération d'encapsulation et de chiffrement des données. Dorénavant, le trafic transitant est chiffré, et la clé correspondante est donnée. A partir de cette étape, le client obtient une adresse IP à partir du serveur DHCP.

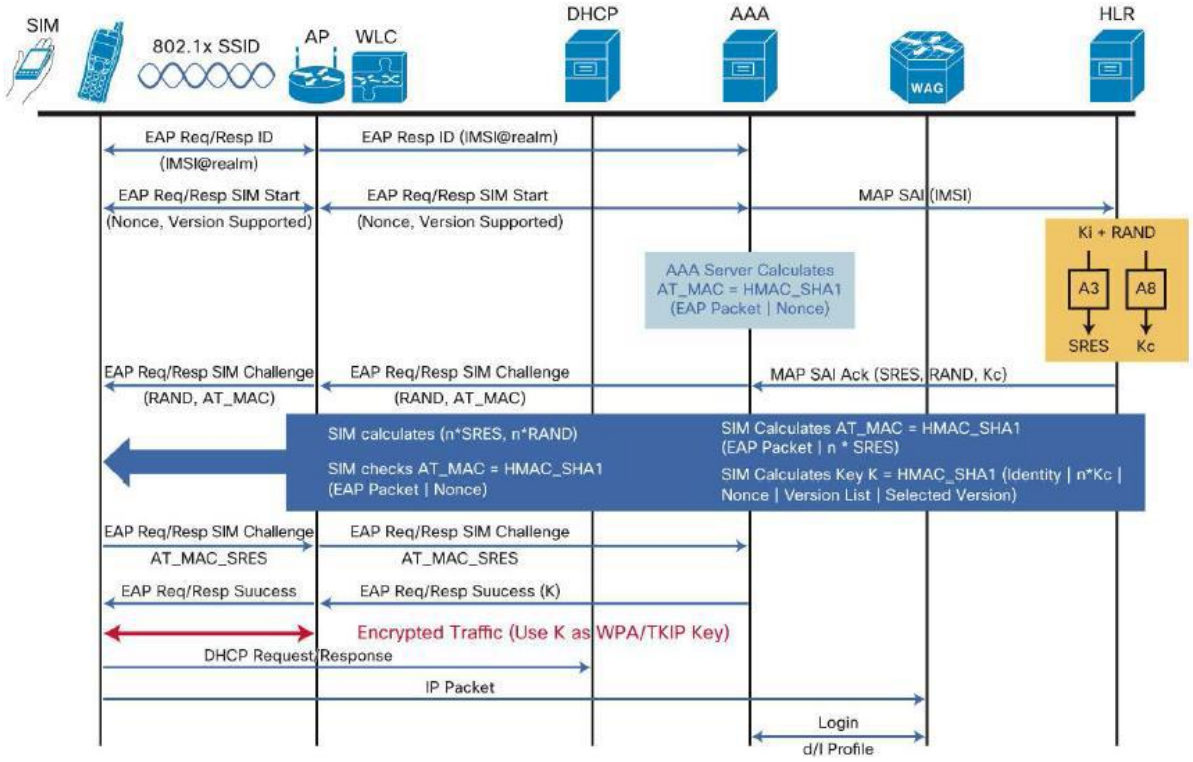


Figure 14 : ETABLISSEMENT SESSION D'AUTHENTIFICATION BASEE EAP

PORTAL-BASED Authentification :

Ce type d'authentification dépend de la connectivité au niveau 3 et de la communication HTTP. La standard WISPr (Wireless Internet Service Provider roaming) utilise également la communication HTTP avec le portail pour une authentification automatique.
L'architecture de ce type est simple et composée de :

- Accès réseau radio RAN.
- Passerelle d'accès sans fil WAG
- Serveur AAA
- Portail captif

Cette méthode repose sur le WAG qui bloque toutes les communications des abonnés non identifiés et les redirige vers un portail captif. Ce dernier demande aux utilisateurs de s'authentifier. S'ils sont autorisés, une requête est envoyée du serveur AAA au WAG qui les autorise à envoyer et recevoir des données. Les abonnés sont enregistrés

automatiquement dans le cache AAA, et sont connus par leur adresse MAC. Ceci permettrait à l'abonné de ne pas être redirigé vers le portail à chaque fois qu'il se connecte. Ce scénario passe par plusieurs étapes (comme illustré sur la figure) :

L'utilisateur détecte un SSID ouvert. Il s'associe alors au point d'accès qui lui fournit une adresse IP d'un serveur DHCP auquel il est connecté. Quand l'utilisateur rentre un URL dans son navigateur, une requête DNS est donc envoyée au WAG qui consulte le serveur AAA pour vérifier si l'adresse MAC de l'utilisateur figure sur la cache. Le serveur d'authentification renvoie une réponse au WAG qui se charge de retourner une requête DNS à l'utilisateur. Si l'authentification échoue et que l'utilisateur ne s'est jamais authentifié sur le SSID concerné, une requête http est donc envoyée au WAG qui la transmet au portail. Ce dernier s'affiche pour l'utilisateur, lui permettant de rentrer son type d'abonnement. Cette requête arrive au portail qui renvoie l'information au WAG, déclenchant ainsi une requête de type Radius vers le portail. Le retour de celle-ci arrive au niveau du WAG sous forme d'une *RadiusAccess Response.*

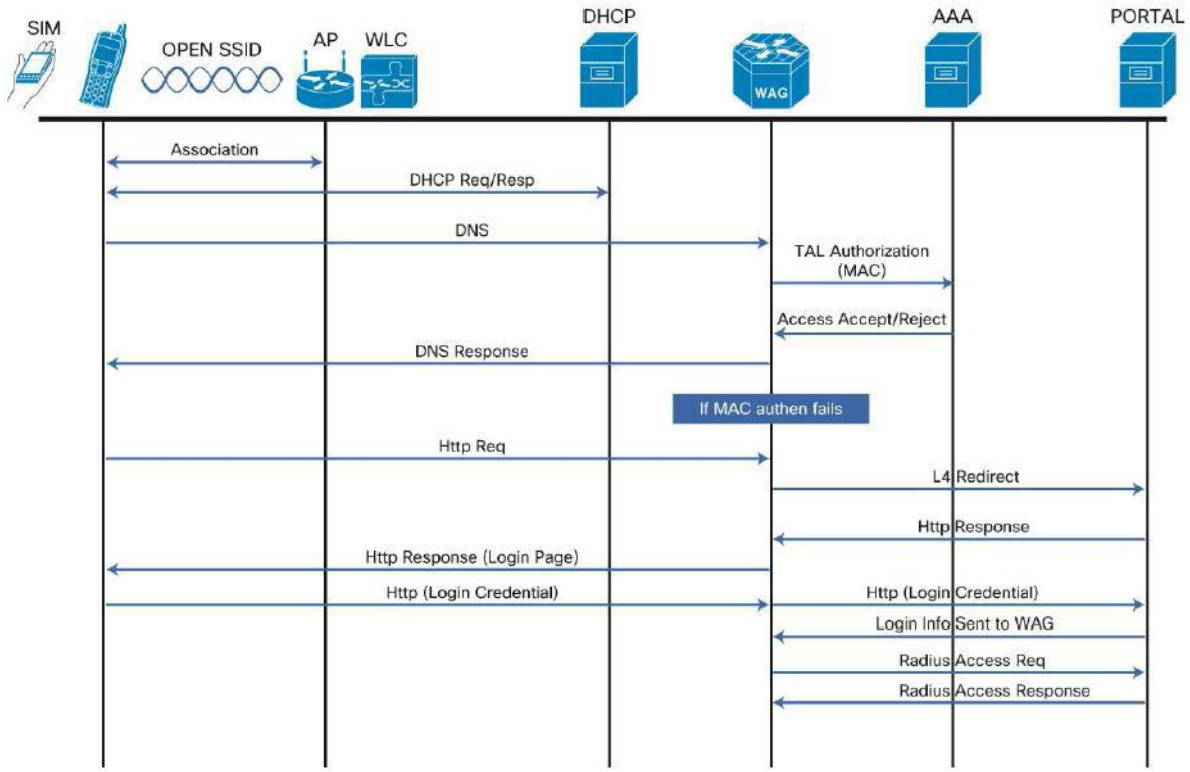


Figure 15 : PORTAL-BASED AUTHENTICATION

2. IMPLEMENTATION DU PCC (POLICY AND CHARGING CONTROL) DANS LE WIFI OFFLOAD.

Le second point important dans la 3G offload est la disponibilité d'une politique identique pour les abonnés, indépendante du réseau d'accès radio utilisé.

La meilleure approche pour l'intégration de cette politique est la réutilisation des éléments servant à déployer les services de la troisième génération. Cela dépendrait également de l'infrastructure PCC existante pour le réseau de l'opérateur mobile. Par exemple, si l'opérateur utilise un équipement avec une fonction PCC autonome, le WAG serait intégré comme étant une passerelle supplémentaire. Si maintenant le PCEF est intégré dans la passerelle du GPRS, le WAG oriente la session Wi-Fi via un tunnel par la passerelle GGSN.

Dans cette architecture, le WAG envoie les données du trafic au PCEF pour l'intégration du PCC. Le trafic qui n'a pas besoin d'être contrôlé est dirigé directement vers Internet.

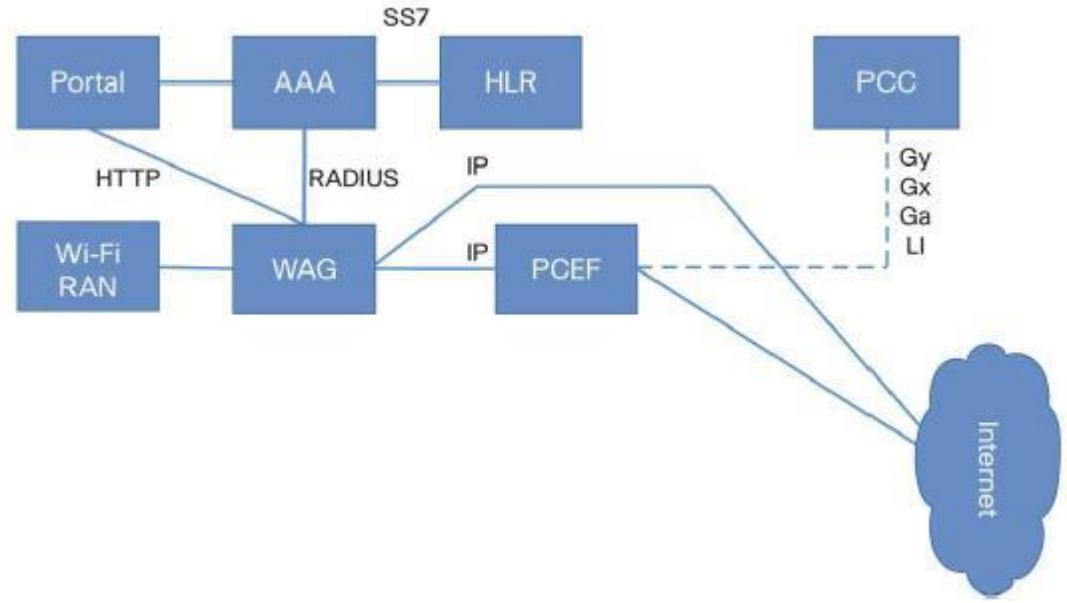


Figure 16 : ARCHITECTURE PCEF

Le PCEF devrait pouvoir corréler l'identité de l'utilisateur et les données transitant par lui, un mécanisme est alors implémenté dans le but de synchroniser l'identité de l'utilisateur avec l'adresse IP de l'abonné. Parallèlement, le proxy Radius sur le PCEF crée une session d'information de l'utilisateur.
Si ce modèle est déployé, l'opérateur s'assure que l'information nécessaire au PCEF est incluse dans le message Radius venant de la passerelle d'accès ou filtré par le serveur AAA. Des informations supplémentaires sont requises, telles que l'identité de l'abonné mobile international, le point d'accès associé…

Le PCEF est une partie intégrante du GGSN. La meilleure solution pour l'intégration PCC est de forcer les sessions Wi-Fi à un tunnel GTP. Ainsi, le trafic qui n'appartient pas à l'abonné de l'opérateur et qui ne peut pas être géré par le GGSN est orienté directement vers Internet. Cette solution présente l'inconvénient de ne pas assurer un handover transparent des sessions IP entre les réseaux Wi-Fi et 3G. Ceci vient du fait que l'utilisateur a la capacité de se connecter simultanément sur le Wi-Fi et sur la 3G.

Remarques

Lors de l'intégration d'une politique et des règles de contrôle, il faut prendre en compte la liste des options valables et nécessaires pour la 3G, la capacité du WAG à fournir les informations nécessaires et les utilisateurs non abonnés.

CONCLUSION

Ce chapitre nous a donné un aperçu sur l'historique du déploiement de la solution de l'offload dans le monde. Au Maroc, cette nouvelle technologie a été déployée aux deux villes, El Jadida et Casablanca, par l'opérateur Inwi sous le nom de « Wifi 7dak ». l'ANRT de son côté, a autorisé le déploiement de la technologie pour ce qu'elle présente comme avantages contre la congestion des réseaux mobiles. Nous avons ensuite détaillé l'architecture de cette technologie, et nous avons vu le standard de son fonctionnement donné par Cisco. La solution fait appel à des techniques d'authentification basées sur le protocole EAP.

Chapitre 5 :

PROJET de WIFI Outdoor « WIFI-7DAK »

Introduction :

Le WiFi Outdoor est une technologie qui permet de se connecter à l'internet avec un débit relativement élevé à l'extérieur et à partir de n'importe quel équipement (Pc ou Telephone) La réglementation de l'ANRT tombe à point nommé, pour les opérateurs nationaux, surtout Inwi qui a lancé le projet « WIFI_7DAK » à ELJADIDA, avec une ambition de faire bénéficier les habitants de cette ville de ce service avec une couverture de qualité et un tarif accessible, dans ce chapitre nous allons parler en détails sur ce projet.

I. Présentation de projet :

1. Contexte général de projet :

Inwi est le premier opérateur de télécommunications marocain à déployer la technologie de Wifi_outdoor. L'opérateur répond ainsi à une des recommandations clés de l'Agence nationale de réglementation des télécommunications (ANRT) concernant le développement du haut débit et du très haut débit au Maroc. Le Wifi Outdoor ou Wifi communautaire permet l'accès, depuis de larges zones urbaines au même niveau de débit qu'offre une connexion Wifi classique. Wifi 7dak offre ainsi un plus grand confort de navigation et permet un meilleur accès aux différents contenus web (vidéo, réseaux sociaux, etc.)

Ce projet est un premier pas vers la technologie Oflload, le Wifi outdoor se veut donc une solution d'appoint accompagnant le déploiement de la 4G, et le Wifi-classique, couvrant par conséquent les zones à haut trafic en l'occurrence les écoles, universités, parcs publics et autres. Techniquement, Inwi renforce le wifi7dak sans recourir à de nouveaux sites. A cet égard, les travaux de câblages n'ont pas eu lieu garantissant ainsi le confort des citoyens.

2. Présentation de système de projet [19] :

Les équipements principaux qui constituent le super réseau wifi de la ville EL JADIDA sont :

- Altai A8EI-n Super WiFi Base Station
- Altai A2/A2e WiFi Bridge
- Altai B5 WiFi Bridge
- Altai C1 Super WiFi CPE
- Altai Wireless Management System (AWMS)

Le réseau wifi de la ville a une architecture fonctionnelle qui se compose de trois parties, le réseau de cœur, le backhaul et le réseau d'accès comme il est illustré dans la figure suivante :

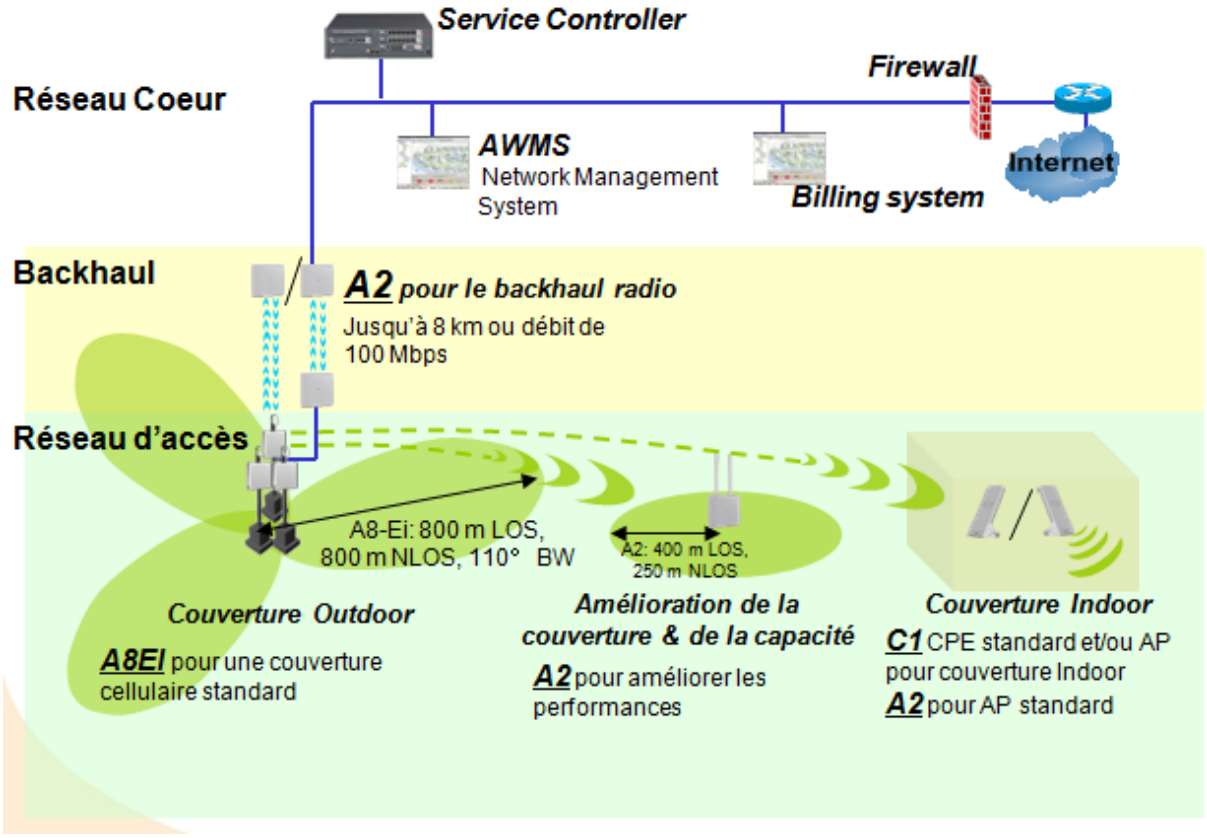


Figure 17 : les composants de réseau super Wifi

II. Les équipements actifs de système [20]:

On peut diviser les équipements actifs mobilisés dans le cadre du déploiement de projet Wi-Fi7dak en quatre catégories des équipements Indoor, des équipements Outdoor, des équipements utilisé coté client et des applications de gestion réseau à distant :

1. Les équipements radio Altai Indoor :

- **Point d'accès ALTAI A2 :**

Le point d'accès Wi-Fi A2 (point d'accés / pont) d'ALTAI est conçu pour être utilisé dans les systèmes Super Wi-Fi pour les zones de grande densité et pour couvrir les zones où le signal est faible ou inexistant à cause des obstacles. En effet, le A2 ne peut pas être seulement utilisé pour de la couverture WIFI mais aussi pour assurer l'interconnexion point-à-point entre deux site distant.

Figure 18 : point d'accés Altai A2

Caractéristique de A2:

LOS : 450 m

NLOS : 12 Km

débit : 300 Mbps

- **Point d'accès ALTAI A2e :**

Le point d'accès Wi-Fi (AP/Bridge) A2e de ALTAI est conçu pour être utilisé dans les systèmes Super Wi-Fi directionnels avec un débit très élevé. Il permet aussi de réaliser une liaison sans fil point-à-point entre deux sites distants. Il est capable de fournir le maximum de débit et de capacité que la norme 802.11n peut offrir.
Le A2e fournit 2 ports externes permettant à l'utilisateur de choisir la capacité d'antenne voulue pour se conformer à une exigence spécifique de distance et de débits, et de choisir le type de panneau d'antenne pour les applications point-à-point ou multipoints.
L'A2E peut être utilisé comme un point d'accès autonome pour la couverture directionnelle. Il peut fournir une longue couverture dans la bande de fréquences 2.4 GHz. Il permet aussi d'augmenter la capacité du réseau à faible coût.

Figure 19 : point d'accès A2E

Caractéristique de A2E :

Distance de couverture : 900 m

distance de backhauling : 50 Km

débit : 300 Mbps

- **Point d'accès ALTAI A2ei :**

Le ALTAI A2ei est conçu pour être utilisé sur le système Super Wi-Fi 2.4 et 5 GHz dual-band pour les zones Outdoor et Indoor. Il permet d'augmenter la capacité du système, d'étendre la couverture et de couvrir les zones où le signal est faible ou inexistant
Le A2ei, peut être utilisé comme un régénérateur du signal, afin d'augmenter la capacité de n'importe quel système. Il supporte aussi le PTMP Bridging utilisé pour les réseaux des campus, des villes ou de vidéosurveillance.

Figure 20 : ALTAI point d'accès A2EI

Caractéristique de A2-EI :

LOS : 450 m

NLOS : 12 Km

débit : 300 Mbps

2. Équipements Radio ALTAI Outdoor :

- **Antennes ALTAI A8n :**

L'A8n est le premier point d'accès Outdoor sans fil 802.11n au monde optimisé pour une couverture maximale et un débit élevé à partir d'un nombre minimum de sites d'installation.

L'A8n a été conçu pour fournir aux opérateurs une meilleure couverture et capacité sans protocoles compliqués de gestion de réseau ou besoin d'une haute densité d'émetteurs en particulier en environnement NLOS.

Les antennes peuvent être configurées pour fournir une couverture optimisée d'une zone en Outdoor grâce à la flexibilité d'installation de ces antennes externes 2.4GHz.

Figure 21 : couverture sectorielle avec une A8n

Caractéristique :

A8n 11n 90° to 360°	Radius
LOS / CPE	2,700 m
LOS Laptops / Smartphones	1,000 m
NLOS Laptops / Smartphones	500 m
LOS Backhaul 5GHz	10 km

Figure 22 : tableau de caractéristique de l'A8-EI

L'A8n peut être déployé en collocation avec les réseaux 3 G existants, afin de fournir une large couverture à haut débit avec un faible coût (OffLoading). L'A8n peut être Co-localisé sur un site GSM cellulaire existant. Ce qui permet l'acquisition immédiate du site Wi-Fi avec un coût d'exploitation beaucoup plus faible, vu que l'infrastructure passive est mutualisée.

Chaque station de base A8n dispose de huit ports d'antenne pour la connexion à quatre antennes sectorielles, chacune avec deux éléments d'antenne à polarisation croisée

- **Antennes ALTAI A8-Ein**

L'A8-Ein est une station de base multi-radio. Il fournit la meilleure couverture sectorielle par station de base, en particulier dans les environnements NLOS. Le réseau d'antennes multifaisceaux de l'A8-Ein est conçu pour fournir un maximum de 5 à 10 fois plus que la couverture de site d'un point d'accès Outdoor standard. En conséquence, jusqu'à 90% moins de sites d'installation pour la même zone de couverture.
L'A8-Ein permet d'avoir une couverture plus large et une bande passante plus grande par point d'accès, avec un coût de déploiement plus faible.

Caractéristiques d'A8-EIN :

A8-Ein 11n Sector	Radius
LOS / CPE	4,000 m
LOS Laptops / Smartphones	1,700 m
NLOS Laptops / Smartphones	800 m
LOS Backhaul	10 km

Figure 23 : caractéristiques de point d'accès A8-ein

3. Altai C1 Super WiFi CPE:

Altai super WIFI CPE est un équipement essentiel dans le système super WIFI ALTAI, il est conçu dans le but d'étendre la couverture dans les zones indoor pour une large bande connectivite.

Cet équipement emploie des algorithmes intelligents de traitement de signal et des antennes brevetées pour améliorer la qualité de signal WIFI et le débit coté client.

Figure 24 : Altai c1 super wifi CPE

4. Altai Wireless Management System (AWMS)

Le système de gestion sans fil de l'Altaï (AWMS) est une application qui fournit aux opérateurs mobiles une gamme complète des éléments de gestion pour les réseaux WiFi. Il facilite les opérations de configuration, gestion des incidents, suivi des performances et la maintenance des équipements à distant.

Figure 25 : Altai Wireless Management System

III. Présentation de l'architecture réseau :

1. Principaux connexion dans le réseau d'accès :

Le réseau WIFI Outdoor de la ville ELJADIDA est constituée de 13 sites, connectées entre eux en utilisant les liens radio d'ALTAI A2 et B5. Le site JAD-POP-ONE est le site principal qui est liée directement avec le réseau MPLS d'INWI, il est lié directement aux deux JAD 008 et JAD007 par des pont B5, l'architecture est présenté dans la figure suivante :

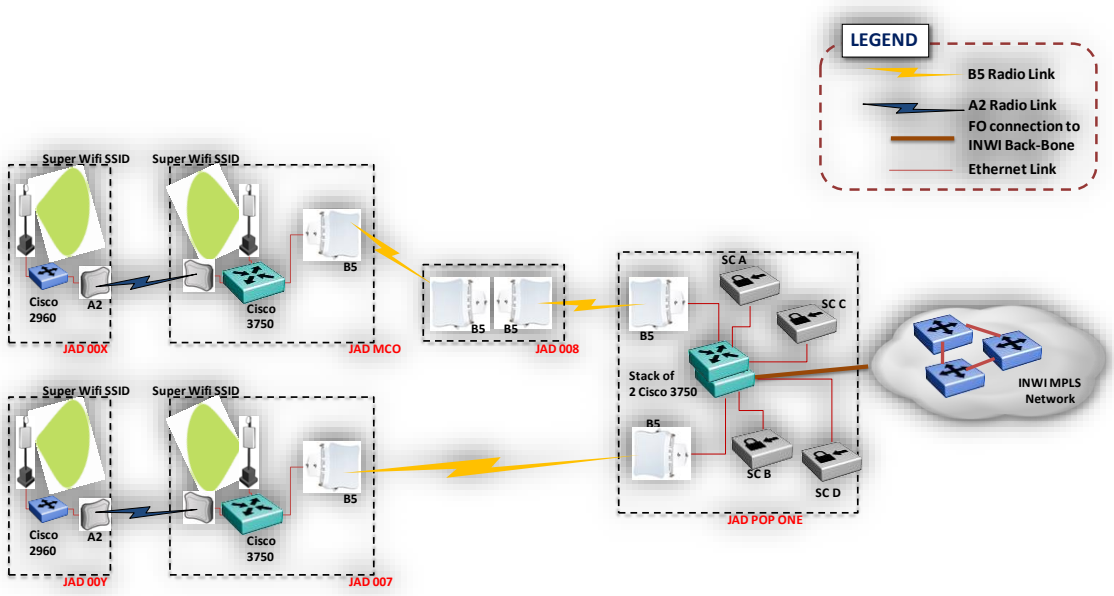


Figure 26 : le diagramme de l'architecture radio du réseau

La distribution des Switch de cette architecture dans le site JAD-POP-ONE est composé physiquement de deux Switch Cisco 3750 en parallèle. En outre, ils seront considérés dans le réseau comme un seul switch. Ces deux switch fournissent la connexion pour les B5 qui vont aux sites JAD MCO et JAD 007.

Ces switch vont fournir aussi la connexion pour les quatre redondants contrôleurs SC A, SC B, SC C et SC D.

2. Le design Backhaul :

En télécommunications, un réseau de backhaul, est un réseau intermédiaire, permettant par exemple, l'émission et la réception de données entre un centre de radio diffusion et une station terrestre d'un réseau satellite ou entre les équipements de raccordement d'abonnés (DSLAM, station de base) et le cœur des réseaux de télécommunication fixes ou mobiles.

Dans ELJADIDA, Le réseau dorsal internet est disponible seulement dans le site JAD-POP-ONE qui est loin de la ville. Le produit ALTAI B5 sera utilisé pour fournir en long distance et haut débit la connexion Ethernet sans fil entre les différents sites, les deux sites JAD-007 et JAD-MCO seront considérer comme des sites HUB pour le trafic des autres sites.

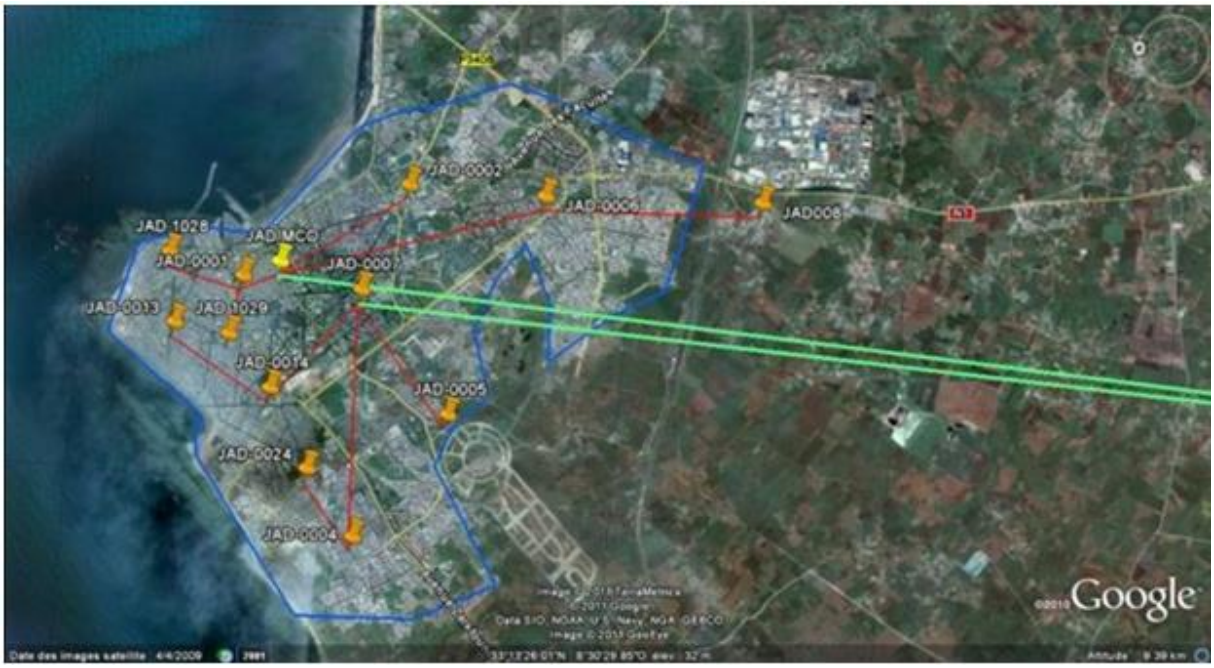


Figure 27 : vue globale des sites WIFI ELJADIDA

Dans cette figure la ligne rouge présente le lien A2 5GHz entre les différents sites, et la ligne vert présente le lien Backhaul entre le site principal et les deux sites HUB.

La figure suivante illustre le réseau Backhaul de système globale, en spécifiant le type de lien utilisé et le nombre de points d'accès dans chaque site.

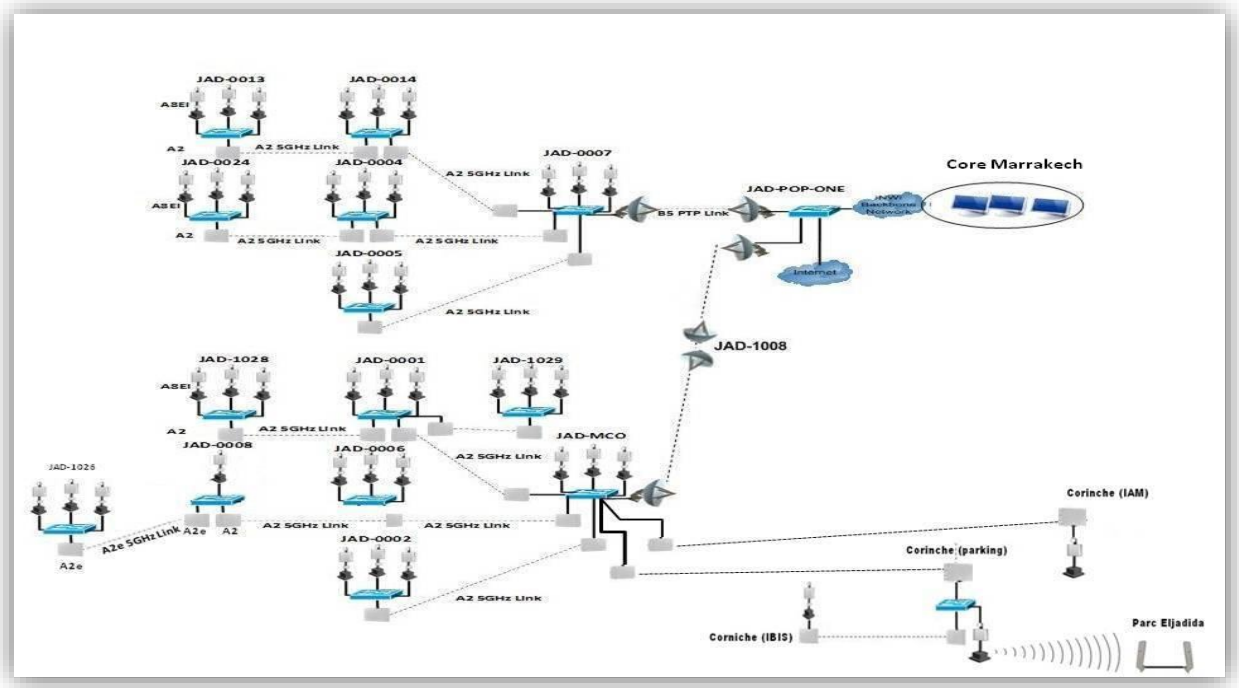


Figure 28 : la topologie backhaul

Conclusion:

Ce chapitre est une brève présentation de projet « wifi 7dak », nous avons commencé par une description des différents équipements utilisés, puis nous avons essayé de mettre le point sur le design de réseau wifi Outdoor et enfin nous avons définit la topologie backhaul.

CHAPITRE 6

REALISATIONS ET TESTS

INTRODUCTION:

Durant le stage de fin d'études, nous avons été amenés à réaliser une série de tests qui se rapporte à la nouvelle technologie de l'offload. Nous verrons en première partie les environnements qui nous ont permis de les réaliser, notamment, l'environnement matériel et logiciel. Ceux-ci nous amènent à décrire la simulation faite pour la prise en main de la solution, et finalement, les tests d'authentifications, d'accounting et de redondance demandés.

I. ENVIRONNEMENT MATERIEL:

1. ROUTEROS MIKROTIK :

Mikrotik est le nom du fabricant de matériel de réseau informatique. Il vend à la fois des composantes de réseau sans fil et des routeurs. Le produit le plus vendu du fabricant est le RouterOS Mikrotik dont le système d'exploitation est bâti sur le keernet Linux. Ce système permet de transformer un ordinateur personnel en routeur, incluant des fonctionnalités telles qu'un Pare-Feu, un serveur et un client VPN, contrôler le trafic en fonction d'une qualité de service (QOS), un accès réseau sans fil. Le système peut également être utilisé afin de créer un portail captif. Une interface graphique, nommé Winbox, est également disponible afin de configurer le système.

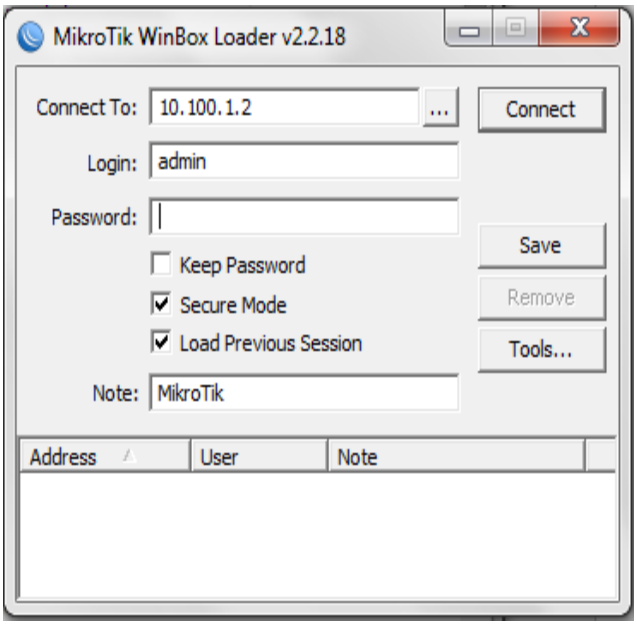


Figure 30 : Interface de Winbox

Figure 29 : Routeur Mikrotik

2. ZONE DIRECTOR RUCKUS :

Ruckus Wireless est un pionnier sur le marché des infrastructures sans fil. La société permet aux opérateurs et entreprises de rester à la pointe dans le domaine des applications et services large bande, qui connaissent une explosion de la demande.
Pour notre projet, nous avons utilisé pour une simulation de la solution un contrôleur de la famille Ruckus Wireless, ZoneDirector 1100. En effet, c'est un système de réseau sans fil intelligent et géré de façon centralisée pour les opérateurs de hotspots. Il est adéquat au besoin d'un WLAN robuste, sécurisé et facile à déployer. Le ZoneDirector se montre parfait pour les opérateurs qui souhaitent offrir des services d'accès Wi-Fi différenciés dans des sites tels que les hôtels, les aéroports ou même les écoles. De plus, Le ZoneDirector de Ruckus s'intègre facilement à l'infrastructure réseau, avec les systèmes de sécurité et d'authentification déjà en place. Il est, par ailleurs, facile à configurer grâce à un assistant Web convivial. Les points d'accès ZoneFlex de Ruckus détectent automatiquement le ZoneDirector, qui procède en retour à leur Configuration.

Toutes ces caractéristiques font de ce contrôleur, l'équipement idéal pour la réalisation de ce projet.

Figure 31 : Zone Director 1100

3. ZONE FLEX RUCKUS :

Le point d'accès Wifi ZoneFlex 7363 fonctionne dans les bandes de fréquence 2.4 Ghz en mode 802.11b/g/n et 5.4 Ghz en mode 802.11a/n. Il bénéficie des avancées technologiques de Ruckus Wireless sur la technologie radio, ce qui lui permet d'avoir une portée supérieure aux autres points d'accès du marché et une intégration très discrète. Comme l'ensemble des bornes de la gamme ZoneFlex, le ZoneFlex 7363 peut fonctionner seul en point d'accès autonome ou être géré par les contrôleurs ZoneDirector 1000. En effet, les points d'accès WiFi ZoneFlex de Ruckus sont les premiers points d'accès WiFi multimédia, gérés de manière centralisée, qui étendent la portée du signal WiFi (de 2 à 4 fois) en contournant automatiquement les interférences pour assurer une fiabilité sans précédent.

Figure 32 : Zone Flex 7363

II. ENVIRONNEMENT LOGICIEL

1. SYSTEMES D'EXPLOITATION :

Pour la réalisation de ce projet, nous avons été amenés à travailler d'une part sur des machines Windows XP, représentant le client. D'autre part, la configuration de Freeradius et de MySQL a été faite sur une machine Ubuntu.

2. OUTIL DE VIRTUALISATION VMWARE WORKSTATION

Cet outil permet de virtualiser les systèmes d'exploitation sur une machine hôte. Conçu pour les professionnels, il est caractérisé par un environnement utilisateur riche, un ensemble complet de fonctionnalités et de hautes performances. Il offre la possibilité d'exécuter plusieurs machines virtuelles au même temps, ce qui répond au besoin de réalisation de notre architecture de test. La version utilisée est la 9.0.2.

3. OUTIL DE SNIFFING WIRESHARK

Wireshark est un analyseur de paquets et de protocoles de communication. Il examine les données d'un réseau en direct et peut faire une capture des différentes communications. Il est souvent utilisé pour des raisons de dépannage et d'analyse de réseaux informatiques ou de développement de protocoles. En effet, il reconnait plus de 759 protocoles et il fonctionne sur de différents environnements compatibles UNIX, MAC OSX et même Microsoft Windows.

4. OUTIL DE SCAN DU RESEAU NET SCAN

Net Scan est un outil permettant de scanner tous les ports ouverts et les adresses IP connectées au réseau. Il offre une analyse intégrale du réseau, qu'il soit public ou privé. Il permet d'afficher l'état de connexion, les adresses IP allouées et le nom du terminal correspond à chaque adresse.

III. PHASE DE SIMULATION:

1. ARCHITECTURE :

Contexte Reel de la simulation :

Afin de simuler le projet et prendre en main les outils de la solution, nous avons procédé à des configurations d'un portail captif pour un mall. Notre objectif est de réaliser deux points d'accès, un diffusant un SSID pour les clients dans le mall, et un autre avec un SSID différent destiné aux clients d'un des magasins du mall. A la connexion d'un utilisateur sur l'SSID qui correspond à son emplacement, il devrait être dirigé vers un portail captif personnel (au mall ou au shop). Dans un premier temps, nous testons avec un seul point d'accès.

Les utilisateurs devront s'authentifier avant de pouvoir avoir accès à Internet. Cette phase d'authentification requiert la configuration du protocole Radius. Les utilisateurs auront ensuite à rentrer un numéro de Voucher leur offrant un profil de connexion particulier, en fonction de ce qui est implémenté sur la plateforme de gestion.

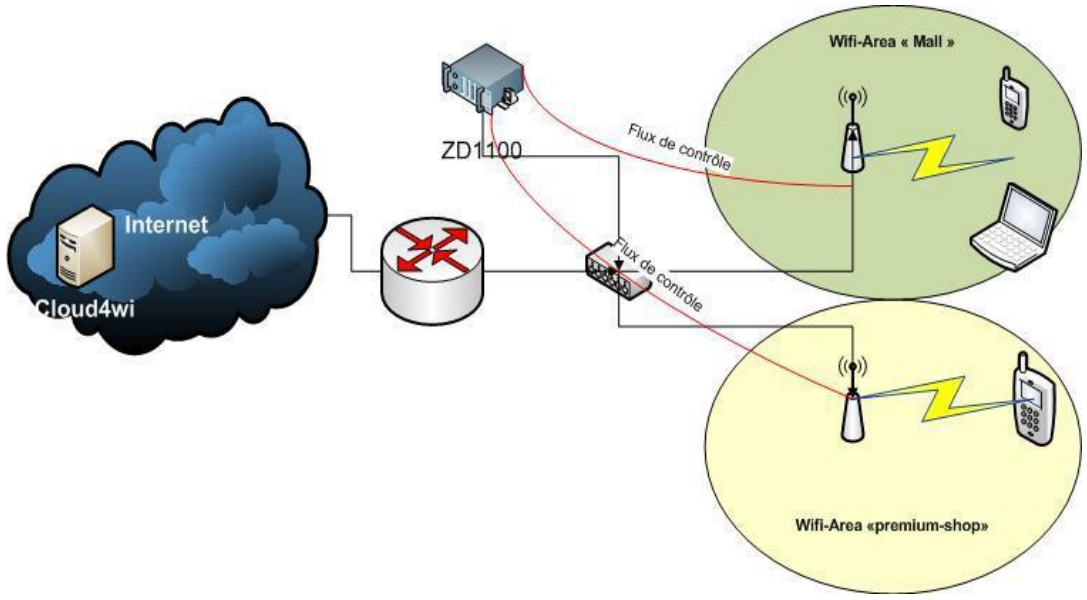


Figure 33 : Architecture CLOUD4WI [21]

2. REALISATION DE LA MAQUETTE ET CONFIGURATION DES EQUIPEMENTS :

L'architecture qui nous permet de réaliser ce test est modélisé sous Packet Tracer. La figure ci-contre montre les différentes entités de cette architecture.

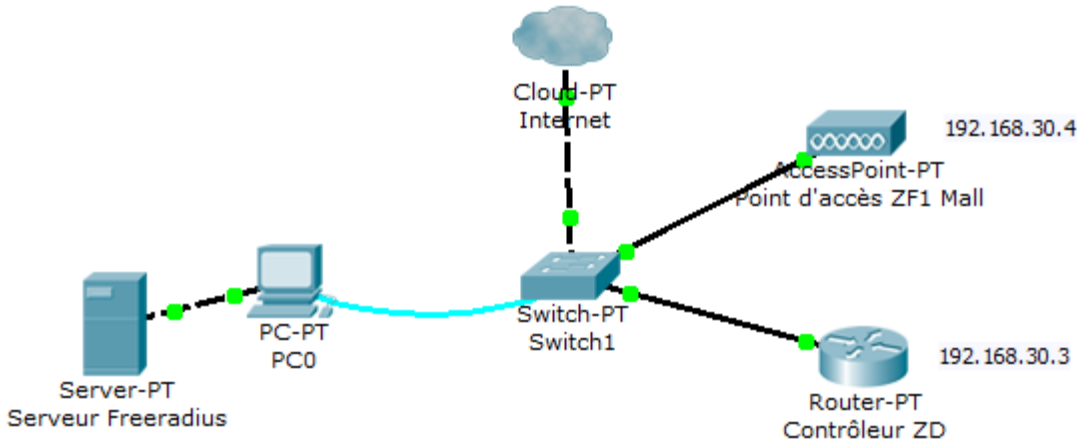


Figure 34 : ARCHITECTURE RUCKUS WIRELESS

Pour cela, nous avons connecté à un switch : un routeur Mikrotik, un contrôleur ZoneDirector, et deux points d'accès Zone Flex. L'image ci-contre montre l'interconnexion du contrôleur avec les deux points d'accès.

Figure 35 : Architecture de Contrôleur et points d'accès

Cette solution permet d'héberger des portails captifs lors de la connexion à Internet sur le Cloud et offre la possibilité d'intégrer plusieurs applications telles que les flux RSS, la météo, les infos, ou des blocs publicitaires, etc…

Le contrôleur WLC à la charge de gérer les points d'accès auxquels il est connecté. Un ensemble de point d'accès constitue ce que nous appelons une Wifi Area, groupant le même SSID pour une meilleure gestion. Le principal avantage de cette solution réside dans le fait que le trafic de contrôle passe pas le contrôleur, et le flux data est dirigé directement vers la passerelle par défaut comme montré dans la figure 33. La configuration du contrôleur se fait sur un navigateur à partir de son adresse IP.

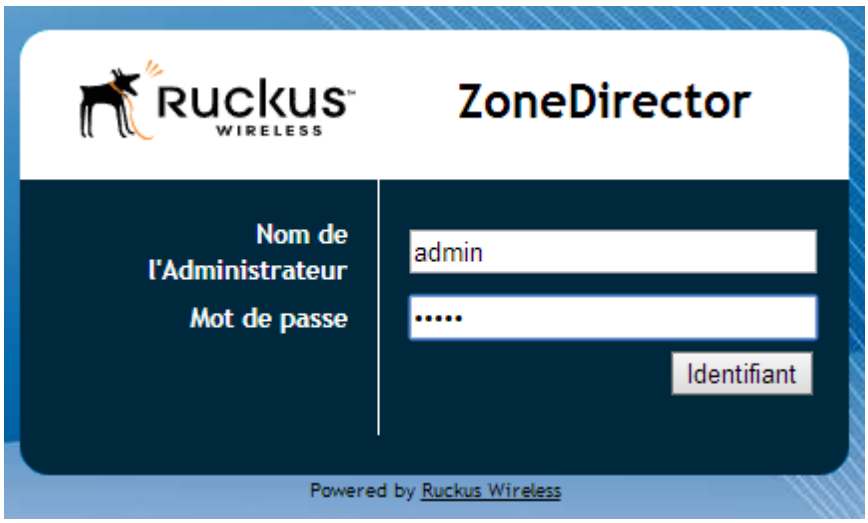


Figure 36 : connexion au ZoneDirector

Après la connexion au Zone Director, son interface de configuration comporte quatre volets : tableau de bord, supervision, configuration et Admin. La partie configuration permet de gérer les points d'accès, les utilisateurs, les services de hotspots (ce qui nous intéresse dans notre projet) et le serveur AAA.

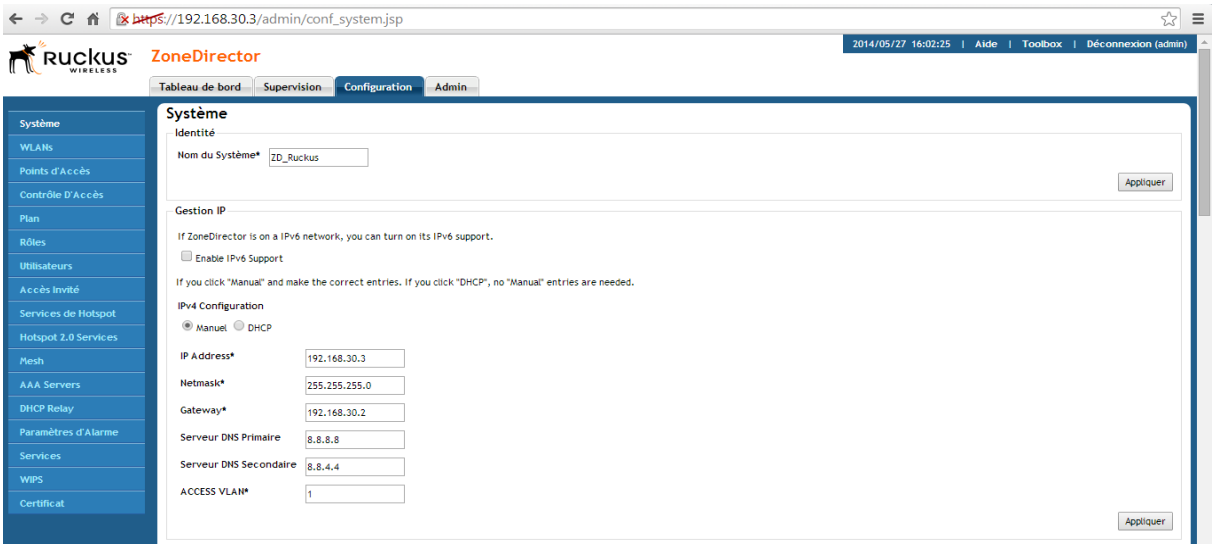


Figure 37 : Configuration des Hotspots

Les utilisateurs voulant se connecter à un réseau à travers le SSID d'un point d'accès, doivent passer par une authentification auprès d'un serveur Radius. La configuration de celui-ci est expliquée dans la figure suivante :

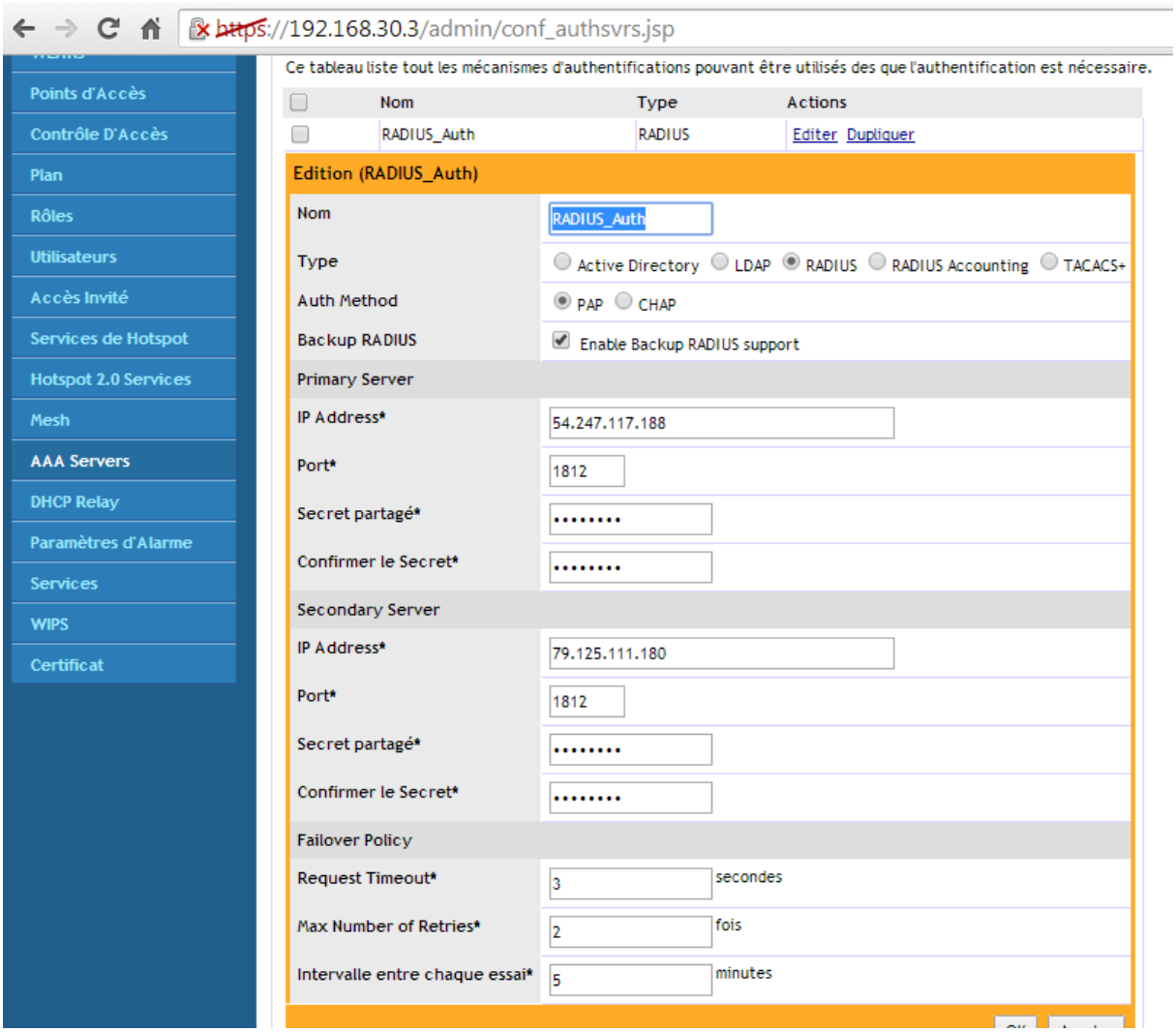


Figure 38 : Configuration du serveur RADIUS

Maintenant que toutes la configuration des adresses IP et du serveur Radius est valide, nous configurons le service de Hotspot, en spécifiant le nom et la page de départ après la connexion de l'utilisateur sur un SSID. Nous spécifions également le serveur Radius (authentification et accounting) rattaché à ce service. Nous pourrons également configurer le jardin fermé qui constitue un ensemble de page web visible à l'utilisateur après que sa durée de connexion ait expirée. La figure ci-dessous montre toutes ces fonctionnalités :

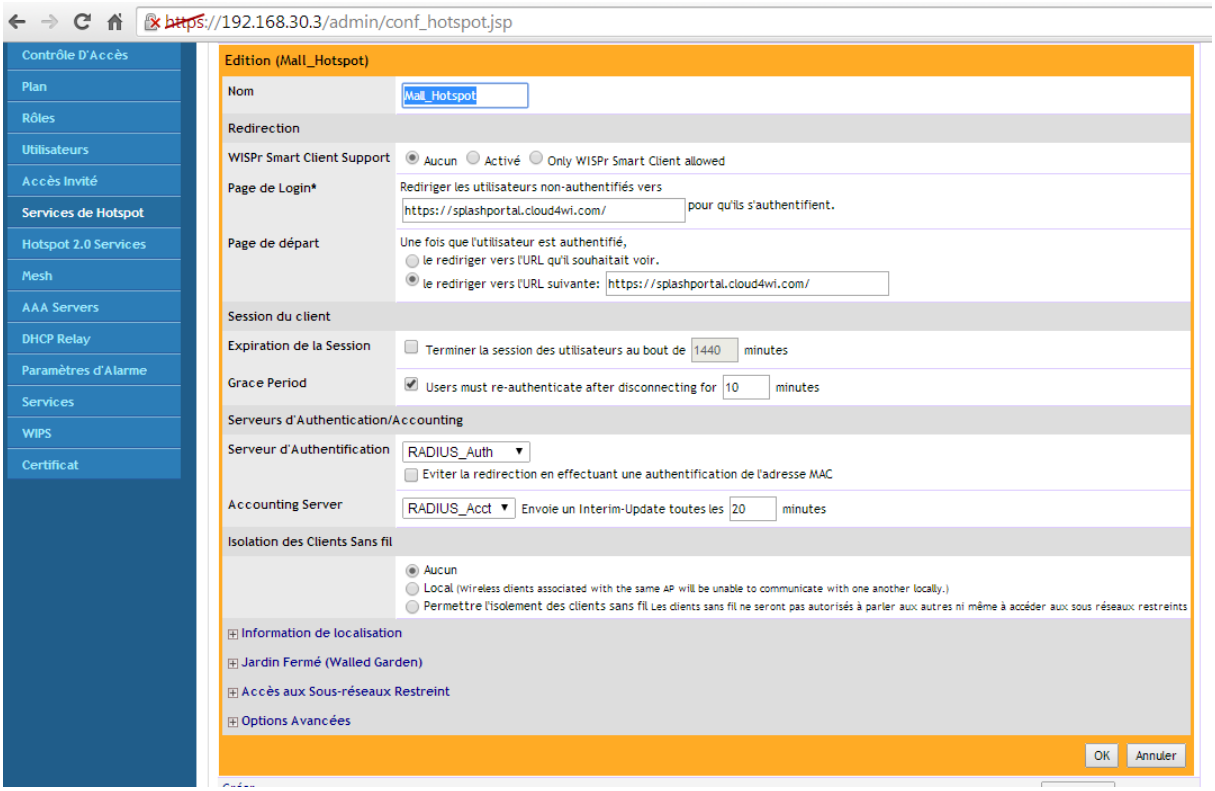


Figure 39 : Configuration de service HOTSPOT

Ceci fait, nous passons à la configuration du point d'accès. Celle-ci se fait également via un navigateur à partie de l'adresse IP de l'équipement.

Figure 40 : Connexion à la configuration du point d'accès

L'interface de configuration dispose d'une partie statut, configuration, maintenance et administration. La configuration du point d'accès ne nécessite que la mise à jour des adresses IP comme s'est montré dans la figure suivante :

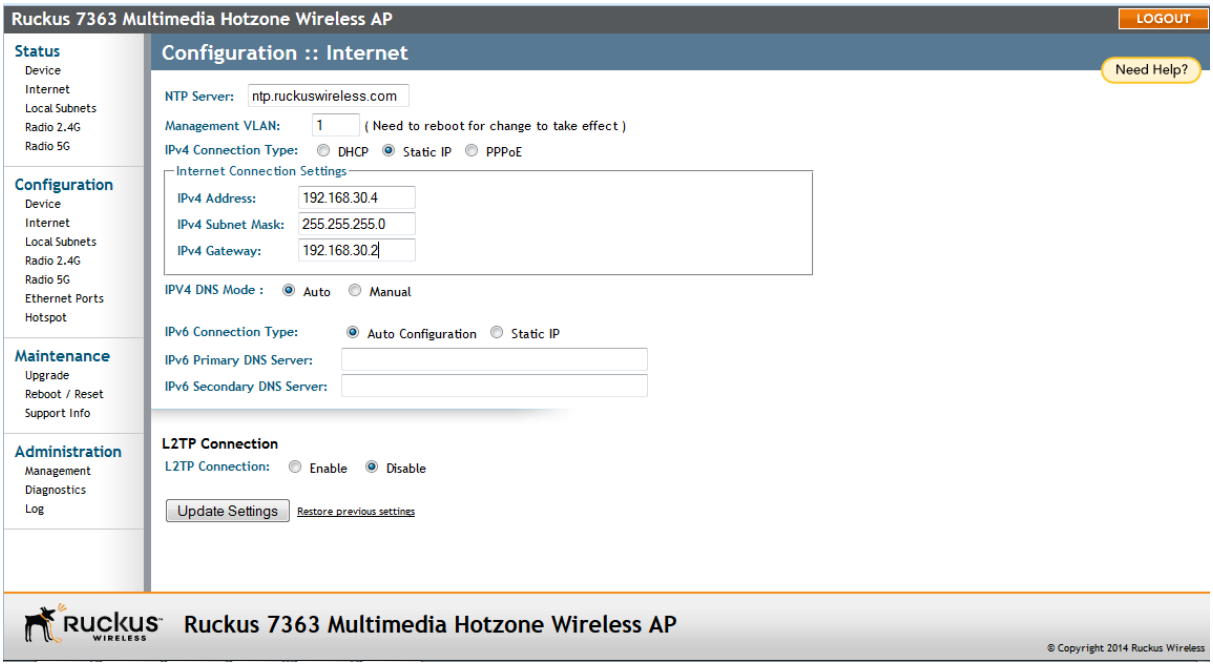


Figure 41 : Configuration Adresses IP de PA

Maintenant que la maquette est mise en place et la configuration est faite, le contrôleur devrait être capable de détecter la présence d'un point d'accès sur la partie supervision. La figure suivante montre le tableau de bord du contrôleur et les différentes informations auxquelles il accède. Nous remarquons que sur ce tableau, le contrôleur peut voir l'adresse MAC et IP du point d'accès, son modèle, son état, etc…

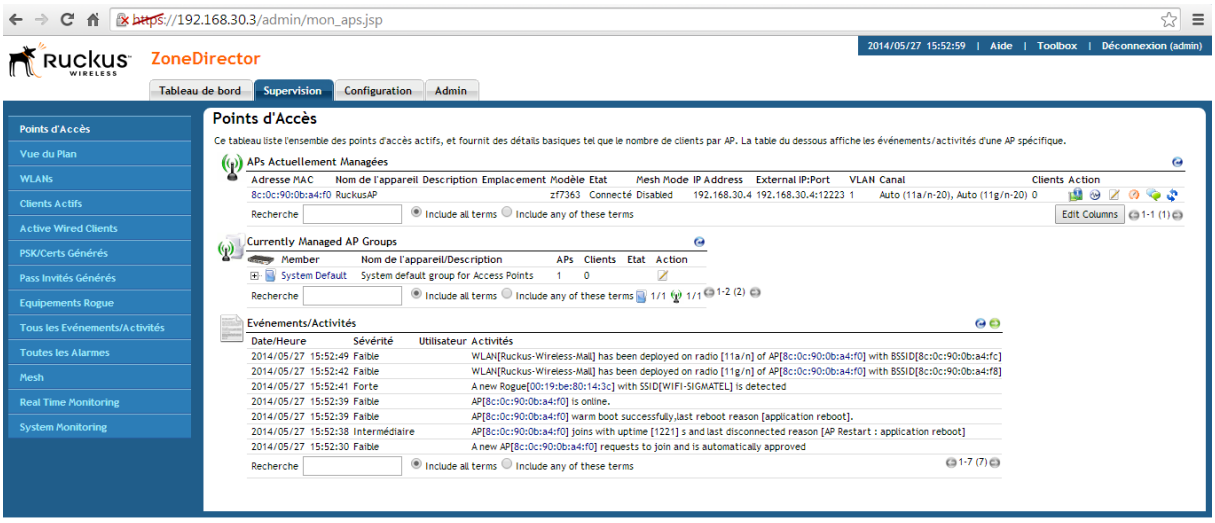


Figure 42 : Supervision Zone Director

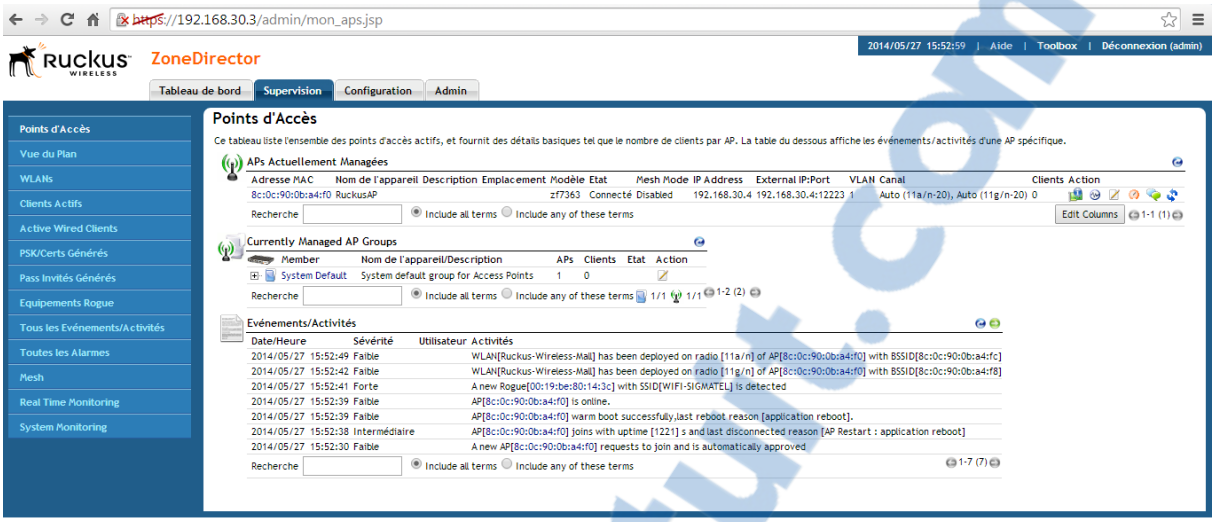


Figure 43 : SUPERVISION ZONE DIRECTOR

3. PRESENTATION DE LA PLATEFORME DE GESTION DES HOTSPOTS :

Le principal apport dont est caractérisée cette solution, est que toute la plateforme de gestion choisie est hébergée sur le web. Cloud4wi est une solution de cloud, permettant la gestion de la prochaine génération de services de point d'accès. Ainsi, elle offre non seulement un accès Internet, mais elle fournit également des applications web géo, des outils d'affaires et des contenus actifs, créant de nouvelles opportunités de revenus. Cette plateforme de gestion propose des modèles prédéfinis adaptables à différents scénarios.

Cette plateforme permet la personnalisation des portails captifs, la mise en place des services de profiles, d'applications web et plusieurs d'autres fonctionnalités. Notre mission sur ce projet était de personnaliser un portail dans le cadre d'un mall.

Comme la plateforme de gestion Cloud4wi est hébergée sur le web, la configuration se fait via un navigateur à partir du lien suivant : ***https://controlpanel.cloud4wi.com/***

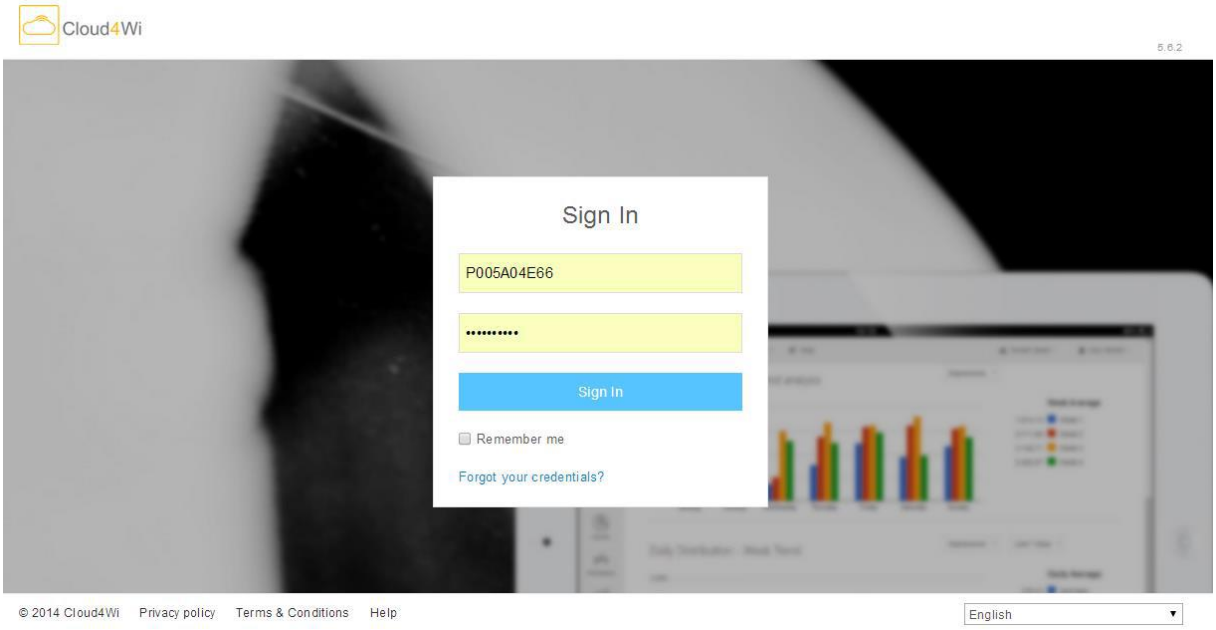


Figure 44 : Acces Plateforme CLOUD4WI

A la connexion à l'interface, nous avons plusieurs onglets nous permettant de personnaliser le portail captif et les services de profiles. La figure suivante montre ces différents onglets :

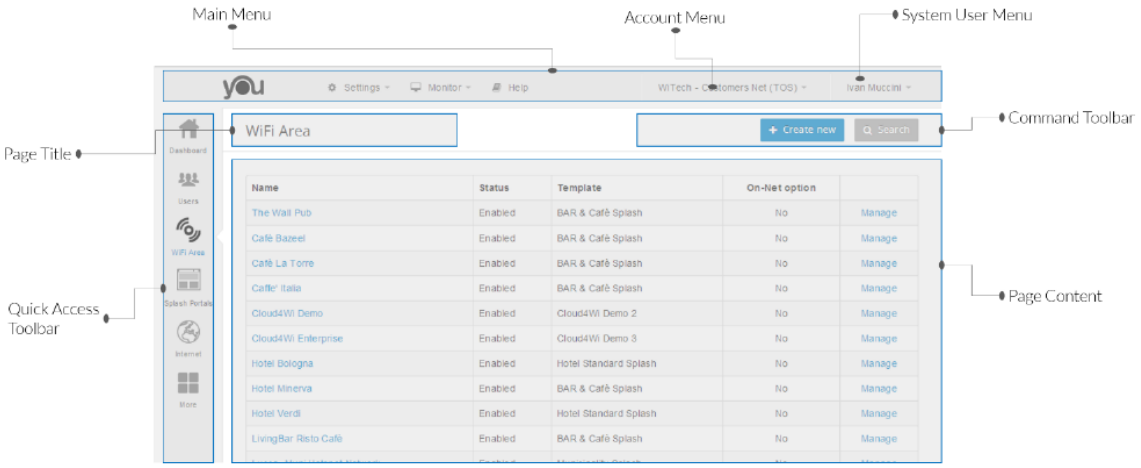


Figure 45 : INTERFACE CLOUD4WI

Comme montré dans la figure ci-dessus, le résumé sur l'onglet d'affichage donne une vision générale sur les utilisateurs actifs à un moment donné de la journée. L'administrateur pourrait alors être informé sur le nombre maximal des utilisateurs en ligne, le nombre d'utilisateurs inscrits et le nombre de tentatives de connexion.

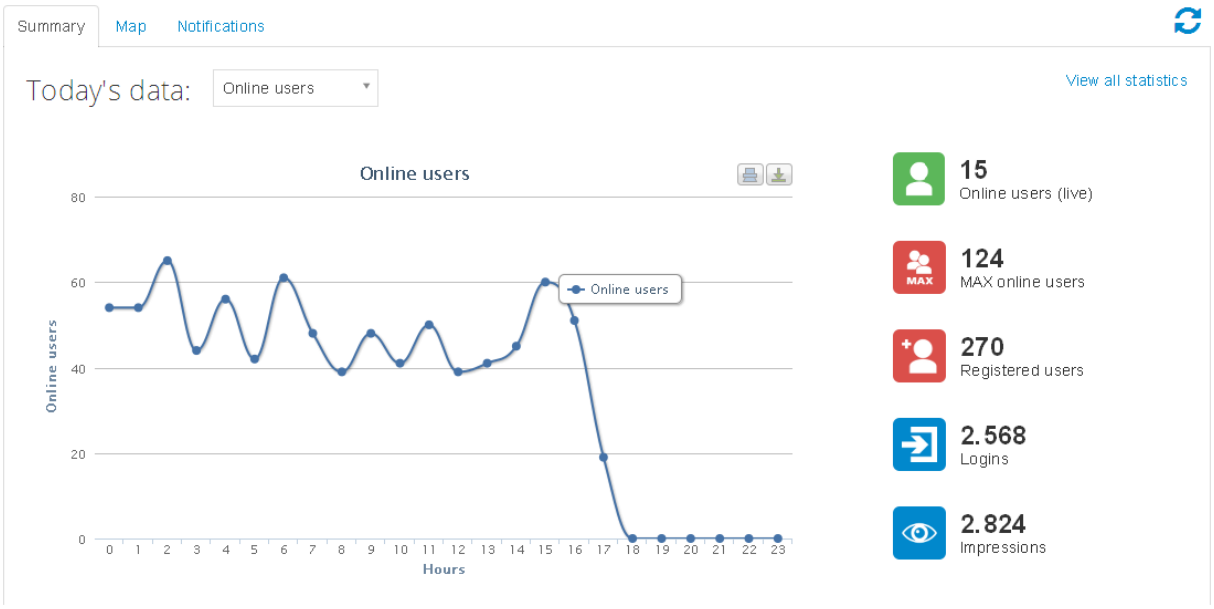


Figure 46 : Affichage, Résumé

La seconde partie importante est celle des Wifi Area. En effet, au moins un hotspot définit une zone wifi ou une wifi area particulière. Cette zone wifi appartient à un seul administrateur qui a la charge de la gérer. La figure «INTERFACE CLOUD4WI » montre une multitude de zones, définie selon l'emplacement des hotspots associés. Nous trouvons par exemple des hotspots dans des cafés ou des hôtels. Et c'est à partir du clic sur manage que l'administrateur gère sa propre zone wifi.

Pour la création d'un portail captif, il y a l'onglet *splash portal* réservé à cet insu. La plateforme propose différentes configurations et des templates, comme montré dans la figure suivante :

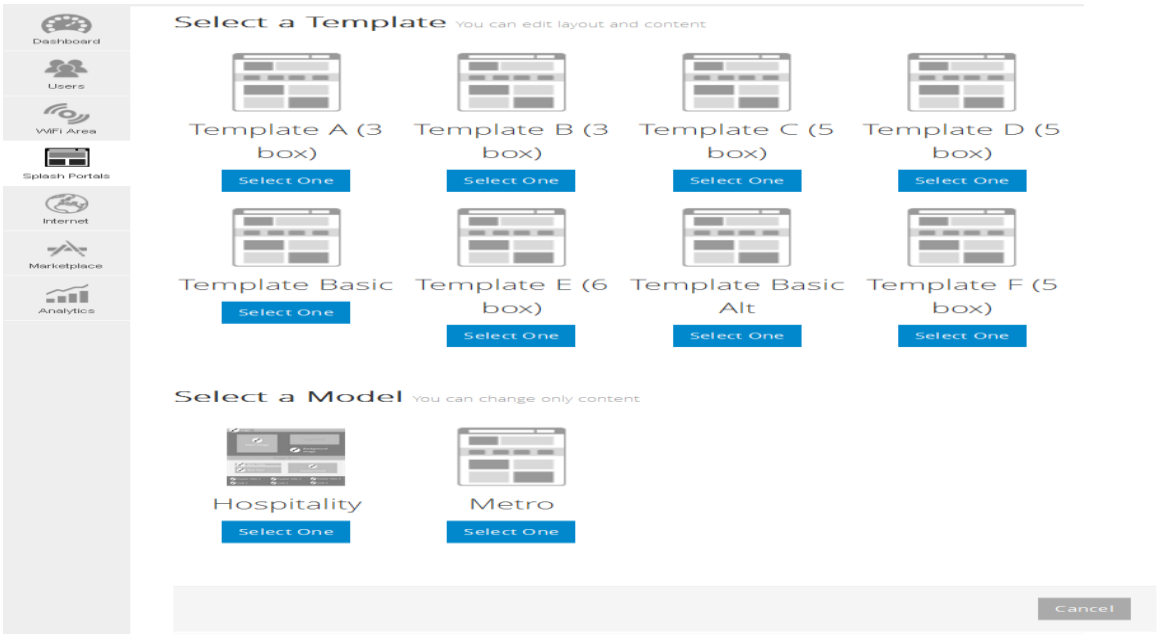


Figure 47 : CREATION DE PORTAIL

Pour notre portail, nous avons choisi un template B (3 box). La figure suivante présente le résultat de ce travail. La figure contient un premier bloc qui constitue l'entête de la page, où figure le logo de l'organisme d'accueil Sigmatel. Un second bloc contient la partie du logout (après connexion bien évidemment). Le troisième bloc est sous forme d'une image qui contient le plan du mall.

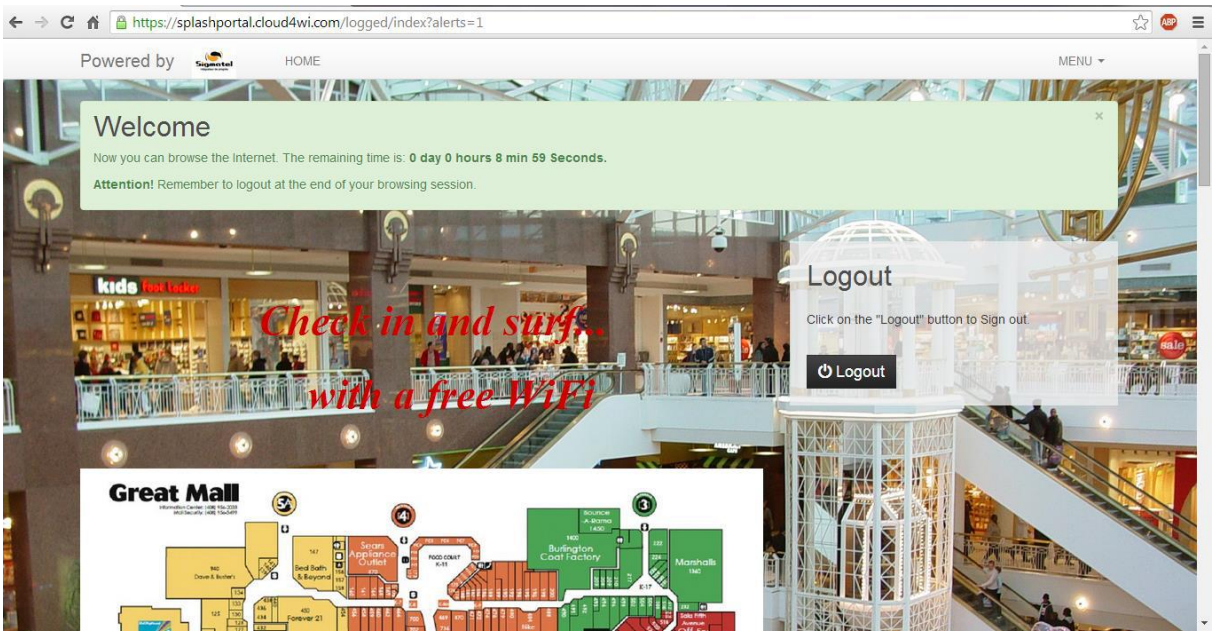


Figure 48 : Portail Captif MALL

IV. ARCHITECTURE DE TEST:

Afin de réaliser les tests demandés, nous avons virtualisé l'architecture globale. Celle-ci se compose de trois blocs et d'Internet comme illustré sur la figure ci-dessous.

- Une machine virtuelle XP qui jouera le rôle du client.

- Une machine virtuelle Ubuntu sur laquelle est configuré le service Freeradius en interaction avec la base de données MySQL

- Un routeur de type Mikrotik. Le routeur est interfacé avec les deux dernières machines et Internet.

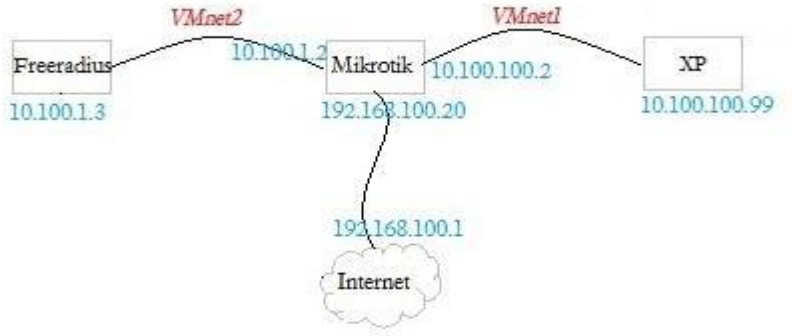


Figure 49 : Architecture de TEST

Sur l'outil ***Winbox*** qui permet de configurer le routeur à partir de la machine physique, les interfaces de celui-ci et les adresses IP de ses interfaces sont mieux visibles dans la figure ci-contre :

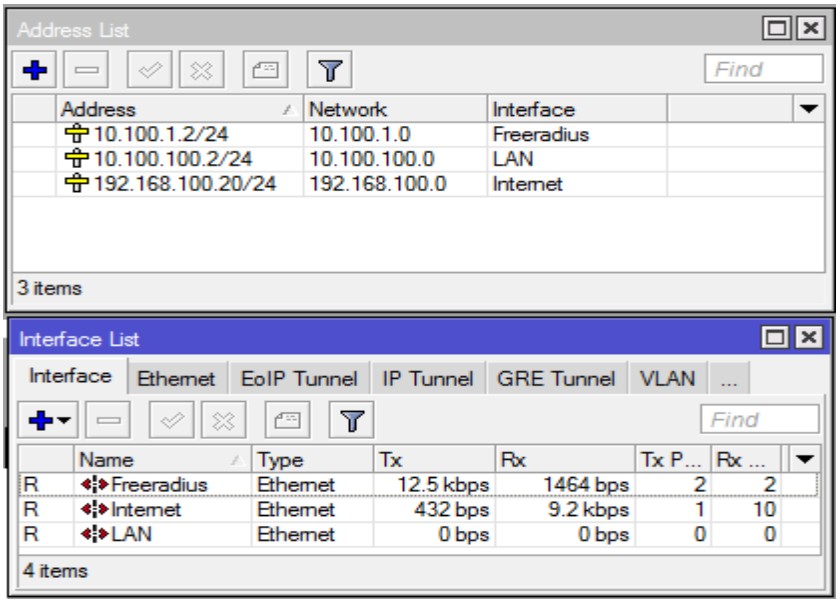


Figure 50 : Adresses et interfaces

Ici, Mikrotik a plusieurs fonctions : il joue le rôle de serveur DHCP pour la machine XP, et le serveur Radius.

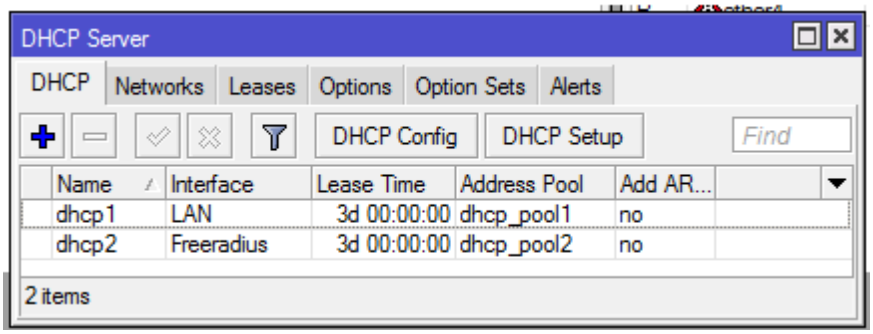


Figure 51 : Serveur DHCP Mikrotik

A chaque fois qu'un client se connecte au routeur, celui-ci lui attribue une adresse IP appartenant à la plage d'adressage consacrée. Nous avons choisi pour notre projet la plage suivante : [10.100.100.3 - 10.100.100.100]

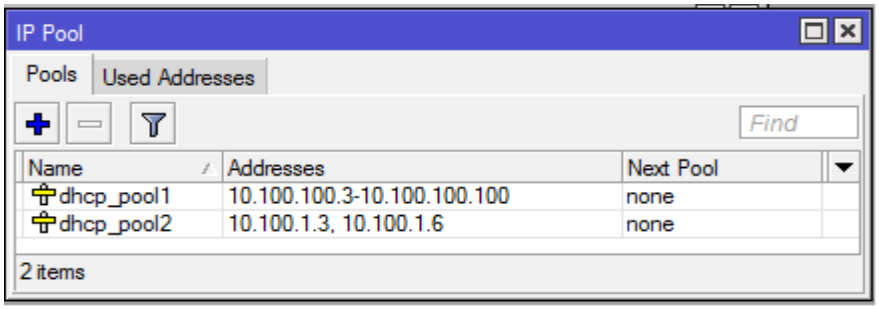


Figure 52 : Plage d'adressage

Ici, nous avons choisi de rendre Mikrotik un serveur DHCP pour le serveur Radius, comme nous pourrions fixer l'adresse IP du serveur et choisir une adresse IP de l'interface du Mikrotik dans la même plage. Celle-ci s'étale entre 10.100.1.3 et 10.100.1.6

1. OBJECTIFS :

Nous voulons par cette architecture de tests virtuelle tester un certain nombre de fonctionnalités.

- La première étant l'authentification des utilisateurs enregistrés dans la base de données MySQL sur le serveur Radius.
- La seconde consiste à voir si le service de comptabilité fonctionne correctement. Autrement dit, si un client atteignant la limite du temps autorisé pour l'accès à Internet est déconnecté.
- Le test suivant a pour but d'autoriser les utilisateurs à visiter un nombre spécifique de page dans une optique publicitaire ou promotionnelle. Ces pages sont appelées les walled garden, et l'utilisateur peut naviguer sur ces pages même s'il a dépassé la limite du temps de connexion autorisé

- L'aspect sécurité de la solution est très important. Si le routeur auquel sont connectés un nombre considérable d'utilisateurs subit une défaillance, une solution tierce devrait être envisagée. La mise en place d'un autre routeur, synchronisé avec le routeur primaire est essentielle. Ce test consiste à voir la redondance du routeur qui est supportée par le protocole VRRP (pour *Virtual Router Redundancy Protocol)*.
- Le dernier test s'intéresse au serveur Billing chargé de comptabiliser les utilisateurs. Le routeur contient la liste des utilisateurs connectés, leur adresse IP et le service de profil correspondant à chacun. Le serveur AAA contient lui aussi une base de données des utilisateurs et leur information respective. Si le routeur primaire est défaillant, le client n'a plus accès à Internet, et sa session est fermée sur le routeur ; par contre, sur le serveur AAA, il est toujours comptabilisé. Ce test consiste à configurer des messages ***« Interim update »*** permettant de répondre à cette fonctionnalité et synchroniser les sessions actives.

2. TEST 1 : AUTHENTIFICATION

Quand un utilisateur, sur une machine Windows par exemple, essaie d'accéder à Internet, celui-ci devrait s'authentifier. Sur un navigateur, il rentre l'URL qu'il souhaite visiter. Un portail est affiché lui demandant de rentrer son login et son mot de passe. Ces identifiants sont situés au niveau du serveur radius dans la base de données MySQL.

Figure 53 : Portail captif

Après que l'utilisateur ait saisi ses identifiants, une fenêtre comprenant quelques informations s'affiche. Elle contient l'adresse IP de l'utilisateur, les octets ascendants et descendants, la durée de connexion, et finalement, l'intervalle d'actualisation de la page.

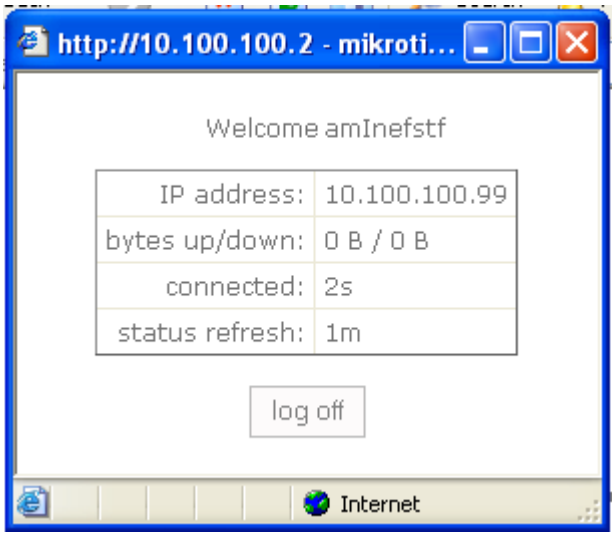


Figure 54 : Authentification utilisateur aminefstf

Pour mieux analyser le processus de communication entre les trois entités formant l'architecture de test, nous réalisons une analyse de trafic lors de cette étape d'authentification à l'aide de ***Wireshark***. L'analyse est faite sur les deux interfaces du Mikrotik, notamment l'interface avec le LAN (la machine XP représentant le client) et l'interface liée au serveur Radius. La capture du trafic est la suivante :

147	24.916331000	10.100.100.99	10.100.100.2	HTTP	576 POST /login HTTP/1.1 (application/x-www-form-urlencoded)
148	24.947605000	10.100.100.2	10.100.100.99	TCP	54 http > ansoft-lm-2 [ACK] Seq=14941 Ack=1577 Win=18972 Len=0
149	24.973357000	10.100.100.2	10.100.100.99	HTTP	1512 HTTP/1.1 200 OK (text/html)
150	24.916921000	10.100.1.2	10.100.1.3	RADIUS	235 Access-Request(1) (id=8, l=193)
151	24.966317000	10.100.1.3	10.100.1.2	RADIUS	62 Access-Accept(2) (id=8, l=20)
152	24.967330000	10.100.1.2	10.100.1.3	RADIUS	176 Accounting-Request(4) (id=9, l=134)
153	24.973174000	10.100.1.3	10.100.1.2	RADIUS	62 Accounting-Response(5) (id=9, l=20)
154	25.130784000	10.100.100.99	10.100.100.2	TCP	54 ansoft-lm-2 > http [ACK] Seq=1577 Ack=16399 Win=64240 Len=0

Notons que l'adresse IP :

- 10.100.100.99 correspond au client
- 10.100.100.2 correspond à l'interface du Mikrotik lié au LAN (VMnet1)
- 10.100.1.2 correspond à l'interface du Mikrotik lié au serveur Radius (VMnet2)
- 10.100.1.3 correspond à l'adresse du serveur Radius

Ici, le client envoie un paquet HTTP lorsqu'il accède à une page web. Il est automatiquement redirigé vers le portail sur lequel il saisit ses identifiants. A partir du paquet 150, le Mikrotik communique avec le serveur Radius afin de vérifier l'identité du

client en envoyant une requête Access-Request. Le serveur lui retourne un Access-Accept après interrogation de la base de données.

Quand un client est connecté à Internet, il est connu par Mikrotik. Ce dernier dispose d'un onglet des utilisateurs actifs rattachés à d'autres informations telles que la durée de connexion ou encore les octets envoyés. La figure suivante montre par exemple que l'utilisateur « aminefstf » est connecté sur le hotspot1 et qui a l'adresse IP 10.100.100.99. Cet utilisateur est connecté depuis 15secondes et il lui reste 2minutes et 45 secondes de connexion.

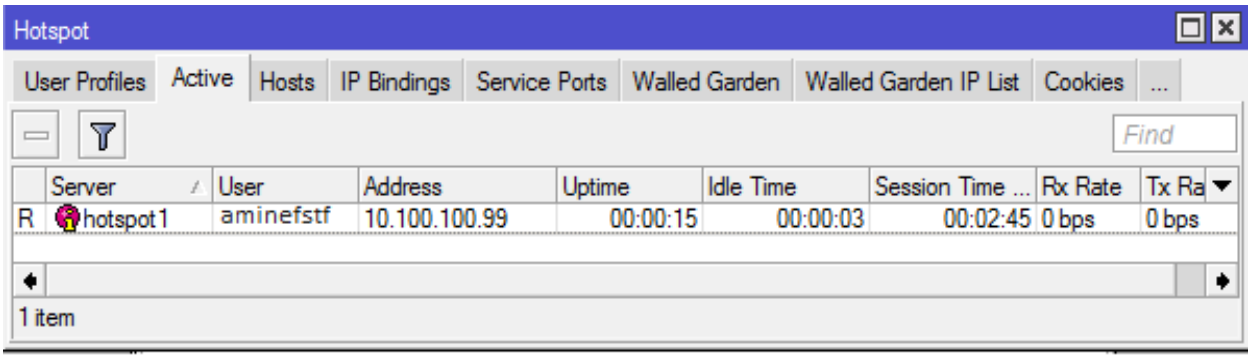


Figure 55 : Utilisateur actifs sur MIKROTIK

3. TEST 2 : COMPTABILITE :

La technologie 3G offload, permet en premier lieu de répondre au problème de congestion des réseaux mobiles. Quoiqu'elle ne nécessite pas un investissement de déploiement important, les sociétés de service en bénéficient en proposant la solution aux opérateurs qui récupère leur marge des clients par les différents profils qu'ils proposent.
La configuration de ces services se fait à travers l'accounting. Disposée par le serveur AAA, elle définit un certains nombres de session de comptabilité. En effet, quand un utilisateur se connecte à Internet (c'est-à-dire après la phase d'authentification), il sera chargé en temps de connexion. Selon le service de profil choisi, il aura une durée limitée, ou illimitée, de connexion.

Techniquement parlons du côté du routeur et du serveur d'authentification Radius, une information supplémentaire concernant le profil choisi par l'utilisateur devrait être prise en compte. En effet, cette information se fait au niveau du serveur Radius. Quand l'utilisateur s'authentifie, une ligne contenant toutes les informations est ajoutée à une table dans la base de données MySQL. Cette table est relative spécialement au service de comptabilité, nommée ***radacct***. Les champs les plus importants de cette table sont les suivants :

- UserName : le nom d'utilisateur du client
- AcctStartTime : temps d'ouverture de la session
- AcctStopTime : temps de fermeture de la session
- AcctSessionTime : temps d'une session en seconde

- CalledStationID : l'adresse MAC de l'équipement duquel l'utilisateur est connecté
- FramedIPAddress : l'adresse IP de l'équipement duquel l'utilisateur est connecté

Le service de comptabilité se base sur les données stockées sur cette table afin de mettre en oeuvre les différents services de profils.

Freeradius met en oeuvre des services par défaut, tel que le service ***noresetcounter*** qui autorise à l'utilisateur de se connecter pendant une durée fixe, sans date d'expiration. Les services ***dailycounter*** et ***mouthlycounter*** spécifient quant à eux, des durées fixes de connexion, mais qui expirent respectivement chaque jour, ou chaque mois. Freeradius dispose également d'un autre service ***expiration*** définit par une date complète (la date d'expiration) à partir de laquelle l'utilisateur est déconnecté directement. Pendant la durée de connexion, l'utilisateur pourrait visualiser combien de temps lui reste sur le compte. La figure suivante montre le compte à rebours actif.

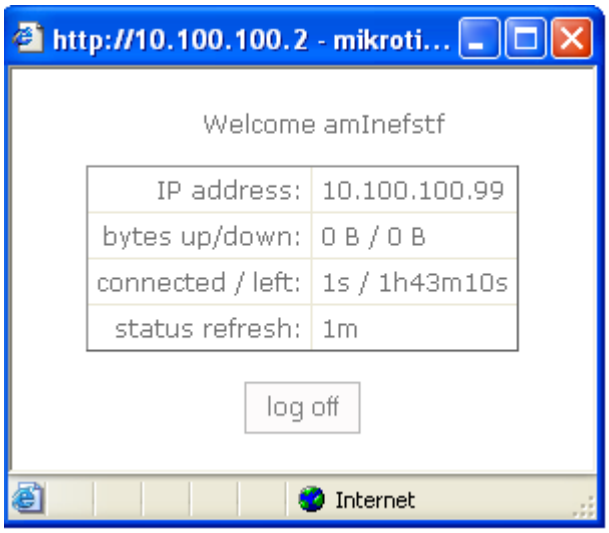


Figure 56 : ACCOUNTING PAR DATE D'EXPIRATION A LA CONNEXION

Par exemple ici, l'utilisateur 'aminefstf' vient de se connecter à l'instant d'une seconde, et il lui reste une heure et 43 minutes et quelques secondes. Après quelques minutes de connexion, la page web affichant la durée de connexion autorisée est rafraichie, et le compte est décrémenté.

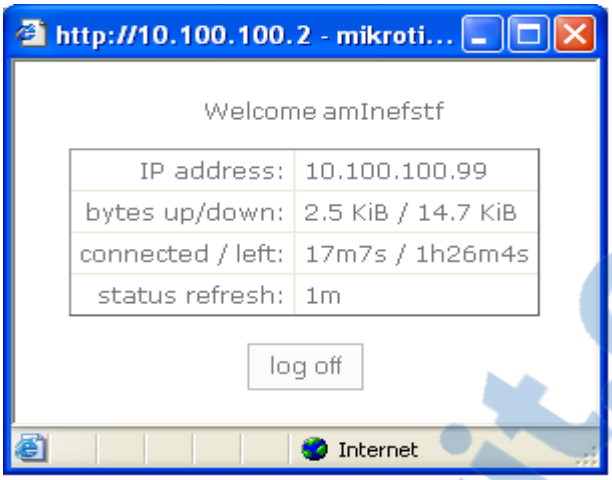


Figure 57 : Accounting par date d'expiration après quelques minutes

Quand nous lançons Freeradius avec le mode debug, nous remarquons l'envoie de deux requêtes : une relative à l'authentification, et un autre paquet de comptabilité. Freeradius collecte toutes les informations sur les paquets et consulte sa base de données MySQL afin de vérifier les autorisations de l'utilisateur.

TEST DE LIMITATION BANDE PASSANTE :

Si nous pensons à limiter les clients en termes de temps, nous pourrons également envisager de les limiter en bande passante. Afin d'optimiser la bande passante et le nombre de clients pouvant être rattachés à un hotspot, les limitations en bande passante est une solution pour remédier à ce problème.

La configuration de ce service se fait au niveau de l'outil Winbox de Mikrotik. A la création de l'utilisateur, l'administrateur lui attribue un profil d'utilisateurs. Ce profil contient les différentes restrictions à appliquer sur un groupe d'utilisateurs. Ici, nous limiterons les utilisateurs en temps et en bande passante. Nous créons alors un profil d'utilisateur pour limiter la connexion à 10 minutes et le débit d'une limite de 32 kbps en up et 512kbps en down. La figure suivante montre la configuration de ces services

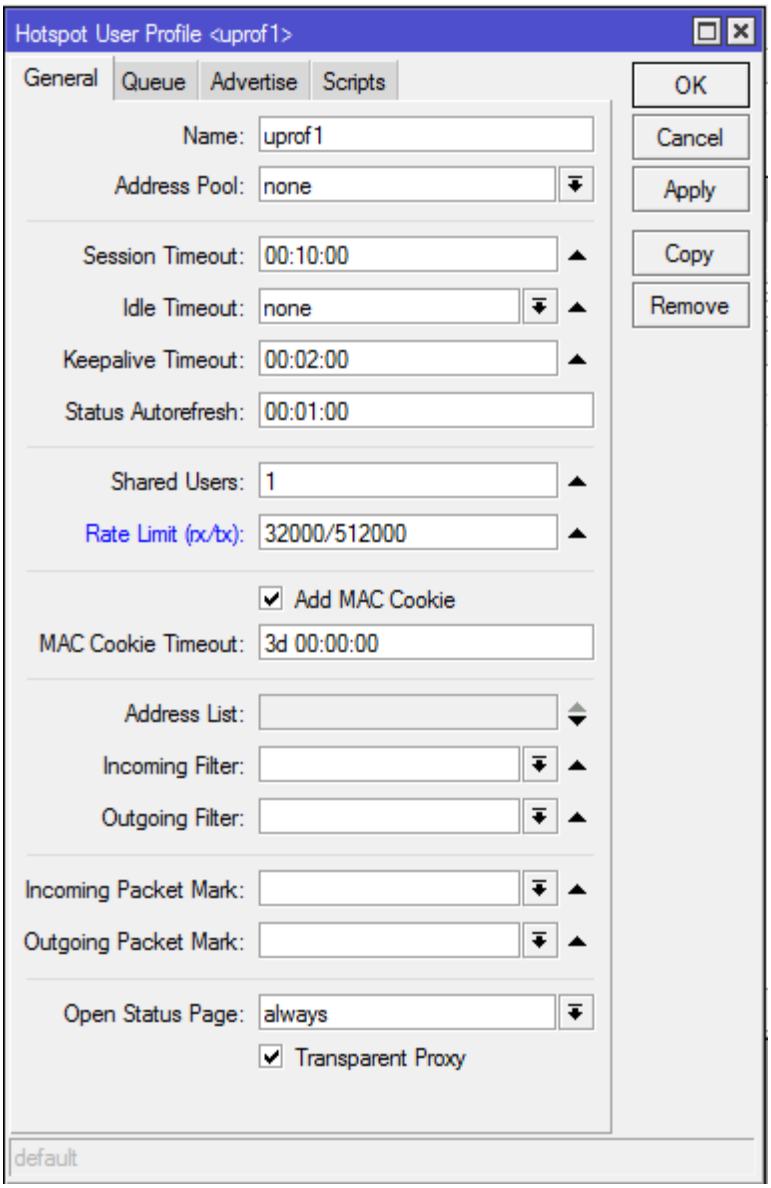


Figure 58 : Configuration de bande passante

Quand l'utilisateur se connecte, il s'affiche dans l'onglet Active des hotspots avec les différentes informations dont il est caractérisé. Une ligne s'ajoute au niveau de la file simple montrant que l'utilisateur connecté est limité en bande passante.

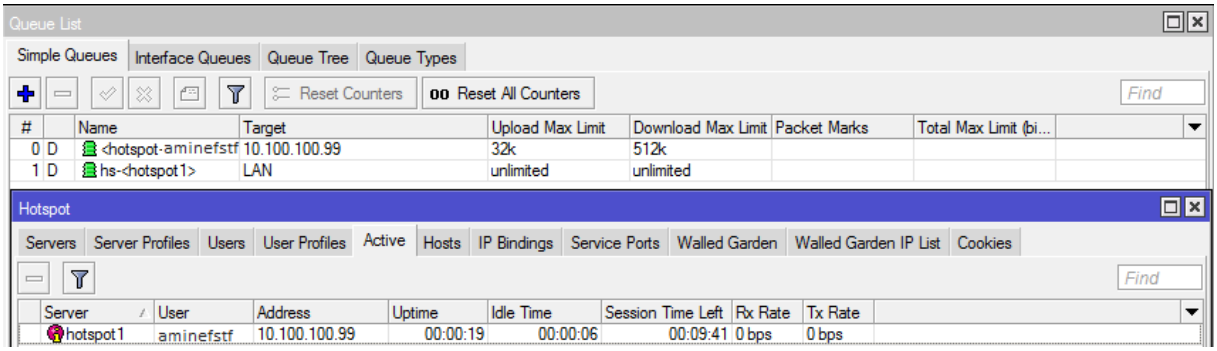


Figure 59 : Utilisateur actif et limitation de connexion

Après que l'utilisateur ait épuisé la limite autorisée, à sa reconnexion, la boîte de dialogue lui annonce qu'il a atteint la limite du trafic autorisé.

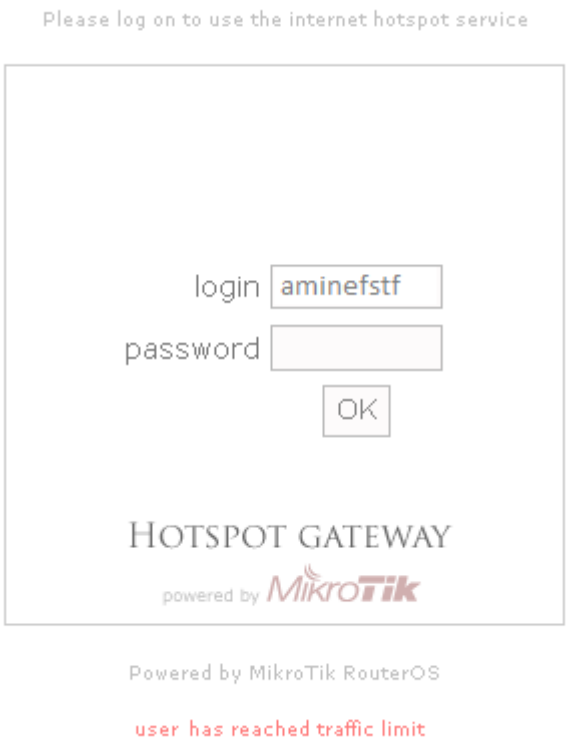


Figure 60 : Limite du trafic autorise

4. TEST 3 : REDONDANCE :

Les réseaux télécoms sont très sensibles aux pannes, et celles-ci sont très fréquentes. En effet, tout système est vulnérable. L'état d'équilibre étant un état exposé aux menaces, plusieurs solutions ont été proposées dans le but de réduire le danger et donc assurer la sécurité.

Dans le cas du Wi-Fi offload, l'élément le plus important et qui assure la connexion des utilisateurs est le contrôleur. Jouant un rôle très important, une quelconque défaillance au niveau de cet équipement est cruciale pour le bon fonctionnement de la solution. Ceci dit, afin d'assurer un fonctionnement à plein temps sans interruption, la redondance géographique de cet équipement pourrait constituer une parfaite solution. Si un problème survient au niveau d'un contrôleur, ou même au niveau de tout le site où est localisé l'équipement n°1, un autre contrôleur n°2, espacé de plusieurs kilomètres du premier, devrait prendre le relais et assurer la connexion des mêmes utilisateurs.

Dans ce cadre se place le troisième test du projet de stage de fin d'études. Sur la même maquette de tests, nous allons installer un autre Mikrotik, et nous allons configurer le protocole VRRP (pour Virtual Router Redundancy Protocol). Ce protocole standard est responsable de la haute disponibilité de la passerelle par défaut des hôtes d'un même réseau. En effet, il se base sur la notion de routeur virtuel et d'adressage virtuel.

ARCHITECTURE :

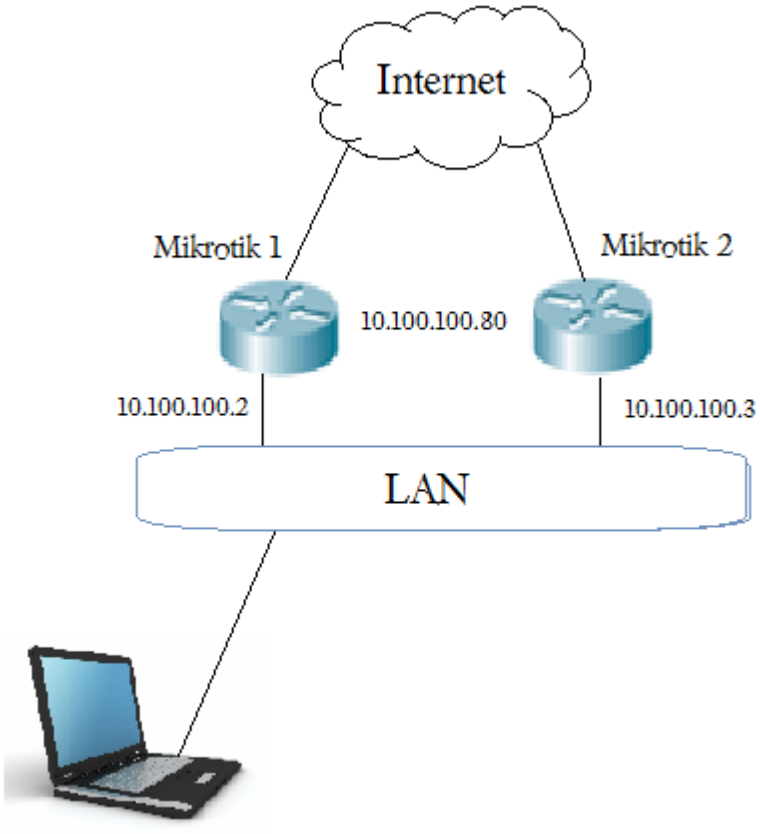


Figure 61 : Architecture de redondance

Afin de répondre à ce cahier de charges, nous avons réalisé les configurations nécessaires pour la mise en place d'un second Mikrotik pouvant prendre le relais en cas de défaillance du premier (en annexe)

Le résultat de ce test et sa simulation n'est pas simple à réaliser du fait que lorsque le service hotspot est activé, les pings ne se réalisent plus avec succès. Nous nous sommes contentés alors de tester cette redondance sans donner suite à l'authentification et les autres fonctionnalités qu'offre la solution.

Nous pourrons voir sur la machine du client, la machine Windows que l'utilisateur arrive à pinger sur l'adresse virtuelle 10.100.100.80.

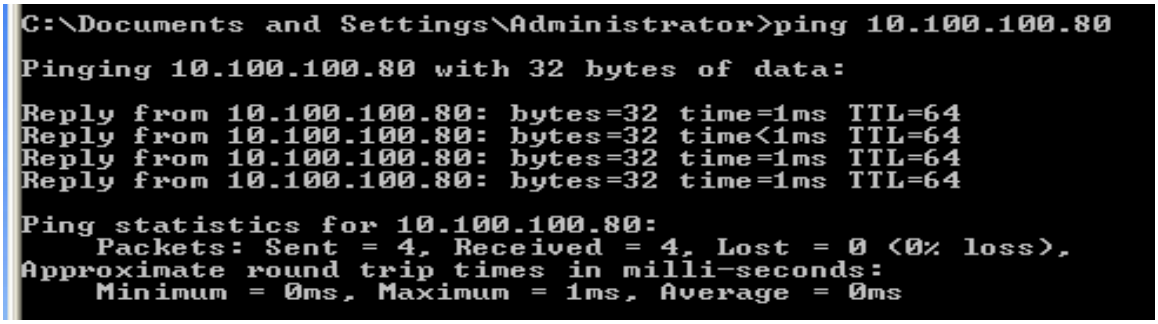


Figure 62 : Adresse virtuelle

Conclusion:

Ce chapitre a résumé le travail pratique réalisé durant le stage de fin d'études. Le but de la simulation faite était de réaliser un portail captif pour les clients d'une grande surface. De plus, les tests confiés ont été réalisés avec succès, sauf quelques problèmes au niveau de la redondance, qui nécessitait une intervention sur la plateforme de production, chose qui n'était pas possible.

CONCLUSION GENERALE

En réaction au fameux tsunami de données qui déferle sur les infrastructures mobiles du monde entier, les opérateurs recherchent activement tout outil capable de soulager les réseaux mobiles. Cet outil est la technologie Wifi Offload qui consiste à décharger le réseau mobile, en basculant la transmission des données vers Internet. Cette technologie attirerait des marchées diverses, notamment, les revenus issus du marché des points d'accès et des contrôleurs Wi-Fi pour les opérateurs devraient atteindre les 2,2 milliard de dollars en 2017, selon l'étude « Carrier Wifi and mobile offload » du cabinet d'études *ABI Research*. Soit près de la moitié du marché résidentiel et d'entreprise. [22]

Ainsi, nous avons fait une étude du projet WIFI 7DAK d'Inwi la première initiative de la technologie Offload au Maroc, qui a pu selon les capacités et les solutions propres à Altai, couplées aux exigences de l'opérateur et aux réalités du marché, nous avons contribué à la mise en place de cette technologie à ELJADIDA qui permettra aux opérateurs de décongestionner leurs réseaux 3G\4G.

Notre travail au sein de Sigmatel a consisté, plus particulièrement à la réalisation d'une maquette qui porte sur la solution Offload, suivi par plusieurs tests. Pour se faire nous été amené à étudier minutieusement les spécifications de la technologie. Ainsi nous avons mis en évidence les avantages par rapport aux autres solutions, le projet s'est déroulé en trois grandes phases : phase de documentation, phase de simulation et prise en main de la technologie et phase d'implémentation et de tests.

Pour conclure, le stage de fin d'étude a été d'un apport métier important, car il met en jeu un ensemble de concepts et de méthodologies relatifs au domaine des réseaux et des télécommunications. Le stage a été une véritable opportunité pour découvrir l'environnement professionnel, où les capacités de communication ont pu être améliorées, notamment grâce aux différentes confrontations avec les ingénieurs et techniciens.

Annexe 1 : RADIUS

RADIUS *(pour Remote Authentication Dial-In User Service)* est un protocole client/serveur, conçu afin de permettre à un équipement contrôlant l'accès à un réseau, appelé NAS *(Network Access Server)* de communiquer avec le serveur centralisé, le serveur Radius dans le but de :

- Vérifier l'identité d'un utilisateur qui cherche à se connecter.
- Savoir quels sont ses droits d'accès et sa configuration particulière
- Comptabiliser les connexions, leur durée, le volume de données échangées et tout autre paramètre de connexion pouvant servir à la facturation du client ou à son suivi

Il est également nommé le protocole AAA pour les trois fonctions qu'il occupe Authentication, Authorization, Accounting. Les échanges se font par le biais du protocole UDP à travers des ports spécifiques, 1812 pour l'authentification et 1813 pour la comptabilité.

L'identification à travers le serveur Radius se fait par un échange de requêtes entre le client Radius et le serveur. En effet, le client envoie une requête de type Access-Request au serveur pour l'accès au réseau ; le serveur Radius lui renvoie des requêtes Access-Challenge si les informations communiquées par le client ne sont pas suffisantes ; pour finalement répondre par une des deux requêtes Access-Accept ou Access-Reject selon l'autorisation du client. La figure ci-dessous illustre les deux cas possible :

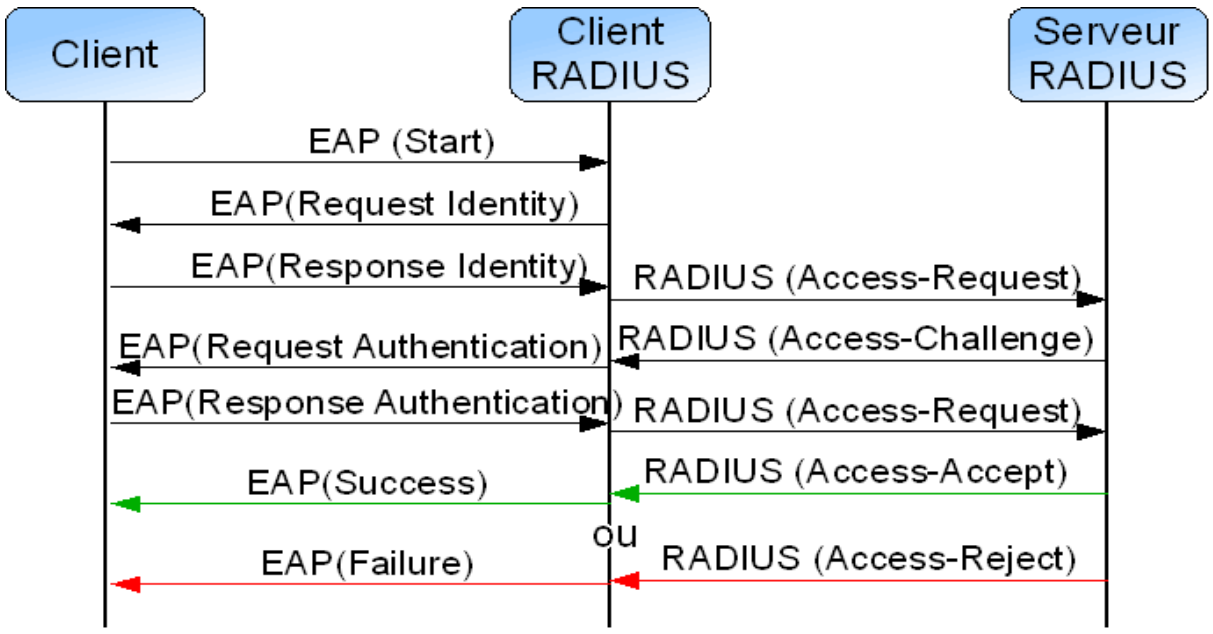


Figure 63 : ECHANGE AUTHENTIFICATION [23]

Authentication

Le processus d'authentification Radius débute quand un utilisateur essaie de se connecter à un réseau à travers un terminal via un serveur d'accès réseau NAS, jouant le rôle d'un client Radius. Cette étape vérifie si une identité appartient bien à celui qui la présente par un échange de requêtes.

Authorization :

Après l'étape d'authentification, le serveur vérifie si l'utilisateur est autorisé à accéder au réseau. Le serveur consulte alors la base de données MySQL et les champs de l'utilisateur en question.

Accounting :

Cette fonctionnalité gère à la fois la journalisation des accès et la facturation. Basée sur les paquets Accouting-Start et Accouting-Stop émis par le client Radius, …
Le protocole EAP (pour Extensible Authentification Protocol) est un protocole complémentaire à Radius. Il est conçu pour étendre les fonctionnalités de celui-ci à des types d'identification plus sophistiqués. Le protocole EAP utilise deux attributs Radius fonctionnant comme des protocoles de transport et donnant naissance aux extensions EAP-MD5, EAP-TLS et EAP-SIM… Généralement, dans un but d'authentification et d'autorisation, nous utilisons le protocole EAP et un serveur Radius.
Nous avons choisi de travailler avec le serveur Freeradius parce qu'il présente plusieurs avantages, notamment la caractéristique open source d'une part, et d'autre part, il supporte toutes les méthodes complémentaires au protocole EAP. De plus, Freeradius est capable d'intégrer tous les supports d'authentification. Nous avons choisi de travailler avec MySQL pour notre projet.

Annexe2 : CONFIGURATION DE FREERADIUS SOUS UBUNTU

INSTALLATION DES PACKAGES

Sudo apt-get install freeradius freeradius-mysql freeradius-utils mysql-server mysql-client php5 phpmyadmin

CONFIGURATION DE FREERADIUS POUR SUPPORTER SQL

Pour configurer le serveur radius sur cette machine, il faut modifier des fichiers :

/etc/freeradius/sql.conf

```
sql {
        #
        #  Set the database to one of:
        #
        #       mysql, mssql, oracle, postgresql
        #

        database = "mysql"
         login = "radius"
         password = "thepassword"
         readclients = yes
```

/etc/freeradius/sites-enabled/default

Décommenter '***sql'*** dans les catégories suivantes : authorize{}, accounting{}, session{} et post-auth{}

See "Authorization Queries" in sql.conf
sql

See "Accounting queries" in sql.conf
sql

See "Simultaneous Use Checking Queries" in sql.conf
sql

See "Authentication Logging Queries" in sql.conf
Sql

/etc/freeradius/radiusd.conf

Décommenter la phrase suivante : $INCLUDE sql.conf

```
#  Now in another file, because it is very large.
#
$INCLUDE eap.conf

#  Include another file that has the SQL-related configuration.
#  This is another file only because it tends to be big.
#
$INCLUDE sql.conf

#
#  This module is an SQL enabled version of the counter module.
```

/etc/freeradius/clients.conf

client 10.100.1.2/24 {
secret = testing123
shortname = testing
nastype= mikrotik
}

CREATION DE LA BASE DE DONNEES ET REMPLISSAGE :

mysql -u root –p
mysql> CREATE DATABASE radius;
mysql> GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY "thepassword";
mysql> exit;

mysql -u root -p radius < /etc/freeradius/sql/mysql/schema.sql
mysql -u root -p radius < /etc/freeradius/sql/mysql/nas.sql

mysql -u root –p
mysql> USE radius;
mysql> INSERT INTO radcheck (UserName, Attribute, Value) VALUES ('aminefstf', 'Password', 'aminefstf');
mysql> exit;

```
root@amine92-virtual-machine: /home/amine92

mysql> USE radius;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> INSERT INTO radcheck (UserName, Attribute, Value) VALUES ('aminefstf','Password',
'fstf');
Query OK, 1 row affected (0.17 sec)
```

CONFIGURATION SERVICE DE COMPTABILITE

Mikrotik :

Sur le routeur, il faut activer le service Accounting en accédant sur ***Winbox*** à ***IP > Accounting***

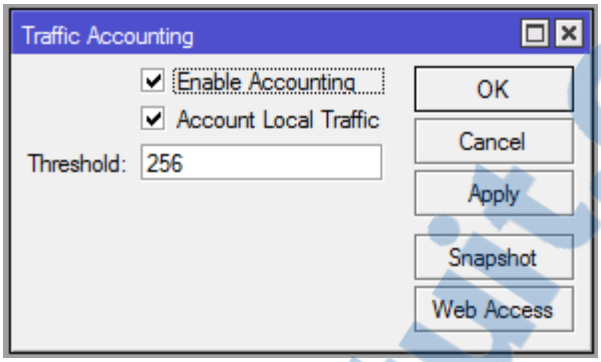


Figure 64 : TRAFFIC ACCOUTING

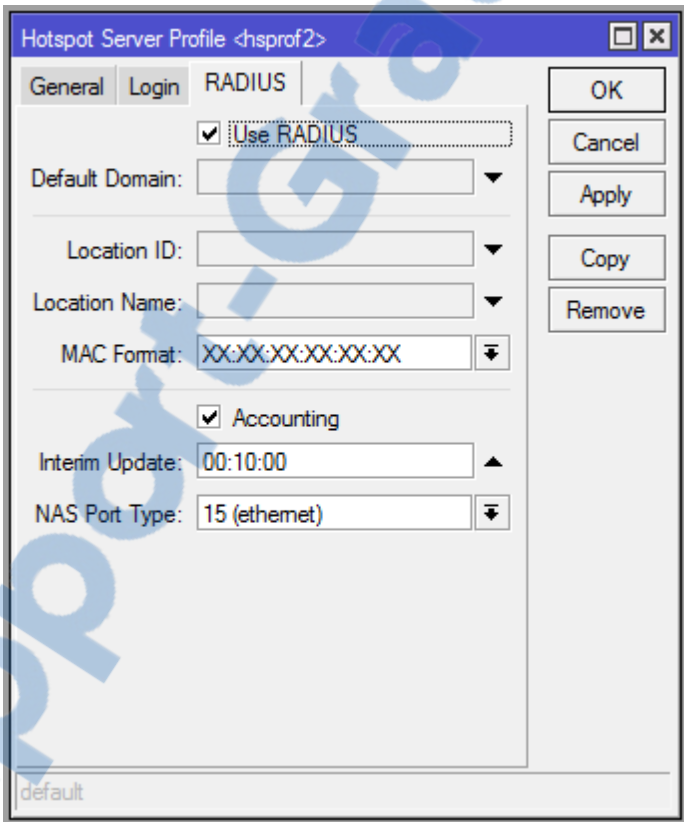


Figure 65 : ACCOUNTING SUR LE HOTSPOT SERVER PROFILE CORRESPONDANT

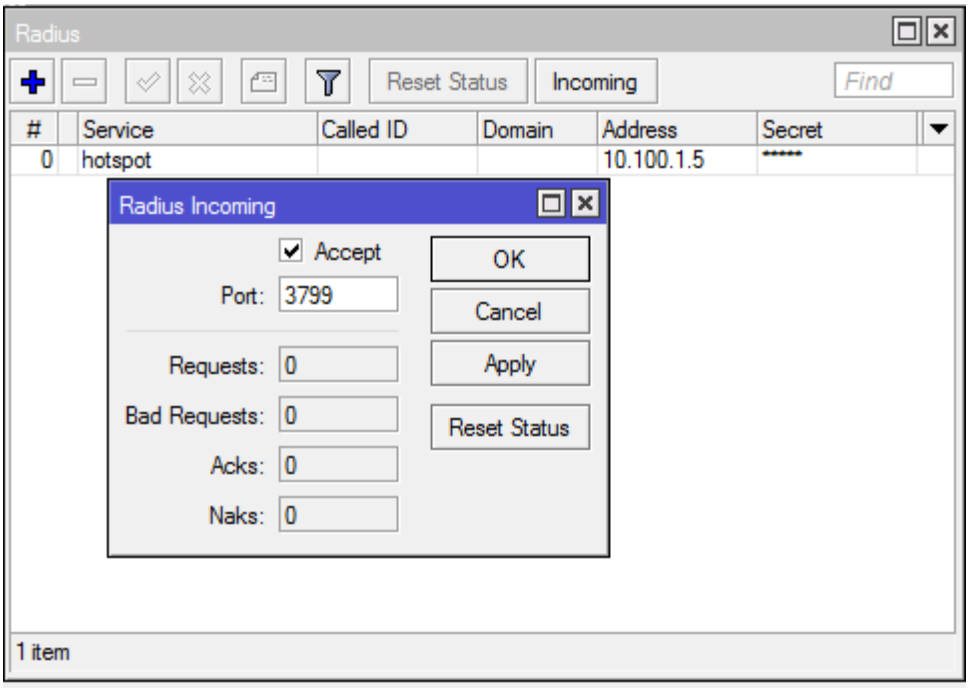


Figure 66 : ACCEPTATION DE L'ACCOUNTING

Freeradius :

Du côté de freeradius, une modification d'un fichier contenant les différents profils de services est nécessaire. Des modules prédéfinis sont configurés par défaut, tel que *noresetcounter* qui définit la durée maximale autorisée pour un utilisateur. Cette durée pourrait être consommée d'un coup ou sur plusieurs connexions. Le module *dailycounter* spécifie la durée pendant laquelle l'utilisateur pourrait se connecter à Internet par jour. Notons également que nous pourrions personnaliser des services par mois ou par années.
Ici, nous voudrons donner à l'utilisateur l'accès à Internet avec un reset quotidien. Il pourrait épuiser la durée de connexion qui lui est accordée comme il le souhaite pendant une journée. Le service à autoriser est donc le dailycounter. Les modifications des fichiers requises sont ci-dessous :

/etc/freeradius/sql/mysql/counter.conf

```
sqlcounter dailycounter {
counter-name = Daily-Session-Time
check-name = Max-Daily-Session
reply-name = Session-Timeout
sqlmod-inst = sql
key = User-Name
reset = daily
query = "SELECT COALESCE(SUM(AcctSessionTime),0) FROM radacct WHERE
UserName='% {%k}'"

sqlcounter noresetcounter {
counter-name = Max-All-Session-Time
check-name = Max-All-Session
```

sqlmod-inst = sql
key = User-Name
reset = never
query = "SELECT SUM(AcctSessionTime) FROM radacct WHERE UserName='% {%k}'"

/etc/freeradius/dictionary

ATTRIBUTE Max-All-Session 3003 integer

/etc/freeradius/sites-available/inner-tunnel

Décommenter sql dans # See ″Autorisation Queries″ in sql.conf
Ajouter noresetcounter

/etc/freeradius/radiusd.conf

Prise en compte des modules en dé commentant ou ajoutant :
$INCLUDE ${confdir}/modules/
$INCLUDE sql/mysql/counter.conf
noresetcounter
logintime
expiration

/etc/freeradius/sites-available/default

Dé commenter et ajouter les lignes suivantes :
Sql
noresetcounter
expiration
logintime

Une fois la configuration achevée, nous vérifions que notre serveur freeradius est bien prêt. Nous lançons alors notre serveur dans un mode debug par la commande ***freeradius –X***

Nous devons obtenir la sortie suivante :

```
Listening on authentication address * port 1812
Listening on accounting address * port 1813
Listening on authentication address 127.0.0.1 port 18120 as server inner-tunnel
Listening on proxy address * port 1814
Ready to process requests.
```

Figure 67 : Sortie FREERADIUS - X

Le serveur est en écoute des différents ports : 1812 pour l'authentification et 1813 pour l'accounting.

Annexe 3 : Configuration de VRPP SUR MIKROTIK

Afin de configurer VRRP sur Mikrotik, il faut d'abord créer les interfaces VRRP sur les deux Mikrotik (le master et le slave / Maître et esclave).

Sur le Mikrotik Master n°1 :

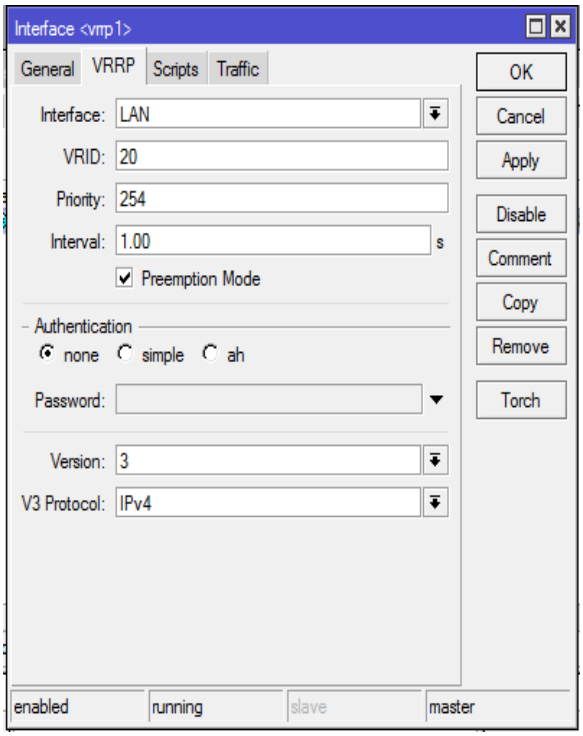


Figure 69 : Interface sur MIKROTIK 1

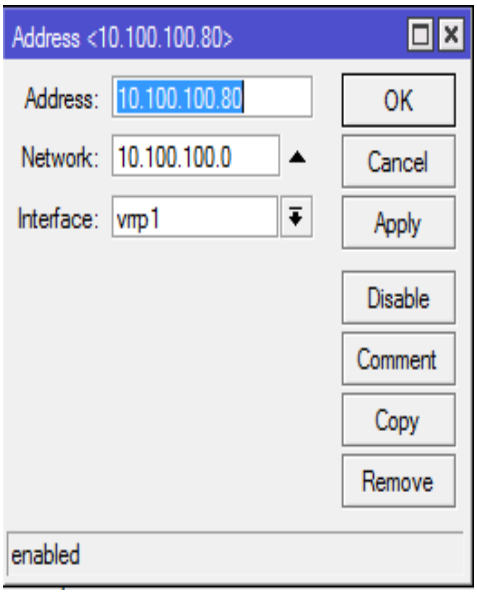


Figure 68 : Adresse VRPP DE MIKROTIK

Sur le Mikrotik esclave n°2 :

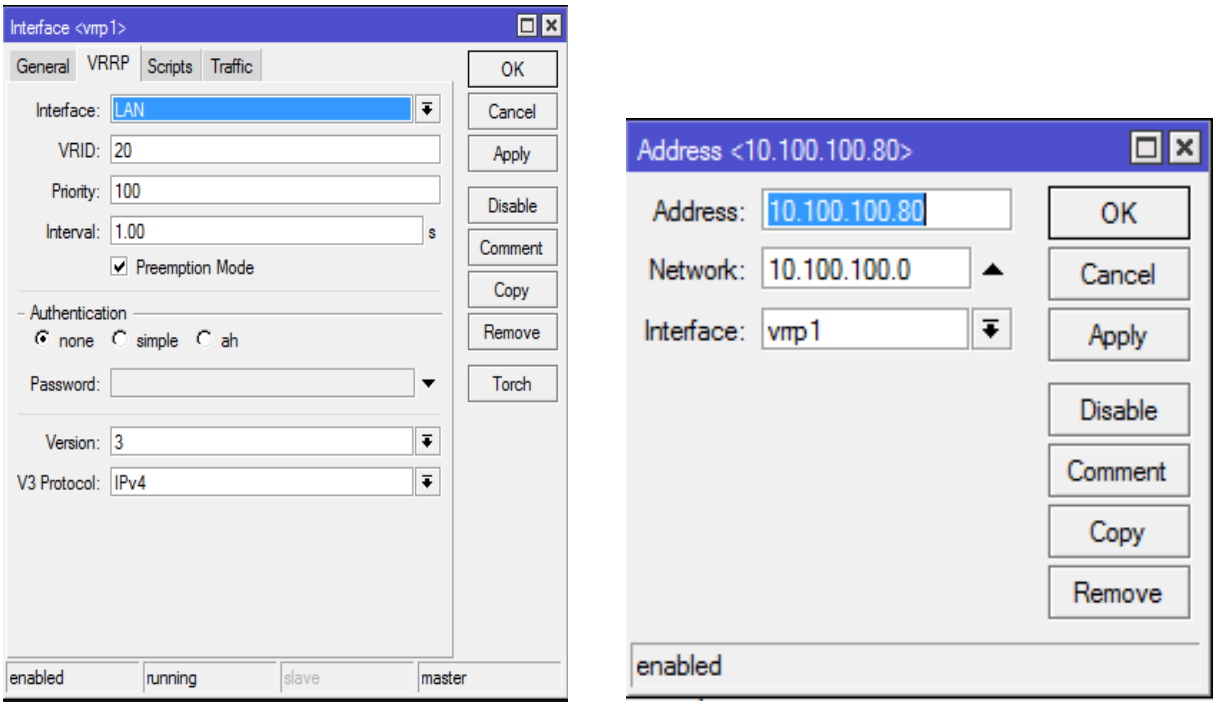


Figure 70 : Interface et Adresse VRRP DE MIKROTIK2

La première vérification consiste à voir si les deux interfaces des deux routeurs disposent de la même adresse MAC. La commande « **interface vrrp print »** nous permet de voir l'état de l'interface VRRP

Sur le Mikrotik master :

```
[admin@MikroTik] > interface vrrp print
Flags: X - disabled, I - invalid, R - running, M - master, B - backup
 #      NAME       INTER... MAC-ADDRESS       VRI PRI INTERVAL            V V3..
 0  RM  vrrp1      LAN      00:00:5E:00:01:14  20 254 1s                   3 ipv4
```

Sur le Mikrotik esclave :

```
[admin@MikroTik] > interface vrrp print
Flags: X - disabled, I - invalid, R - running, M - master, B - backup
 #      NAME       INTER... MAC-ADDRESS       VRI PRI INTERVAL            V V3..
 0  RM  vrrp1      LAN      00:00:5E:00:01:14  20 100 1s                   3 ipv4
```

La configuration n'est pas fastidieuse comme celle de la Freeradius, encore ici, nous n'avons configuré qu'une interface VRRP et une seule adresse IP virtuelle.

Bibliographie

[7] Wifi professionnel La norme 802.11, le déploiement, la sécurité, Aurélien GERON, 3e édition DUNOD

[8] Jean-Christophe Rios, Architecture de réseau WiFi centralisée Cisco UMLV, Ingénieurs 2000

[11] Transmissions et Protocoles, Nathalie Mitton, Equipe projet POPS, Lille, 02/2011

[17] Bulletin Officiel N° 6184 – 28 chaoual 1434 (5-9-2013), Page n° 2337

Webographie

[1] Nishant GOEL, http://mcpsinc.blogspot.in/2012/07/wi-fi-offloading-key-to-seamless-user.html, 09/03/2015

[2] www.sigmatel.ma 30/05/2015

[3] http://www.telecomspourtous.fr/lte.html 21/03/2015

[4] Christophe Lagane, http://www.silicon.fr/operateurs-wifi-offload-75881.html, le 20/04/2015

[5] Phil Goldstein, http://www.fiercewireless.com/story/report-new-roaming-tech-more-hotspots-drive-wi-fi-offloading/2015-4-21

[6] http://www.inwi.ma/internet-hdm/wifi-7dak 30/04/2015

[9] https://code.google.com/p/seek-for-android/wiki/EapSimAka 25/04/2015

[10] http://www.golzari.nl/wlan/eaptls.html 01/06/2015

[12] http://www.nec.co.jp/press/en/0309/1001.html 18/04/2015

[13] http://www.mpirical.com/blog/article/157 01/05/2015

[14] Mark Poletti, CableLabs, www.cablelabs.com 11/05/2015

[15] Rafael MARQUEZ, Marketing Director at TIM Intelig, www.aptilo.com /mobile-data-offloading/wifi-offload-3g-4g 16/03/2015

[16] http://www.anrt.ma/infos-pratiques/presentation

[18] http://www.cisco.com/c/en/us/solutions/collateral/service-provider/service-provider-wi-fi/white_paper_c11-701018.html

[19] Documentation WIFI 7DAK sigmatel.

[20] http://www.altaitechnologies.com/?page_id=877

[21] Architecture physique en Labo, M. Othmane DOUIRI, Sigmatel

[22] http://www.silicon.fr/operateurs-wifi-offload-75881.html

[23] Julien GAUTHIER, Professeur à l'université Paris-Est Marne la vallée