REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POLULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET INFORMATIQUE

DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention

Du Diplôme D'ingénieur d'Etat en Electronique

Option : Contrôle

ETUDE ET RÉALISATION D'U N RÉSEAU WIFI HOTSPOT DANS LE SERVICE PUBLIC

Proposé et dirigé par :

Promoteur: M^{r}. TAHANOUT

Encadreur : M^{r}. KIRAT

Réalisé et présenté par :

M^{elle} : KARIMA BELHADJ

M^{elle} : AMINA ABID

Promotion : 2011 / 2012

Remerciements

En premier lieu, nous remercions le Bon Dieu de nous avoir donné la force et le courage pour accomplir ce travail et qui nous a procuré ce succès.

Nous tenons à remercier notre encadreur Mr. Kirat Mourad, pour l'orientation, la confiance, la patience qui a constitué un apport considérable sans lequel ce travail n'aurait pas pu être mené au bon port. Qu'il trouve dans ce travail un hommage vivant à sa haute personnalité.

Nous exprimons nos gratitudes à tous le personnel de la DPN-Athir en particulier à la directrice Mme Cheriet pour leurs collaborations très étroites durant notre séjour au sein de la direction.

Nous tenons à exprimer nos remerciements à notre promoteur Mr «M. Tahanout» pour ses encouragements et son précieux soutient pour mener à bien notre travail.

Nous remercions également, les membres du jury pour nous avoir fait l'honneur d'évaluer notre travail.

Nous tenons enfin à remercier, toute personne ayant contribué, de près ou de loin, à la réalisation de ce travail.

Dédicaces

A la mémoire de mon père.

A ma très chère mère ma raison d'être, qui a toujours été la pour moi, et qui ma donné un magnifique modèle de labeur et de persévérance.

A mes chers frères et sœurs

A ma grand-mère Yamina.

A toute ma Famille.

A chrikti Nina et sa familles.

A mes anges Karim, Aymen et leurs père Smail.

A tous mes amis et collègues de promotion.

A tous ceux ou celles qui me sont chers et que j'ai amis involontairement de citer.

Je dédie ce modeste travail.

Karima

Dédicaces

A la mémoire de mes défunts parents.

A ma très chère grand mère, mon exemple dans la vie, qui m'a éclairé mon chemin et ma encouragée et soutenue au long de ma vie.

A mon cher frère

A mes chères sœurs

A mes chers neveux et nièces

A toute ma Famille.

A ma chère binôme Karima

A mon ange Aziz

A mon très cher ami Tayeb

A Mr.Ami, Hakima et Akila

A tous mes amis (es)

A tous ceux qui ont participé de prés ou de loin à la réalisation de ce travail.

Je dédie ce modeste travail.

Amina

Sommaire

Chapitre I : Généralités sur les réseaux sans fils

Chapitre II : La technologie WiFi

Partie Pratique

Chapitre III : Etude et déploiement du réseau Wifi hotspot

Liste des figures

Chapitre 1 : Généralités sur les réseaux sans fil

Chapitre II : La technologie WiFi

Partie Pratique

Introduction Générale

Introduction

Dans ce vaste monde des réseaux sans fils qui offre une très grande portabilité et mobilité aux utilisateurs en matière de communication, notre mémoire de fin d'étude stipule l'étude et le déploiement de l'architecture d'une infrastructure hotspot.

Afin de diffuser tout le travail effectué, ce document est constitué de deux parties : la partie théorique, constituée de deux chapitres : le chapitre I contenant un aperçu sur les notions importantes dans les réseaux sans fils, ensuite le chapitre II contenant l'état actuel en connectivité et en sécurité, et description des équipements Wifi proposés et recommandations pouvant permettre d'améliorer la connectivité et le niveau de sécurité d'un réseau sans fils.

Pour la partie pratique, l'étude de la connectivité en sélectionnant bien les scénarios faites par le simulateur mettant en évidence les considérations en termes de puissance de signal, de débit de transmission et l'influence du bruit ambiant sur la qualité du signal, avec une synthèse de ces résultats pour le cas du réseau campus et une proposition de déploiement. En ce qui concerne la sécurité après une définition d'une politique de sécurité acceptable basé sur l'authentification et l'autorisation centralisé à un serveur d'authentification radius mise en œuvre par Siemens. Avant de conclure, quelques perspectives implémentées par des moyens simples qui sont des idées également importantes pour la suite de ces travaux.

Chapitre I
Généralités sur les réseaux sans fil

I.1. Introduction

La radio, la télévision, plus récemment la téléphonie, ont eu un déploiement dont le succès a tenu essentiellement à la maîtrise de techniques de transport de l'information sans fil. Toutes les autres techniques de transport utilisant un support conducteur électrique ou optique se sont trouvées un jour ou l'autre freinées par des problèmes techniques. Ces problèmes de travaux publics, ou de bâtiment font que les techniques utilisant le câble sont hautement discriminatoires dans la possibilité d'accès à l'information. Un câble n'amènera jamais le réseau à un coût uniforme que ce soit dans une entreprise, dans un pays ou dans le monde. L'explosion de la téléphonie mobile dans des pays où le téléphone filaire était très en retard est une démonstration flagrante de cette réalité.

Dans le domaine des réseaux informatiques nous sommes en train de vivre depuis 1997 la même mutation. Le signal qui transporte l'information est en train de s'affranchir de son support conducteur électrique ou optique, pour utiliser tout l'espace. Dans la même année, sous l'instigation de Lucent (ex Bell labs), l'IEEE éditait la première spécification des réseaux sans fils.

De fait des avancées technologiques réalisées au cours de dernières décennies, les réseaux sans fil ont connu des changements radicaux allant des techniques de transmission jusqu'à la nature des services offerts.

I.2. Les réseaux sans fil

I.2.1. Définition : Qu'est ce que un réseau sans fil ?

D'une manière générale, le terme communications sans fil (réseaux sans fil) fait référence à des communications mettant en jeu des signaux infrarouges ou radio-fréquences permettant le partage d'informations et de ressources entre les déférentes entités d'un réseau. Ces entités sont de nos jours de déférents types (PDAs, capteurs sans fil, récepteurs satellitaires, terminaux mobiles, etc..).

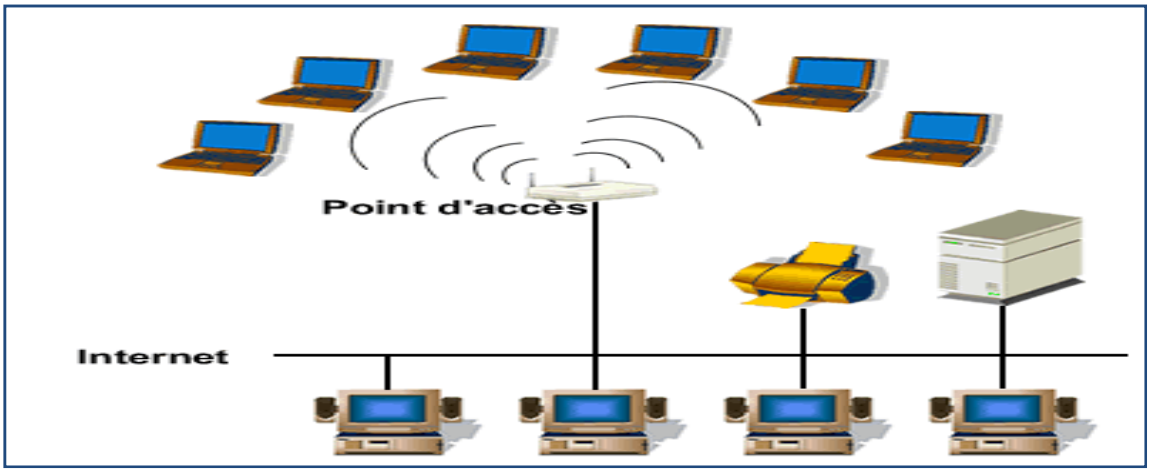


Figure.I.1 : réseau câblé associé a un réseau sans fils

I.2.2. Caractéristiques des réseaux sans fil

Du fait de la nature du canal de transmission, les réseaux sans fil se distinguent des réseaux filaires par les propriétés suivantes :

- Environnement imprédictible : Les interférences, la mobilité, le changement de canaux, les variations des puissances du signal sont des facteurs qui font en sorte que le réseau soit d'une grande variabilité.
- Médium non fiable : La transmission sur un canal radio s'accompagne d'erreurs. De plus, les interférences et la qualité non prédictible des liens réduisent la fiabilité du médium. En fin, du fait de la limitation de la capacité, des protocoles de la couche transport responsables de la fiabilité peuvent ne pas être supportées par les nœuds du réseau.
- Ressources limitées : Dans le cas des nœuds mobiles, la puissance est délivrée par des batteries. De plus, dans un souci de légèreté et de pratique, des nœuds sont limités en capacité de stockage et de puissance de traitement. En fin, le canal radio est une

ressource partagée, rare, onéreuse et dont l'usage est défini par des règlementations restrictives.

- Limitation de la taille des équipements due aux exigences de la portabilité.
- Topologie dynamique : La dynamique des réseaux sans fil est beaucoup plus importante que celle des réseaux filaires, en particulier dans le cas des réseaux mobiles. Du moment que les nœuds peuvent se déplacer à la portée des autres ou en dehors de celle-ci, des liens se coupent, d'autres se forment.

I.3. Classification des réseaux sans-fils

Il existe une multitude de réseaux sans fil. Ces réseaux peuvent être classés en plusieurs catégories selon les critères retenus.

I.3.1. Classification selon la zone de couverture

La classification des réseaux sans- fil peut être menée selon le périmètre géographique offrant une connectivite (appelé zone de couverture), On distingue ainsi quatre catégories : réseaux personnels sans-fil, réseaux locaux sans-fil, réseaux métropolitaines sans-fil et réseaux étendus sans-fil.

I.3.1.1. Les réseaux personnels sans fil (WPAN)

Appelé aussi réseaux domestique, Ils assurent l'interconnexion entre des terminaux distants à quelques dizaines de mètres, c'est des réseaux a faible portée. Ils servent généralement à relier des périphériques (PC, Imprimante…etc.) ou un assistant personnel (PDA) à un ordinateur sans liaison filaire.

Plusieurs technologies sont utilisées pour les WPAN tel que :

- **Bluetooth : 1 Mb/s sur 30 meters**

Si le Wifi est adapté à la construction de réseaux locaux sans fil, cette technologie consomme énormément d'énergie et sa portée comme son débit ne sont pas adaptés à l'échange d'information entre deux périphériques informatiques : ordinateur à imprimante, téléphone portable ou PDA vers PC, etc.

Pour ce type de réseaux domotiques, la norme Bluetooth (IEEE 802.15.1) lancée par Ericsson en 1994 est mieux adaptée. Elle permet d'échanger des données à un débit d'1 Mb/s

pour une portée de 5 à 30 mètres selon l'environnement. Bluetooth consomme très peu d'énergie et est donc bien adapté aux appareils mobiles.

- **Home RF**

Se veut le plus perfectionné des réseaux locaux actuels, opérant dans la bande des 2,4 GHz. Sa modulation radioélectrique, dite FHSS (Frequency Hopping Spread Spectrum), résiste mieux aux interférences et au brouillage que celle du Wi-Fi, dite DSSS.

Home RF est doté de fonctions de "qualité de service", QoS (Quality of Service), comme la gestion des priorités d´acheminement. Il s´adapte ainsi au transport des flux audio et vidéo, notamment dans sa version Home RF 2, à 10 Mbps. En outre, il incorpore le protocole du DECT (Digital Enhanced Cordless Telephony), qui lui permet d´assurer par lui-même des fonctions performantes de téléphonie numérique. Home RF permet de constituer des réseaux radioélectriques multimédias complets, à partir de micro-ordinateurs. Cependant, il reste confiné au marché grand public américain.

- **La technologie Zig Bee**

Aussi connue sous le nom IEEE 802.15.4, Permet d'obtenir des liaisons sans fil à très bas prix et avec une très faible consommation d'énergie, ce qui la rend particulièrement adaptée pour être directement intégré dans de petits appareils électroniques (appareils électroménagers, hifi, jouets, ...

- **Les liaisons infrarouges**

Permettent de créer des liaisons sans fils de quelques mètres avec des débits pouvant monter à quelques mégabits par seconde. Cette technologie est largement utilisée pour la domestique (télécommandes) mais souffre toutefois des perturbations dues aux interférences lumineuses.

I.3.1.2. Les réseaux locaux sans fil (WLAN)

Correspond au périmètre d'un réseau local installé dans une entreprise, un foyer ou encore dans les espaces publics **(hotspot**). Tous les terminaux (PC, assistant PDA…etc.) situés dans la zone de couverture du WLAN peuvent s'y connecter.

Il existe plusieurs technologies concurrentes :

- **Le Wifi (ou IEEE 802.11)**

Soutenu par l'alliance WECA (Wireless Ethernet Compatibility Alliance) offre des débits allant jusqu'à 54Mbps sur une distance de plusieurs centaines de mètres.

N B *:* Cette technologie sera beaucoup plus détaillée dans le chapitre suivant.

- **hiperLAN2 (High Performance Radio LAN 2.0)**

Norme européenne élaborée par l'ETSI (European Telecommunications Standards Institute), permet d'obtenir un débit théorique de 54 Mbps sur une zone d'une centaine de mètres dans la gamme de fréquence comprise entre 5 150 et 5 300MHz.

- **DECT**

Norme des téléphones sans fils domestiques. Alcatel et Ascom développent pour les environnements industriels, telles les centrales nucléaires, une solution basée sur cette norme qui limite les interférences. Les points d'accès résistent à la poussière et à l'eau. Ils peuvent surveiller les systèmes de sécurité 24/24h et se connecter directement au réseau téléphonique pour avertir le responsable en cas de problème.

I.3.1.3. Les réseaux métropolitains sans fil (WMAN)

Connus sous le nom de Boucle Locale Radio (B.L.R) ; Ils sont basés sur les normes IEEE 802.16. Le B.L.R offre un débit utile da 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres, ce qui destine cette technologie aux opérateurs de télécommunication.

Les réseaux sans fil de type WMAN sont se entrain de se développer ; la norme 802.16 est plus connue sous son nom commercial WiMax.

I.3.1.4. Les larges réseaux sans fil (WWAN)

Est également connu sous le nom de réseau cellulaire mobile, il s'agit des réseaux sans fil les plus répondu, puisque tous les téléphones mobiles sont connectés à un WWAN.

Les principales technologies sont les suivants :

- **GSM**

Basé sur une bande de fréquence de 890 à 960 MHz dans le sens montant, de 935 à 960 MHz dans le sens descendant, la liaison entre les mobiles et les stations de base est numérique à 13Kbit/s ce qui obtenu par un codage spécifique de la parole. La technique numéricienne permet de transporter des données par le même canal, à 9600bit/s max.

- **GPRS**

La mise en place d'un réseau GPRS va permettre à un opérateur de proposer de nouveaux service de type ''Data'' à ses clients. Le GPRS est en mode paquets. Le débit maximal instantané annoncé pour le GPRS est de 171.2 Kbit/s même s'il est limité à 48 Kbit/s en mode descendant. (Limite actuelle des terminaux GPRS).

La mise en place d'un réseau GPRS permet à un ordinateur de proposer de nouveaux services de type Data avec un débit de données 5 à 10 fois supérieur au débit maximum théorique d'un réseau GSM. (Rappel débit max. en GSM : 9.6 Kbit/s). Le réseau GPRS constitue finalement une étape vers le réseau UMTS.

- **UMTS**

Système de communication mobile universel, soit parallèlement autres normes. On a un réseau téléphonique comme le GSM. Mais contrairement au GSM il fonctionne dans la bande de fréquence de 2000MHz : entre 1885 et 2025MHz. Et au lieu d'avoir une multitude de canaux de 200KHz de large répartis sur la bande de fréquence attribuée à la cellule ; pour l'UMTS il n'y a qu'un seul et unique canal de 5KHz par cellule, et chaque terminal se partage cette ressource radio.

L'évolution technique de l'UMTS apport un débit en données de 2Mbit/s dans un futur proche ; même s'il plafonne pour le moment à 384Kbit/s c'est supérieur à celui du GSM.

- **Le WiMax**

Désigne en fait un ensemble de normes regroupées sous une application commune. Techniquement : il permet des débits de l'ordre de 70 Mbps avec une portée de l'ordre de 50 km. Actuellement, le WiMax peut exploiter les bandes de fréquence 2.4Ghz, 3.5Ghz et 5.8Ghz.

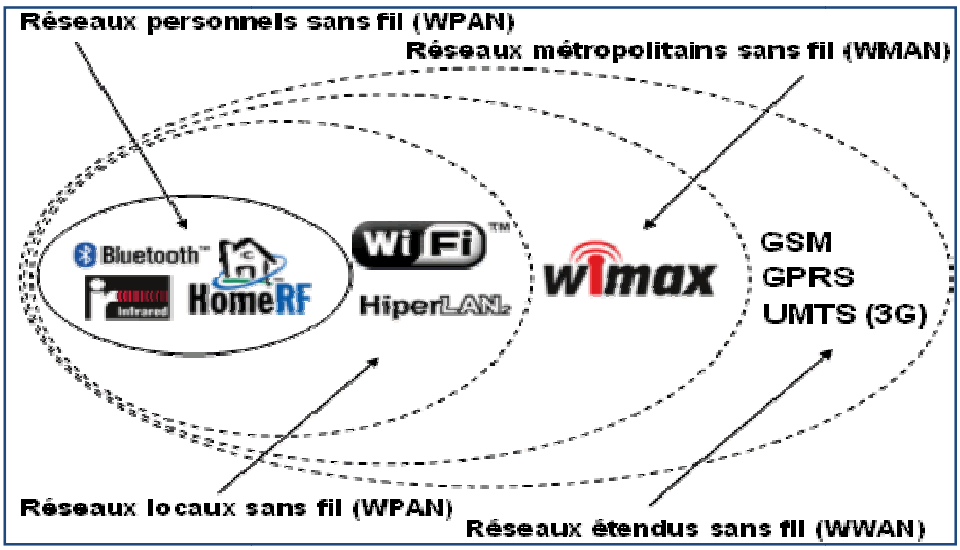


Figure. I.2 *:* Les catégories des réseaux sans fils.

I.3.2. Selon la technique d'accès

Les réseaux sans fil peuvent être classés selon le standard de la couche physique, la fréquence, l'usage du spectre, etc.…

Si le critère retenu est la technique d'accès, on distingue :

- Les réseaux TDMA (Time Division Multiple Access).
- Les réseaux FDMA (Frequency Division Multiple Access).
- Les réseaux CDMA / WCDMA (Code Division Multiplexe Access).
- Les réseaux SDMA (Space Division Multiplexe Access).

I.3.3. Selon le type d'application

Les réseaux sans fil peuvent aussi être classés en fonction dz leurs usages spécifiques et les applications qu'ils supportent. On peut citer à titre d'exemple :

- Les réseaux d'entreprises.
- Les réseaux domestiques.
- Les réseaux de capteurs (Sensor Networks).
- Les réseaux tactiques (Tactical Networks).
- Les réseaux pervasifs (Pervasive Networks).
- L'informatique portative (Wearable Computing).
- Les réseaux des véhicules automatisés (Automded Vehical Networks).

I.4. Fonctionnement d'un réseau sans fil

Un réseau sans fil utilise des radiofréquences (ondes électro-magnétiques) comme porteuse d'un signal. Chaque point d'une liaison est constitué d'une antenne utilisée en émission et réception, et d'un module de traitement (modulation - démodulation) du signal. Une onde électromagnétique est caractérisée par sa fréquence ou sa longueur d'onde, les 2 étant liées :

$$\lambda \times f = C \approx 3\times10^{8} \text{ m/s.}$$

$$\lambda = c / f$$

f(GHz)	λ (cm)
2.4	12.5
5.5	5.5

Sa longueur d'onde est une caractéristique à connaître car elle indique à quelle taille de structures elle va être sensible, c'est à dire absorbée ou bien transmise. Pratiquement, l'électronique qui gère le codage de l'information et la modulation sur une porteuse (ainsi que les fonctions inverses) est intégrée dans une carte de format PCMCIA ou bien PCI. Ces cartes sont appelées selon les constructeurs Orinoco, Air Port, Wifi ou 802.11b.

L'émetteur est cadencé sur une fréquence de base et va coder 2^n bits sur une porteuse sous la forme d'une modulation d'amplitude et phase. Lorsque le rapport signal sur bruit de la porteuse baisse, les valeurs de la grille d'amplitude phase utilisables vont être réduites et le nombre de bits pouvant être ainsi codés va passer à 2^{n-1} (ce qui correspond à une division du débit physique par 2).

Un ordinateur équipé d'une carte 802.11b détermine une zone spatiale dans laquelle il est possible d'établir une liaison avec un ordinateur. Cette zone spatiale est déterminée par la portée jusqu'à laquelle le rapport signal sur bruit est suffisant pour porter encore de l'information. La forme de cette zone de couverture spatiale dépend énormément de la qualité du dessin d'antenne et peut aller de quasi-sphérique (antenne omnidirectionnelles) à un lobe allongé (antenne directionnelle).

I.5. Avantages et inconvénients

I.5.1. Avantages

Si les caractéristiques actuelles d'un réseau sans fils permettent de rivaliser avec celles d'un réseau filaire, les réseaux locaux sans ne visent toute fois pas à remplacer les réseaux locaux mais plutôt à leur apporter de nombreux avantages découlant d'un nouveau service : la mobilité de l'utilisateur.

Les principaux avantages résident dans la réduction du coût de câblage et une souplesse accrue.

- **Topologie:** Le sans fil libère des contraintes imposées par les réseaux câblés. Avec un logiciel adéquat, il devient possible de mettre en service un nouvel appareil à n'importe quel moment, ce dernier se connecte, s'identifie, propose ses services et reçoit alors une partie des tâches à exécuter. Tout cela automatiquement, sans aucune connexion physique.
- **Mobilité:** les utilisateurs sont généralement satisfaits des libertés offertes par un réseau sans fil et de fait sont plus enclins à utiliser le matériel informatique.
- **Facilité et souplesse:** un réseau sans fil peut être utilisé dans des endroits temporaires, couvrir des zones difficiles d'accès aux câbles, et relier des bâtiments distants.
- **Évolutivité:** les réseaux sans fil peuvent être dimensionnés au plus juste et suivre simplement l'évolution des besoins

I.5.2. Inconvénients

De part la nature du canal radio, un certain nombre de problèmes se posent qui ne trouves pas d'équivalent dans le monde filaire. On peut citer en particulier :

- **L'Energie :** les applications relatives aux réseaux sans fils ont en général un caractère nomade et tirent leur autonomie de batterie. Emettre ou recevoir des données consomme de l'énergie et l'on chercher à l'économiser en optimisant les protocoles de gestion du réseau.
- **Qualité et continuité du signal :** ces notions ne sont pas garanties du fait des problèmes pouvant venir des interférences, du matériel et de l'environnement.
- **Une faible sécurité :** Il est facile d'espionner un canal radio de manière passive. Les protections ne pouvant pas se faire de manière physique (il est en générale difficile

d'empêcher quelqu'un de placer discrètement une antenne réceptrice très sensible dans le voisinage), elles devront êtres mises en place de manière logique, avec de la cryptographie ou éventuellement des antennes très directionnelles.

I.6. Conclusion

Dans ce chapitre on a présenté un état d'art des réseaux sans fil qui sont des technologies intéressantes et très utilisées dans de divers domaines comme l'industrie, la santé et le domaine militaire. Cette diversification d'utilisation revient aux différents avantages qu'apportent ces technologies, comme la mobilité, la simplicité d'installation (absence de câblage), la disponibilité (aussi bien commerciale que dans les expériences). Reste à choisir la solution adaptée et anticiper les évolutions d'une technologie encore immature.

Chapitre II

La technologie WiFi

II.1. Historique

En 1997 ; alors que l'intention est accaparée par le succès d'Internet et l'euphorie boursière montante, un événement est passé inaperçu sauf pour quelque spécialistes et observateur : L'adoption du standard IEEE 802.11 ou Ethernet sans fil. En 1998, la norme 802.11 est finalisée. En 1999 : Les IBooks d'Apple Inc sont les premiers ordinateurs à proposer un équipement Wi-Fi intégré. En 2000, l'alliance WECA (Wireless Ethernet Compatibility Alliance) est créée. La WECA est l'organisme chargé de veiller au respect de la norme 802.11 et notamment de l'interopérabilité entre les différents matériels. 2000 est l'année également du lancement de la première communauté Wifi (premier réseau d'ordinateurs reliés grâce à la technologie Wifi permettant, notamment, de partager une connexion Internet). En 2003 les PC portables avec la technologie Intel Centrino sont commercialisés. Depuis 2003, la technologie Wi-fi s'est développée rapidement et de nombreuses applications ont été déployées pour le grand public, En 2007, la technologie Wifi n'est plus considérée comme expérimentale par l'ARCEP (Autorité de régulation des télécoms) et entre dans la législation classique appliquées aux réseaux de télécommunications électroniques.

Le Wifi est une technologie intéressante pour de nombreuses sociétés liées au monde des télécoms et d'Internet. Les collectivités locales et surtout les particuliers profitent de la facilité d'accès à Internet haut débit liée à cette norme. Dans sa déclinaison la plus connue, 802.11b, le Wifi utilise la bande de fréquence de 2,4 GHz et atteint un débit théorique de 11 Mbits/s (contre 128,512 Kbits/s ou 1 Mbits/s pour l'ADSL), le 802.11a culmine à 22 Mbits/s et le 802.11g, enfin, flirt avec le 54 Mbits/s. le Wifi peut certes servir à surfer sur Internet, mais pas seulement. Il autorise l'organisation de réseaux – pourvus ou pas d'Internet – pour échanger des fichiers, des données, et bien entendu pour jouer… ce ne sont là que quelques exemples de ses usages possibles. Les avantages des réseaux sans fils ne sont plus à démontrer surtout à une génération de plus en plus habituée à la mobilité. La multiplication des appareils (PDA, PC portables, terminaux et bientôt les téléphones portables) capables de communiquer entre eux en fait le support idéal des réseaux modernes.

II.2. Définition du réseau WIFI

II.2.1. Principe

Le Wi-Fi est une technique de réseau informatique sans fil mise en place pour fonctionner en réseau interne devenu un moyen d'accès à haut débit à Internet. Il est basé sur la norme IEEE 802.11 (ISO/CEI 8802.11) correspondant au standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN).

Le WIFI est utilisé par différent types d'utilisateurs que l'on peut regrouper ainsi :

- **Home spot :** réseau pour les particuliers : il permet de partager sa connexion Internet sans utiliser les câbles.
- **Workspot :** réseau d'entreprise: s'associe à un réseau filaire Ethernet ou le remplace.
- **Hot spot :** réseau publique en accès libre accessibles dans les lieus publics fréquentés (gares, aéroport, hôtels …) par un ordinateur ou PDA.
- **Réseaux associatifs** : utilisation, par des associations ou des collectivités locales, de liaison wifi en point à point sur des distances pouvant atteindre quelques kilomètres, dans le but notamment de palier à un manque de ligne ADSL.

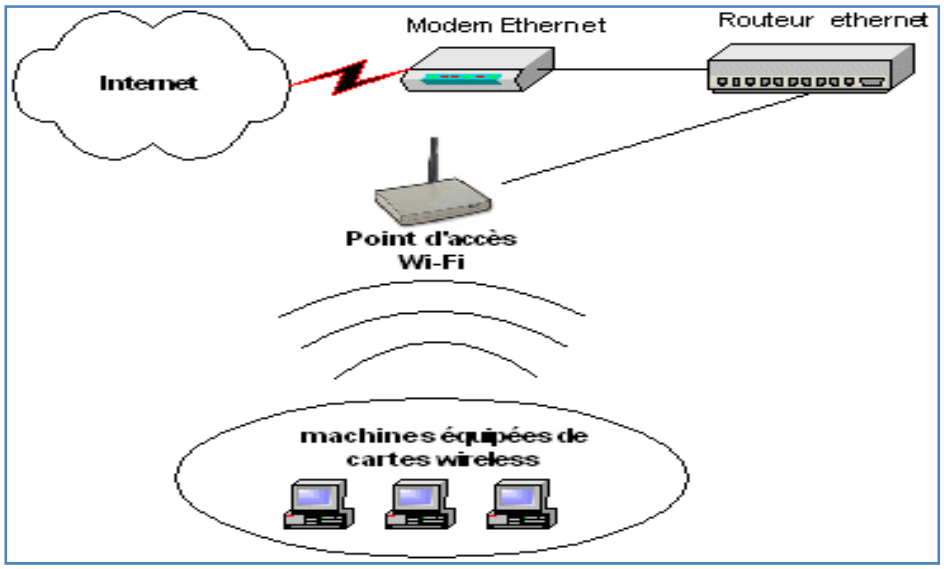


Figure. II.3 : Principe d'un réseau WIFI

II.2.2. Standard

La norme 802.11 s'attache à définir les couches basses du modèle OSI (Open System Interconnection) pour une liaison sans fil utilisant des ondes électromagnétiques, c'est-à-dire :

- **La couche physique** (notée parfois couche PHY), proposant des types de codage de l'information.
- **La coche liaison de données**, constituée de deux sous – couches : le contrôle de la liaison logique (Logical Link Control ou LLC) et le contrôle d'accès au support (Media Access Control ou MAC).

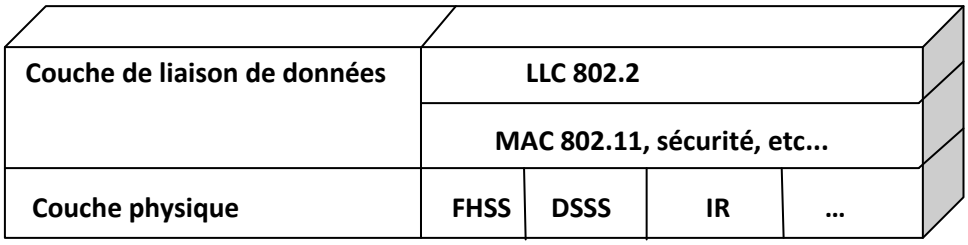


Figure.4 : Modèle IEEE 802.11

Remarque : Il est possible d'utiliser n'importe quel protocole sur un réseau sans fil wifi au même titre que sur un réseau Ethernet.

II.3. Les Différentes Normes WIFI

La norme IEEE 802.11 est en réalité la norme initiale offrant des débits de 1 ou 2 Mbps. Des révisions ont été apporté à la norme originale afin d'optimiser le débit (c'est le cas des normes 802.11a, 802.11b et 802.11g, appelées normes 802.11 physique) ou bien préciser des éléments afin d'assurer une meilleure sécurité ou une meilleure interopérabilité, voici un tableau présentant les différentes révisions de la norme 802.11 et leur signification :

Nom de la Norme	Nom	Description
802.11a	Wifi5	La norme 802.11a (baptisé Wi-Fi 5) permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). La norme 802.11a spécifie 52 canaux de sous-porteuses radio dans la bande de fréquence des 5 GHz. Il y a huit combinaisons, non superposées sont utilisables pour le canal principal.
802.11b	Wifi	La norme 802.11b est la norme la plus répandue actuellement. Elle propose un débit théorique de 11 Mbps (6 Mbps réels) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2.4 GHz, avec, en France, 13 canaux radio disponibles dont 4 au maximum non superposés (1 - 5 - 9 - 13).
802.11c	Pontage 802.11 vers 802.1d	La norme 802.11c n'a pas d'intérêt pour le grand public. Il s'agit uniquement d'une modification de la norme 802.1d afin de pouvoir établir un pont avec les trames 802.11 (niveau liaison de données).
802.11d	Internationalisation	La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11. Elle consiste à permettre aux différents équipements d'échanger des informations sur les plages de fréquence et les puissances autorisées dans le pays d'origine du matériel.
802.11e	Amélioration de la qualité de service	La norme 802.11e vise à donner des possibilités en matière de qualité de service au niveau de la couche liaison de données. Ainsi cette norme a pour but de définir les besoins des différents paquets en termes de bande passante et de délai de transmission de telle manière à permettre notamment une meilleure transmission de la voix et de la vidéo.
802.11f	Itinérance (roaming)	La norme 802.11f est une recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole Inter-Access point roaming protocol permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau. Cette possibilité est appelée itinérance (ou roaming en anglais)
802.11g		La norme 802.11g offre un haut débit (54 Mbps théoriques, 30 Mbps réels) sur la bande de fréquence des 2.4 GHz. La norme 802.11g a une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b
802.11h		La norme 802.11h vise à rapprocher la norme 802.11 du standard Européen (HiperLAN 2, d'où le h de 802.11h) et être en conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie.
802.11i		La norme 802.11i a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'AES (Advanced Encryption Standard) et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
802.11Ir		La norme 802.11r a été élaborée de telle manière à utiliser des signaux infra-rouges. Cette norme est désormais dépassée techniquement.
802.11j		La norme 802.11j est à la réglementation japonaise ce que le 802.11h est à la réglementation européenne.

II.3.1. Normes

1. IEEE 802.11b (en1999)

- Norme du Wi-Fi de base la plus répandue.
- Distance d'utilisation : jusque 300 mètres.
- Débit théorique de **11Mbit/s** – **6Mbit/s** Réel.
- Bande de fréquence de **2,4 GHz**.
  - Bande ISM: Industrial Scientific Medical.
- 13 canaux possibles – 4 utilisable non superposées.
- Technique d'utilisation d'une bande de fréquence venant des techniques modem : QAM64, OFDM.
- Technique d'accès : CSMA / CA.

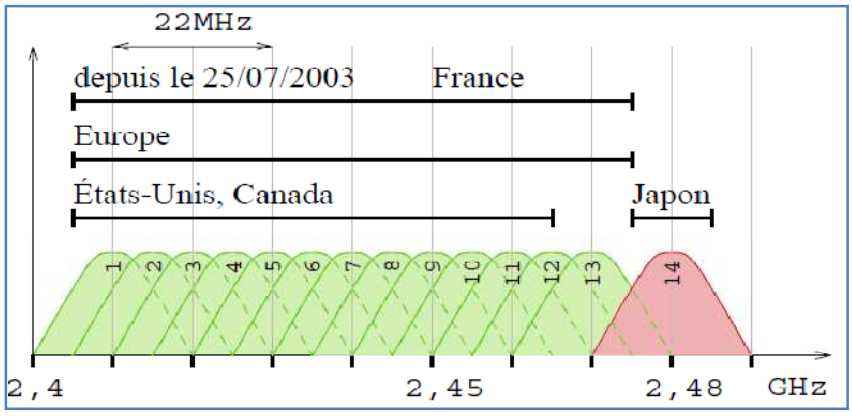


Figure. II.5 *:* Canaux utilisable en 802.11b

2. IEEE 802.11a (en 2000)

- Première norme du Wi-Fi.
- Courte distance d'utilisation : 10 mètres.
- Débit théorique de 54Mbit/s – 27Mbit/s Réel.
- Bande de fréquence de 5 GHz.
  - Bande UNII (Unlicensed National Information Infrastructure).
- 52 canaux possibles – 8 utilisable non superposées.
- Technique de modulation : OFDM, sur 52 porteuses distinctes.
- Méthode d'accès : CSMA / CA.

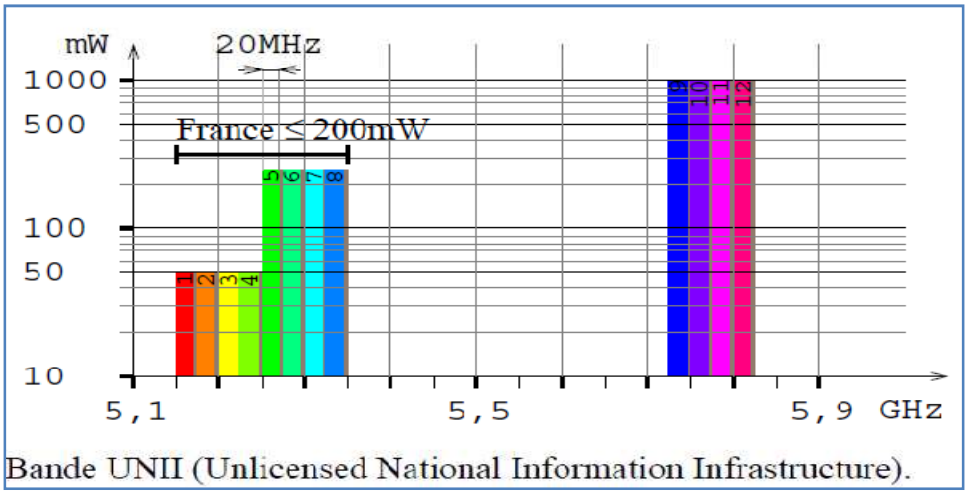


Figure. II.6 *:* Canaux utilisable en 802.11a

3. IEEEE 802.11g (en 2003)

- La norme la plus répandue actuellement sur la marché.
- Distance d'utilisation : jusque 300 mètres.
- Haut Débit théorique de 54Mbit/s – 25Mbit/s Réel.
- Bande de fréquence de 2,4 GHz.

o Bande ISM : Industrial Scientific Medica

- 13 canaux possibles – 4 utilisable non superposées.
- Compatibilité ascendante avec la 802 .11b

o Les équipements 802.11g fonctionnent sur des APs 802.11b.

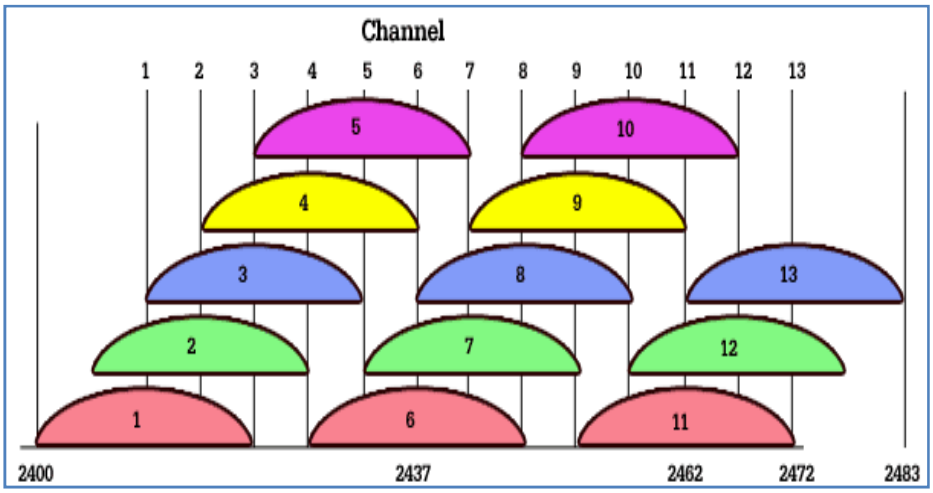


Figure. II.7 : Distribution des 13 canaux du wifi 802.11 b/g.

4. IEEE 802.11n (2009)

- Technologie MIMO : Multiple-Input Multiple Output.
- Technologie OFDM : Orthogonal Frequency Division Multiplexing.
- Distance d'utilisation : jusque 90 mètres.
- Haut Débit théorique de 600Mbit/s – 108Mbit/s Réel.
- Bande de fréquence de **2,4 GHz** et **5GHz.**
- 13 canaux possibles – 8 utilisable non superposées.

II.3.2 Fréquence

Le 802.11a opère dans la plage des 5 GHz mais la plupart des réseaux wifi actuels sont des 802.11b et 802.11g qui opèrent dans la bande 2,4 -2,4835 GHz. Ces bandes appartiennent au spectre ISM besoin de licence ou d'autorisation préalable.

Le débit de la portée dépend essentiellement de l'environnement :

- Type de construction (mur, cloisons, etc.).
- Implantation des antennes.
- Interférences (Bluetooth, micro-ondes, autre réseaux wifi, etc.).

II.4. Le mode de fonctionnement

On distingue deux modes de fonctionnement

II.4.1. Le mode infrastructures

Le réseau sans fil consiste au minimum en un point d'accès à l'infrastructure du réseau filaire et un ensemble de postes réseaux sans fil. Cette configuration est baptisée Basic Service Set (BSS, ou ensemble de service de base). Un Extented Service Set (ESS, ou ensemble de service étendu) est ensemble d'au moins deux BSS formant un seul sous-réseau

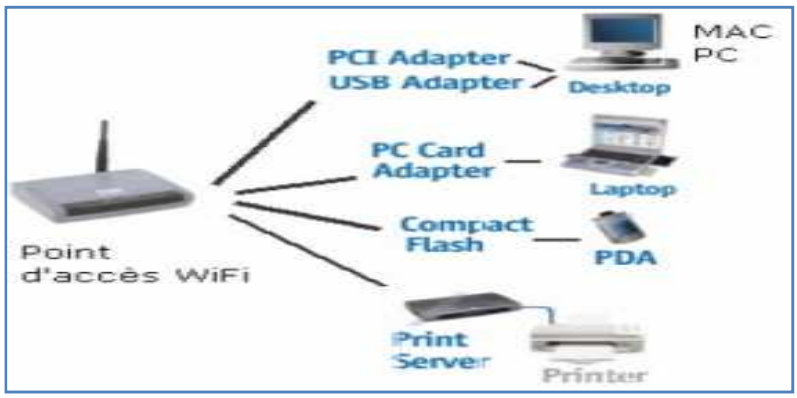


Figure. II.8: Mode infrastructure.

II.4.2. Le mode Ad hoc

Egalement baptisé point à point, il représente simplement un ensemble de stations sans fil 802.11 qui communiquent directement entre elles sans point d'accès ni connexion à un réseau filaire ; les ordinateurs sont en même temps émettrices et réceptrices de données.

Figure.II.9*:* Mode Ad hoc.

II.5. Les Equipements Wifi

La mise en place d'un réseau sans fil Wifi nécessite deux éléments : le point d'accès et les terminaux.

Pléthorique, l'offre actuelle s'appuie sur trois standards : 802.11b (le plus répandu), 802.11a et 802.11g. L'idéal est de sélectionner des équipements 802.11b (les moins chers) lorsqu'une bande passante partagée de 11Mb/s est suffisante, ou des équipements 802.11g lorsque le nombre d'utilisateurs est plus élevé. Les normes 802.11b et 802.11a étant incompatibles entre elles et 802.11g offrant le débit de 802.11a, les équipements 802.11a ont généralement peu d'intérêt.

II.5.1. Les Adaptateurs Sans Fil

En anglais Wireless adapter ou network interface contrôler, noté NIC. Il s'agit d'une carte réseau à la norme 802.11 permettant à une machine de se connecter à un réseau sans fil. Les adaptateurs Wifi sont disponibles dans de nombreux formats (carte PCI, carte PCMCIA, adaptateur USB, carte compact flash,...). On appelle station tout équipement possédant une telle carte. A noter que les composants Wi-Fi deviennent des standards sur les portables (label Centrino d'Intel).

Figure. II.10 : carte PCI.

II.5.2. Les Points D'accès

Notés AP pour Access point, parfois appelés bornes sans fil, permettant de donner un accès au réseau filaire (auquel il est raccordé) aux différentes stations avoisinantes équipées de cartes Wifi. Cette sorte de hub est l'élément nécessaire pour déployer un réseau centralisé en mode infrastructure. Certains modèles proposent des fonctions de modem ADSL et comprennent plus ou moins de fonctions comme un pare-feu.

Figure. II.11 : Access point.

II.6. Avantages et contraintes du wifi

II.6.1. Les avantages

Comme les autres réseaux sans fil, le Wifi possède plusieurs avantages tels que :

- la facilité de déploiement.
- le faible coût d'acquisition.
- la mobilité.

De plus, le Wifi est interopérable avec les réseaux filaires existants et garantit une grande souplesse sur la topologie du réseau.

- Attention, il est toutefois nécessaire de relativiser les trois avantages cités ci-dessus en fonction du niveau de sécurité que l'on compte appliquer sur son réseau.

II.6.2. Les contraintes

- **Débit**

  Débits proches des réseaux filaires, mais plus le sans fil est plus sensible à des phénomènes de congestion.

- **Zone de couverture (10 à 100 m)**

  Varie en fonction des interactions avec les murs, de la puissance du signal.

- **Interférences**

  Problème si plusieurs réseaux sans fil proche.

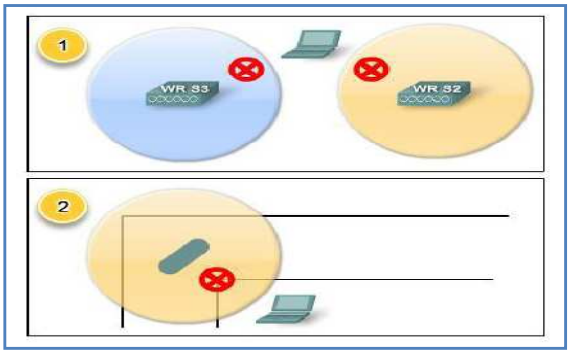


Figure.II.12 : Problème de couverture

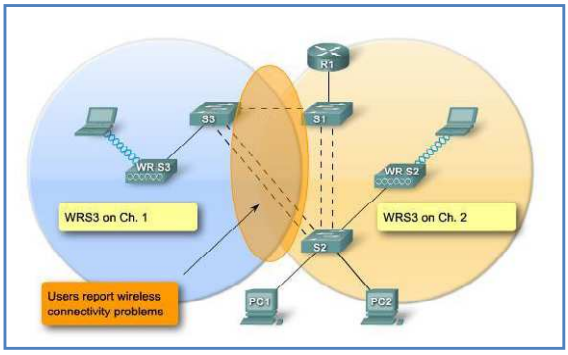


Figure.13 : Problème d'interférence

II.7. Sécurité dans les réseaux WIFI

La confidentialité des informations traitées par les équipements et réseaux Wifi étant encore insuffisante, car les technologies sans fil gèrent mal la sécurité.

- La première raison tient au fait que ce type de connexion s'appuie sur une transmission radio et qui se propage « dans l'air ».
- La deuxième raison est liée à la norme 802.11b qui présente des failles de sécurité.

- Et enfin la troisième vient souvent des utilisateurs qui omettent de mettre en œuvre les protocoles de sécurité de cette norme ou les logiciels de sécurité fournis avec les cartes Wifi.

Des systèmes de protection et de sécurité existent, pour l'essentiel sur les points d'accès et la carte, mais ils ne sont pas toujours activés.

II.7.1. Types de menace

- ✓ L'interception de données.
- ✓ L'usurpation de connexion.
- ✓ Le brouillage des transmissions: interférences.

II.7.2. Mécanismes de sécurité

1. Le WEP: (Wide Equivalent Privacy).

- ✓ Utilisé dans le Wifi: pour gérer le SSID (Service Set ID).
- ✓ Vulnérable à cause du chiffrement RC4.

2. Le WPA: (Wi-Fi Protocol Access).

- ✓ Prévu pour remplacer le WEP.
- ✓ Repose sur un échange de clés dynamiques (TKIP:Temporal Key Integrity Protocol)
- ✓ Renouvelées tous les 10 Ko de données

3. AAA: (Authentication, Authorization and Accounting).

- ✓ Mieux gérer les authentifications, autorisation, et gestion des comptes utilisateurs.
- ✓ Utilisé avec un serveur RADIUS.

4. Le filtrage d'adresses MAC

Déclarer au niveau AP les adresses MAC ayant le droit d'accès au réseau, Ce mécanisme contraignant permet d'éviter l'intrusion réseau mais pas la confidentialité des échanges.

5. La disposition intelligente des AP

Les valeurs par défaut: à éviter.

- ✓ Mots de passe.
- ✓ Désactiver la diffusion du SSID: SSID broadcast.

6. Les VPN

Evitent un bon nombre d'intrusions

- ✓ Pour les communications sensibles ou il faut avoir un haut niveau de sécurité.
- ✓ L'utilisation des VPN est nécessaire.

7. Le DHCP (Dynamic Host Configuration Protocol)

A désactiver si possible (IP fixes).

8. Le Pare-feu: à installer

Figure.II.14 : Réseau filaire et Wifi sécurisé

II.8 Conclusion

Comme en vient de la voir, si le réseau Wifi représente des avantages en confort et en utilisation qui est considérables, il n'est pas adapté à de lourdes charges, et il faut savoir que les coûts économisés en évitant un câblage Ethernet pour les postes des utilisateurs peuvent être dépassés par d'autres coûts auxquels on n'a pas forcément pensé à l'origine.

En pratique, les réseaux Wifi sont performants en mode client-serveur avec des échanges courts (navigation Internet par exemple), ce qui explique leur succès auprès des particuliers. Il est quasiment certain que lors de l'utilisation d'application métier « lourdes» (montage vidéo, transferts de gros fichiers, CAO et dessin, etc.) via des réseaux Wifi cela posera un certain nombre de difficultés.

Les problèmes de sécurité (confidentialité, intégrité) ont été résolus avec succès, ce qui permet un déploiement sans craintes en entreprise par rapport à cet aspect. Cependant l'aspect disponibilité ne pourra en aucun cas être garanti, et pour les applications critiques nécessitant une disponibilité maximale, l'utilisation de réseaux wifi doit être proscrite.

Partie pratique

Chapitre III
Etude et déploiement du réseau WiFi Hotspot

III.1. Simulations

Afin de mieux apprécier les contraintes techniques à prendre en compte lors du déploiement d'un réseau sans fil, compte tenu des technologies existantes, nous commencerons par l'étude de plusieurs scénarios réalistes au moyen de simulations mettant en œuvre des topologies particulières propres à l'université.

Ces simulations seront faites à l'aide du simulateur Ekahau. L'objectif de ces simulations sera de voir les facteurs pouvant influencer sur la puissance du signal reçu et le débit de la connexion.

En ce basant sur le fait que les problèmes de connexion et de faiblesse du signal dans les réseaux sans fils sont dus à un mauvais déploiement, nous allons dans le premier lieu donc faire une analyse en ce qui concerne le déploiement d'un réseau sans fils en générale et enfin utiliser les résultats de cette analyse et d'autres informations afin de proposer un modèle de déploiement pour le réseau sans fils de site pilote au profit de la résidence universitaire.

III.1.1. Outil de simulation

L'outil de simulation fournit par l'équipementier Siemens est le logiciel nommé **Ekahau Site Survey** v 2.2 conçu et utilisé pour pallier aux problèmes de mauvais déploiement des réseaux Wifi et aux contraintes techniques tels que les interférences et signal/bruit.

III.1.2. Etude du site

Les analyses et les études de site consisteront sur la partie radio et couverture qui appuieront sur les points essentiels rémunérés comme suite :

- **Intensité du signal (*RSSI)*** en dBm.
- **Rapport signal-bruit (RSB)** en dB.
- **Interférences** en dBm.
- **Signaux sur le canal (RSSI)** Bande / Canal.
- **Point d'accès le plus puissant** ESS.
- **Compte des points d'accès** (Nbre AP)
- **Conseil de placement du point d'accès**.
- **Estimation de l'emplacement du point d'accès** (localisation des AP).
- **Débit** (basé sur la charge du réseau/l'adaptateur/RSB).

L'étude de site pilote nécessitera un plan architecturale en fichier (.drw) à l'échelle et pixels bien définis et choisis afin de l'intégrer sur la carte du logiciel afin de générer et créer un rapport en model sélectionné.

III.2. Rapport de l'étude

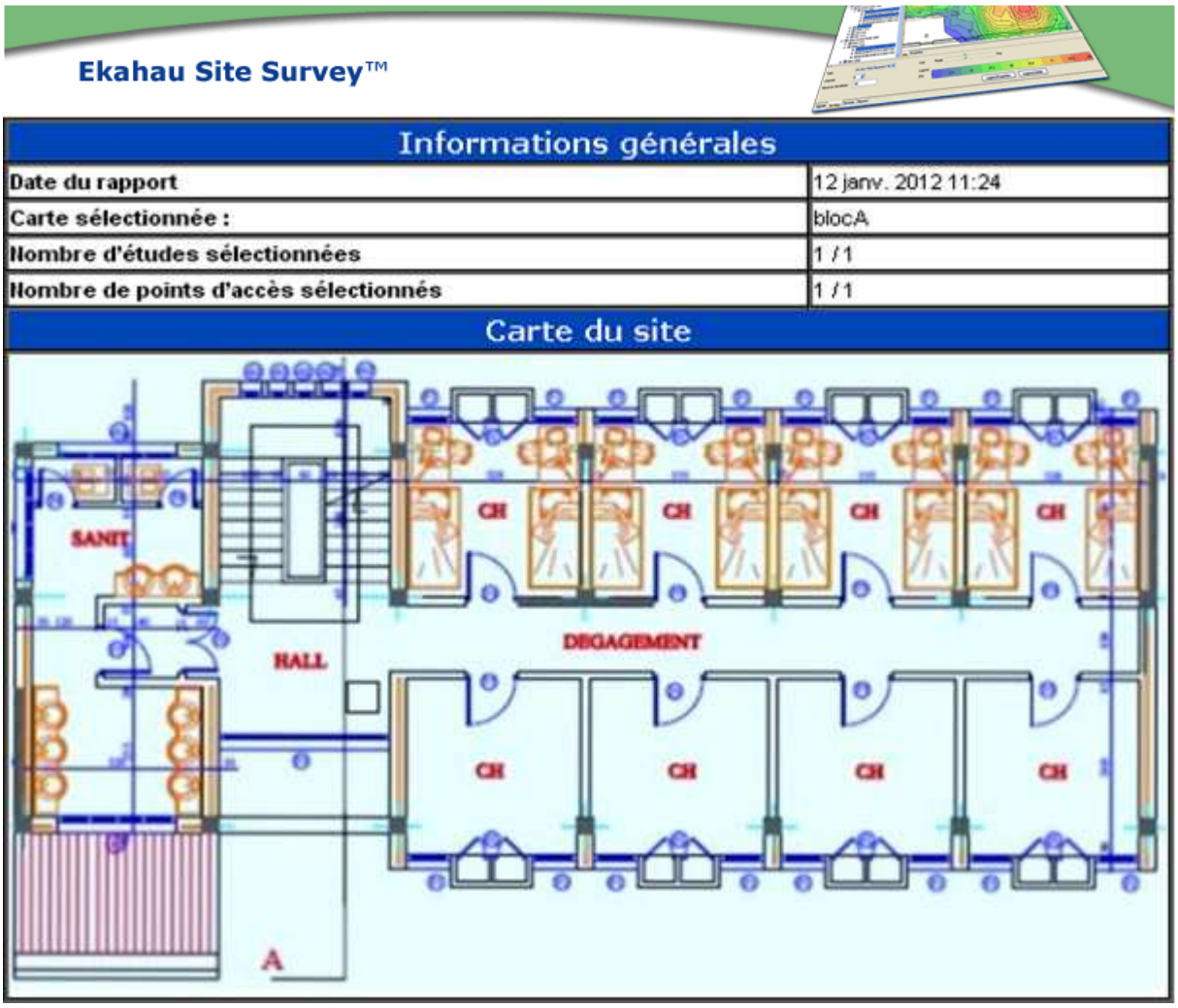


Figure.III.15 : Carte de site à étudier.

Études sélectionnées

Nom	Créée	Notes
12 janv. 2012	12 janv. 2012 1:44:39	

Points d'accès sélectionnés

ESSID	Nom	Bande / canal	Confidentialité
Réseau simulé	00:00:00:00:00:01	802.11g / 1	

Puissance de transmission et informations sur l'antenne

Nom	Puissance de transmission	Antenne	Hauteur	Direction
00:00:00:00:00:01	50	Omni-directional Antenna (2.15 dBi)	2.7	360

Notes sur le point d'accès

Nom	Notes
00:00:00:00:00:01	

Points d'échantillonnage et position des points d'accès

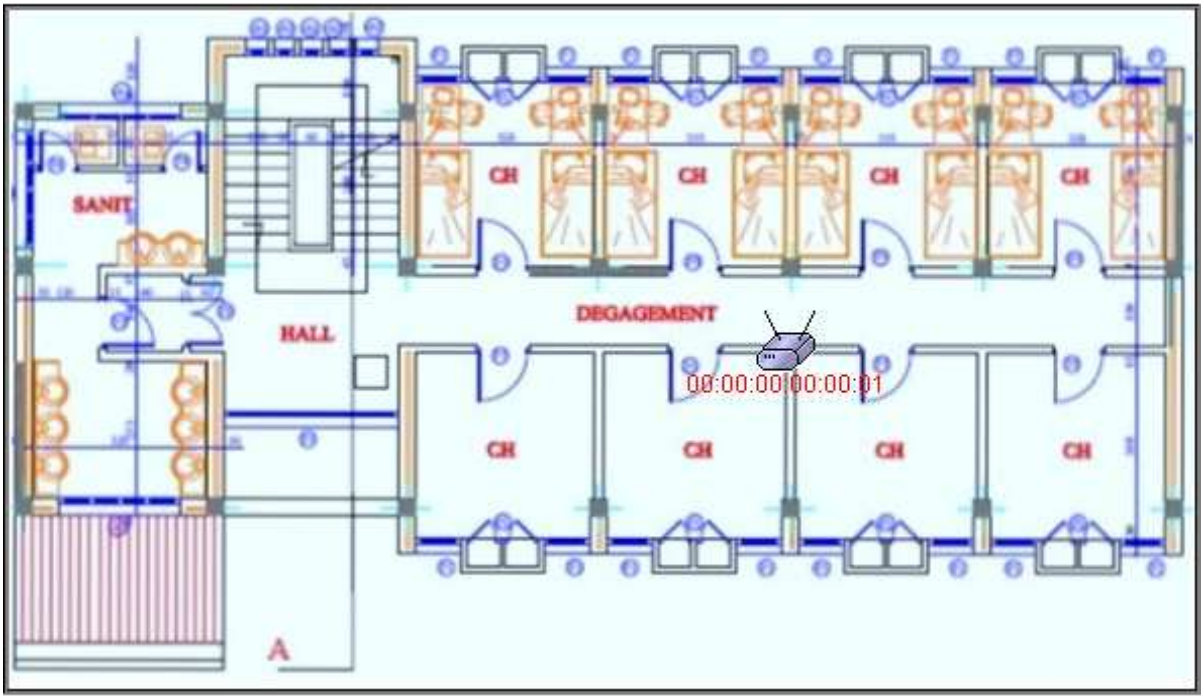


Figure.III.16 : Echantillonnage et positionnement des APs.

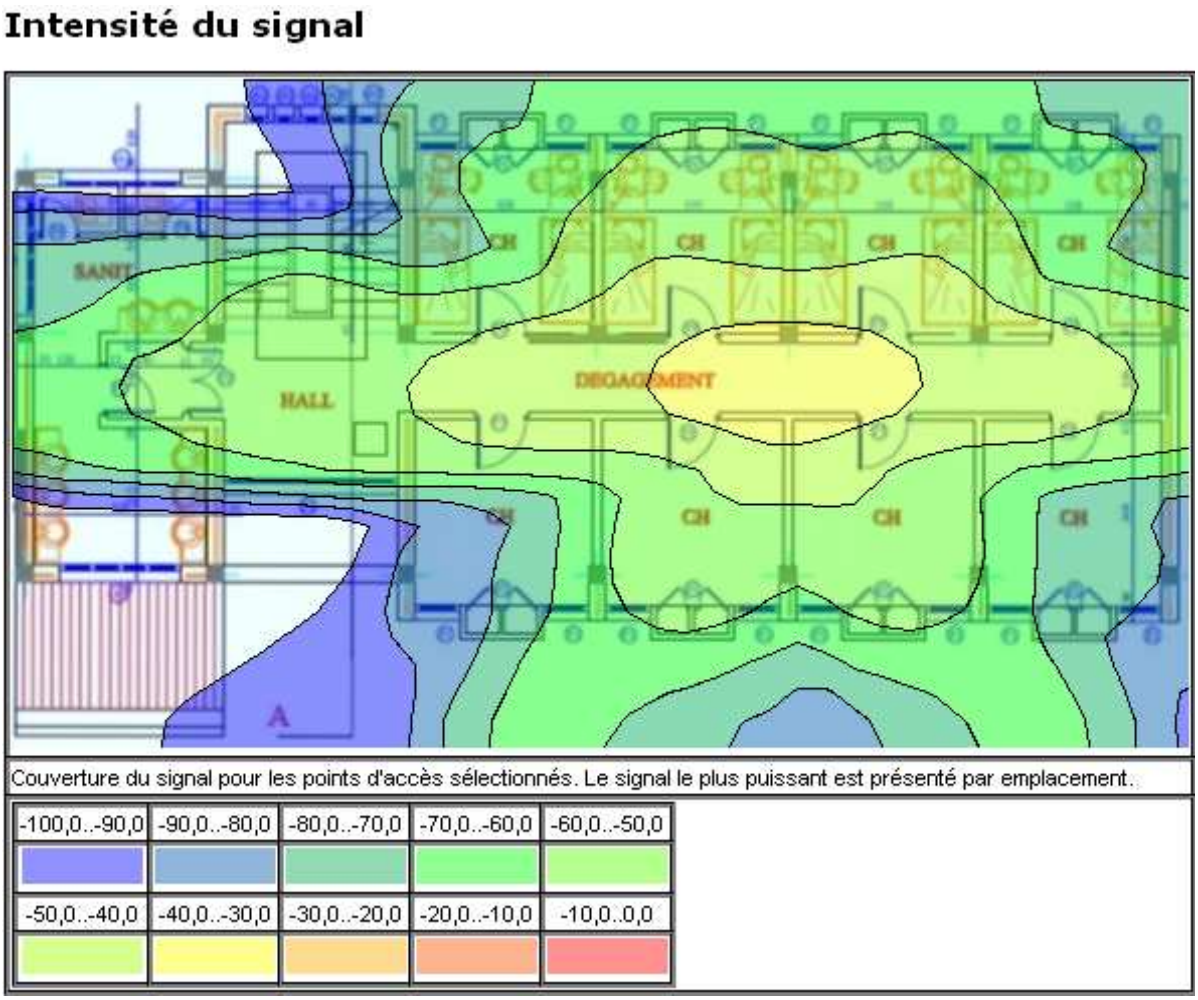


Figure.III.17 : Intensité Du Signal

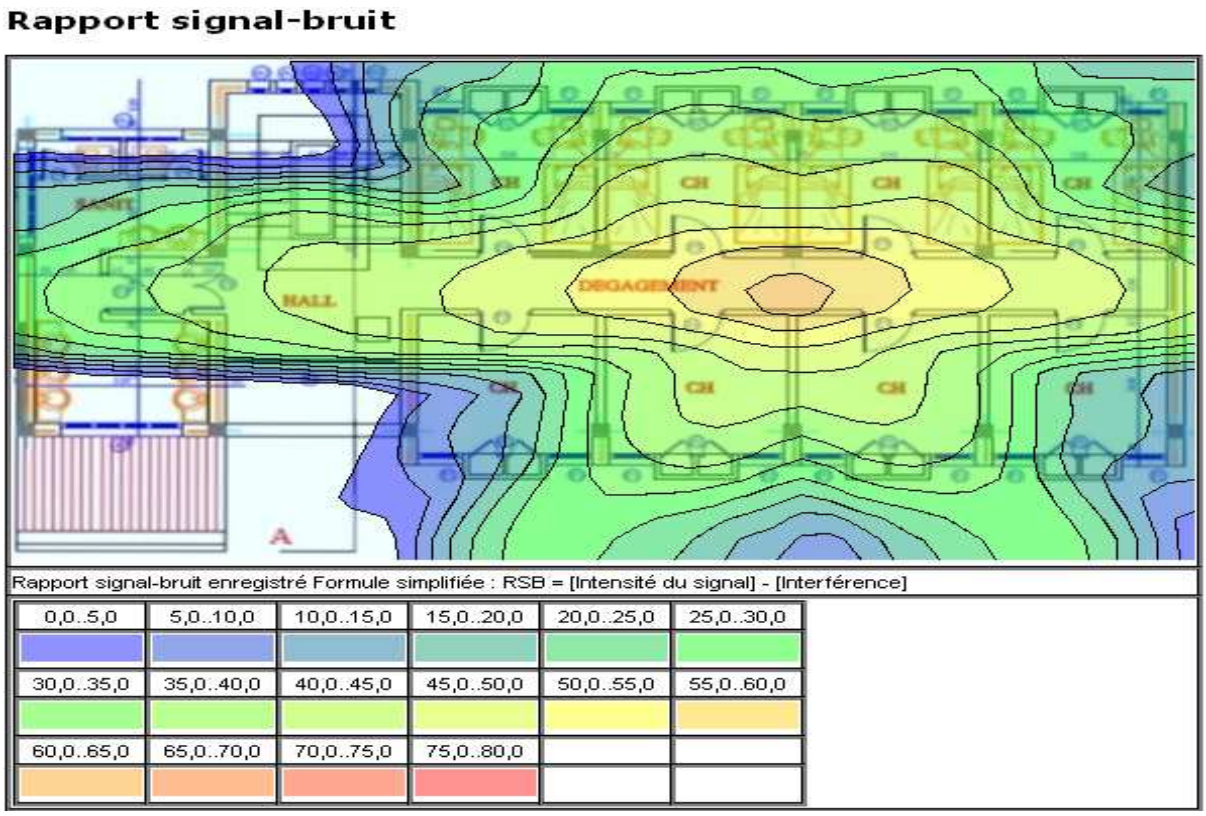


Figure.III.18 : Rapport Signal-Bruit.

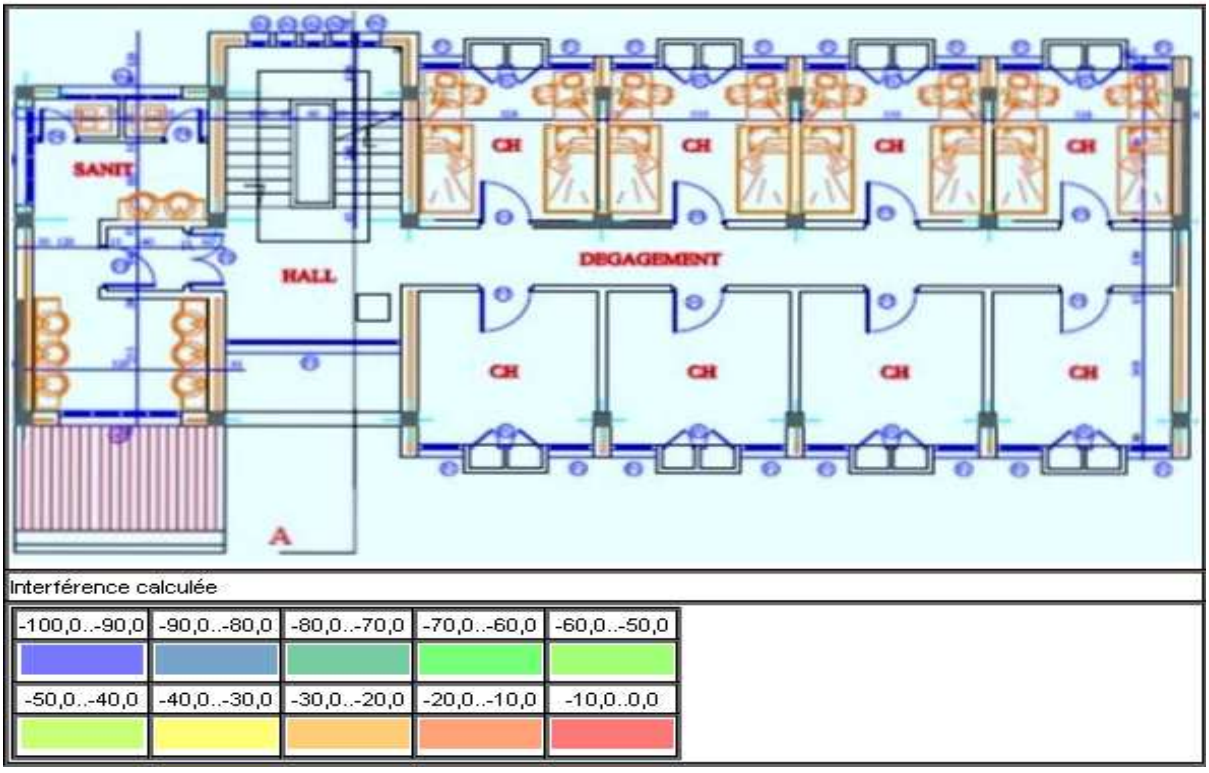


Figure.III.19 : Les Interférences.

Compte des points d'accès

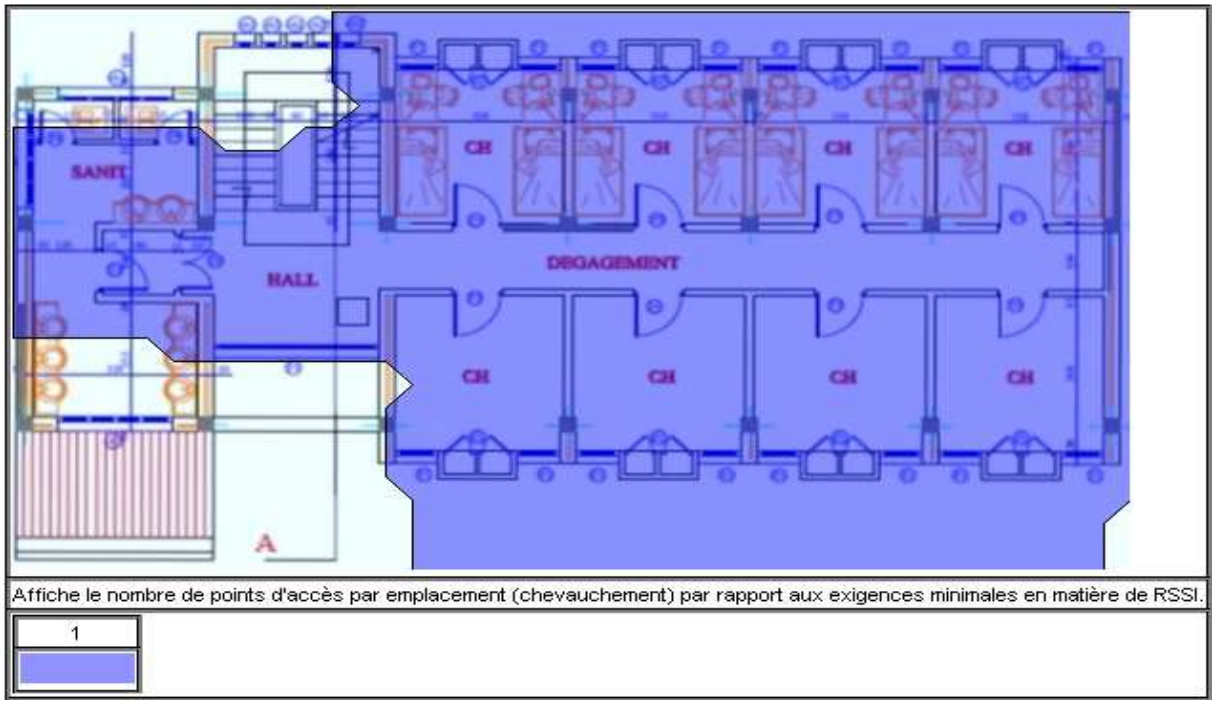


Figure.III.20 : Compte des APs.

Débit

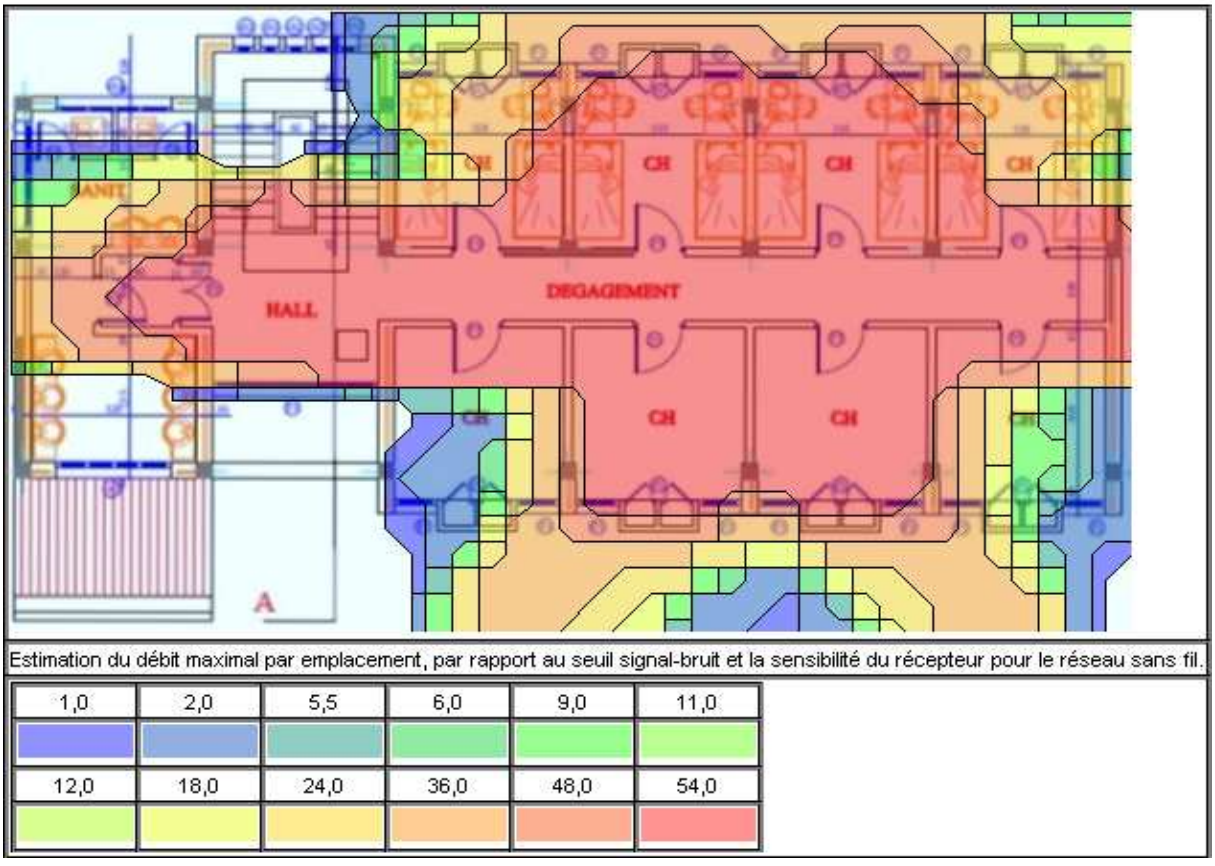


Figure.III.21 : Le Débit.

III.3. Optimisation de déploiement

Pour confirmer et compléter les résultats de ses simulations nous allons également faire quelques mesures sur le terrain afin d'étudier de façon plus concrète l'impact du bruit ambiant sur la puissance utile. Nous verrons également comment la présence des murs et d'autres obstacles peuvent absorber le signal et causer une couverture partielle ou incomplète.

En plus des solutions existantes citées dans l'état de l'art, il existe également d'autres recommandations pour lesquels nous ne pourrons pas faire de teste ni de simulation nous allons tout simplement faire confiance à la source de ces informations et les respecter dans nos déploiement :

- La détermination du nombre de maximal de connexions possible par point d'accès nécessaires pour assurer la connexion et garantir un certain débit pour chacun des utilisateurs.
- Placer les points d'accès sur les obstacles afin de minimiser les zones d'ombre.
- Prévoir un chevauchement de 10 à 15% entre les diamètres de couverture des points d'accès pour assurer le roaming (passage d'un point d'accès à un autre sans déconnexion).
- Positionnez les points d'accès à la verticale près du plafond et au centre de chaque zone de couverture.
- Installez les points d'accès à des endroits où les utilisateurs sont appelés à travailler.

III.3.1 Modèle de déploiement

L'étude de faisabilité et la couverture radio du site universitaire nous a permit de dresser un tableau quantitatif du besoin aux équipements Wifi, connectique, passifs et actifs consommés par le dite réseau informatique suite à une architecture élaborée en préalable.

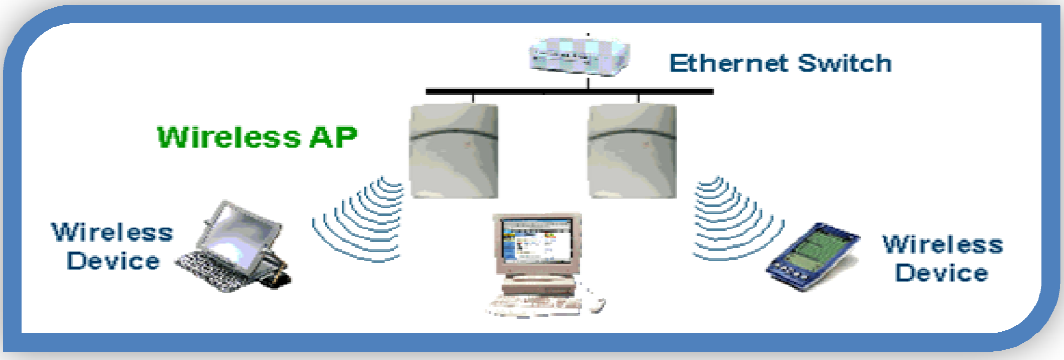


Figure.III.22 : Modèle de déploiement.

Selon la fonctionnalité et les caractéristiques techniques et spécifiques aux points d'accès de marque Siemens.

III.3.2 Déploiement de site

Figure.III.23 : Architecture De Réseau WiFi.

Installation sur site

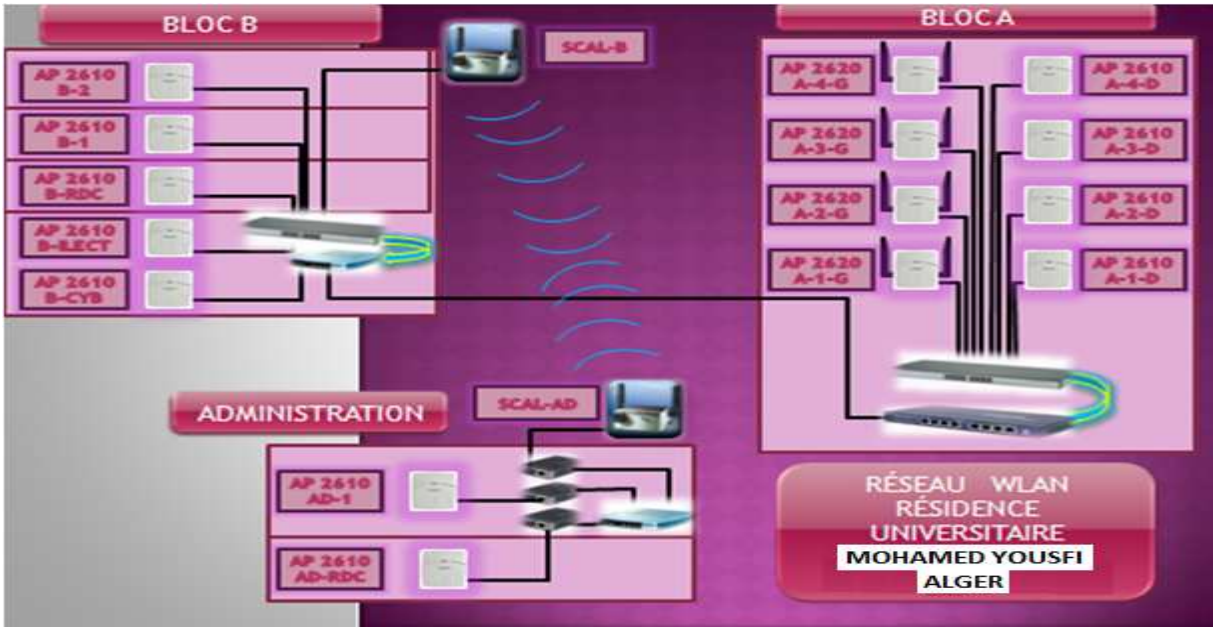


Figure.III.24 : Installation du réseau sur site.

III.4. Tableau Quantitatif des Equipements Informatiques

DESIGNATION	Model	Quantité
Contrôleur	C1000	01
Point d'accès Hipath	2610	32
Scalance	W788	02
Jarretière optique duplex	MTRJ/LC	02
Switch L 3 24 ports	Q3528	01
Module SFP	850nm	02
Convertisseur SC	FO/FE	02
Tiroir optique		02
Pigtail monomode	SC	02
Switch Ethernet	24 ports	02
Switch Ethernet	08 ports	00
Hub PoE	08 ports	04
Injecteur PoE	01 port	02
Armoire de brassage	9 U	02
Panneau de brassage	24 ports	02
Onduleur	1 KVA	02
Bandeau d'alimentation	05P + Int	02
Câble FTP	cat5e	500ml
Câble FTP	Cat6	00
Connecteur	RJ45	70
Goulotte	40x20	150ml
Accessoires goulotte	Angles	20

III.5. Travaux réseau WiFi

Le déroulement des travaux se feront dans l'ordre suivant

- Fixation de goulotte.
- Tirage de câble FTP cat 5e dans les goulottes reliant chaque point d'accès vers le l'armoire 9U contenant le Switch Ethernet à travers les colonnes montantes.
- Fixation des armoires de brassage 9U sur les murs.

- Pose des équipements actifs rackables dans les armoires tels que le Switch Ethernet, Hub et injecteur PoE qui alimente les AP 2610/20 via le câble FTP, onduleur pour secourir le matériel informatique.
- Fixation des bornes Wifi AP2610/20 sur les murs à la hauteur prédéfinie avec sertissage des connecteurs RJ45.
- Raccordement et branchement de tous les équipements en câble FTP et l'énergie.
- Cascade entre toutes les armoires par câble FTP, Scalance ou fibre optique en utilisant les convertisseurs FO/FE.

SOLUTION TECHNIQUE

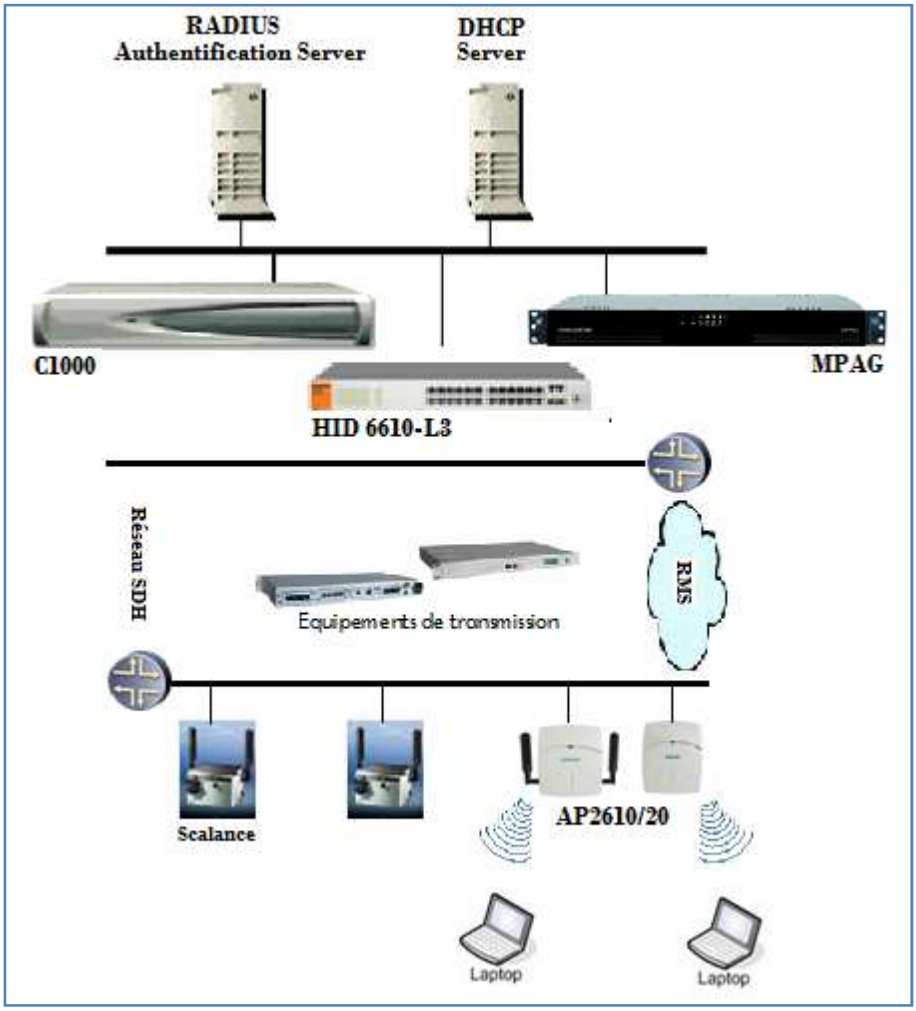


Figure.III.25 : Solution technique.

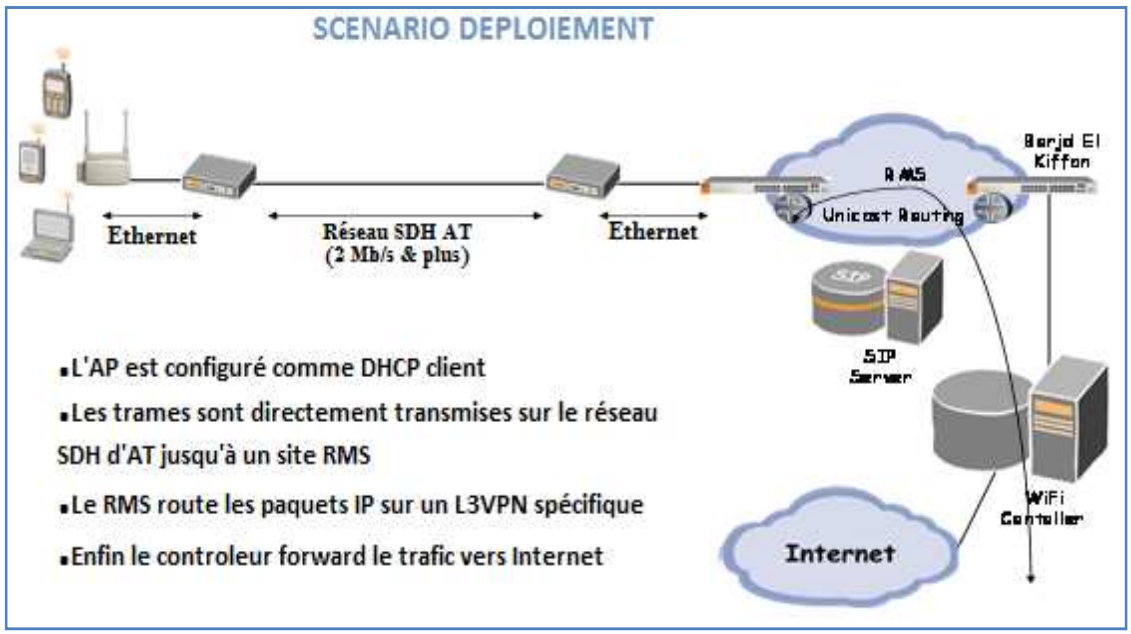


Figure.III.26 : Scenario déploiement.

III.6. Les équipements Wi-Fi

III.6.1. Points d'accès

Les points d'accès Siemens possèdent deux modèles dans la série 26xx non manageables :

- AP 2610 : antenne interne double multimode.
- AP 2620 : double antennes externe.

antenna name= "AP2610_2400MHz"		antenna name= "AP2620_2400MHz"	
Angle	Gain (dbi)	Angle	Gain (dbi)
0	2.5	0	4
60°	5		
90°	-0.5	90	0.3
180°	0	180	4
270°	-1	270	0
360°	2.5	360	4

Ces points d'accès ont deux bandes radios avec le standard 802.11 :

- Bande 2.4 GHz: supporte le standard 802.11b/g pour un débit théorique de 11-54Mb/s.
- Bande 5 GHz: supporte le standard 802.11a pour un débit théorique de 54Mb/s.

La solution pour gérer et administrer les points d'accès repose sur deux services :

- DHCP : (Dynamic Host Configuration Protocol) protocole qui attribue automatiquement les adresses IP aux périphériques réseaux (cartes réseau, points d'accès, PDA,…)
- SLP : (Service Location Protocol) protocole qui alloue des applications (SA ou DA) pour découvrir les services réseau sans connaitre leurs emplacements DA (directory agent)

III.6.2. Les antennes (Scalance 788W)

Les Scalances sont des antennes fiables, robustes et étanches à l'eau et aux poussières désignés dans le milieu industriel utilisé comme point d'accès ou liaison point à point servant à interconnecter entre différents blocs les sous réseaux WiFi ou LAN, transport de données ainsi d'assurer la couverture radio pour se connecter dans une zone arrosée dans un périmètre, et supportant et conviennent pour les deux radios de fréquences 2.4 GHz & 5 GHz respectivement conformes aux standards 802.11b/g & a pour une bande passante jusqu'à 54Mbps.

Figure.III.27 : Scalance 788W.

III.6.3. Le Contrôleur C1000

Le Contrôleur doit être compatible et synchronisable avec n'importe quel produit WLAN standard et constitue une solution de gestion complète de services d'accès au réseau, aussi bien pour un usage prive que public ou mixte.

La prise en compte des contraintes techniques par un contrôleur d'accès libère le gestionnaire de sites de tâches complexes ou répétitives.

Figure.III.28: Contrôleur C1000.

Pour la mise en place de la norme 802.11i et l'authentification EAP sur une infrastructure WiFi en entreprise, le Local contrôleur agit comme serveur RADIUS permettant aux utilisateurs de s'authentifier avec les méthodes EAP, PEAP, TTLS ou TLS.

Le contrôleur proposé protège le réseau entreprise en authentifiant les utilisateurs avant qu'ils n'accèdent à ses ressources ; l'authentification se fait en environnement sécurisé et les communications entre le terminal utilisateur et le contrôleur sont cryptées (SSL). Un firewall protège des intrusions, et le contrôleur gère les black lists et les white lists par IP, par protocole et par plage d'adresses.

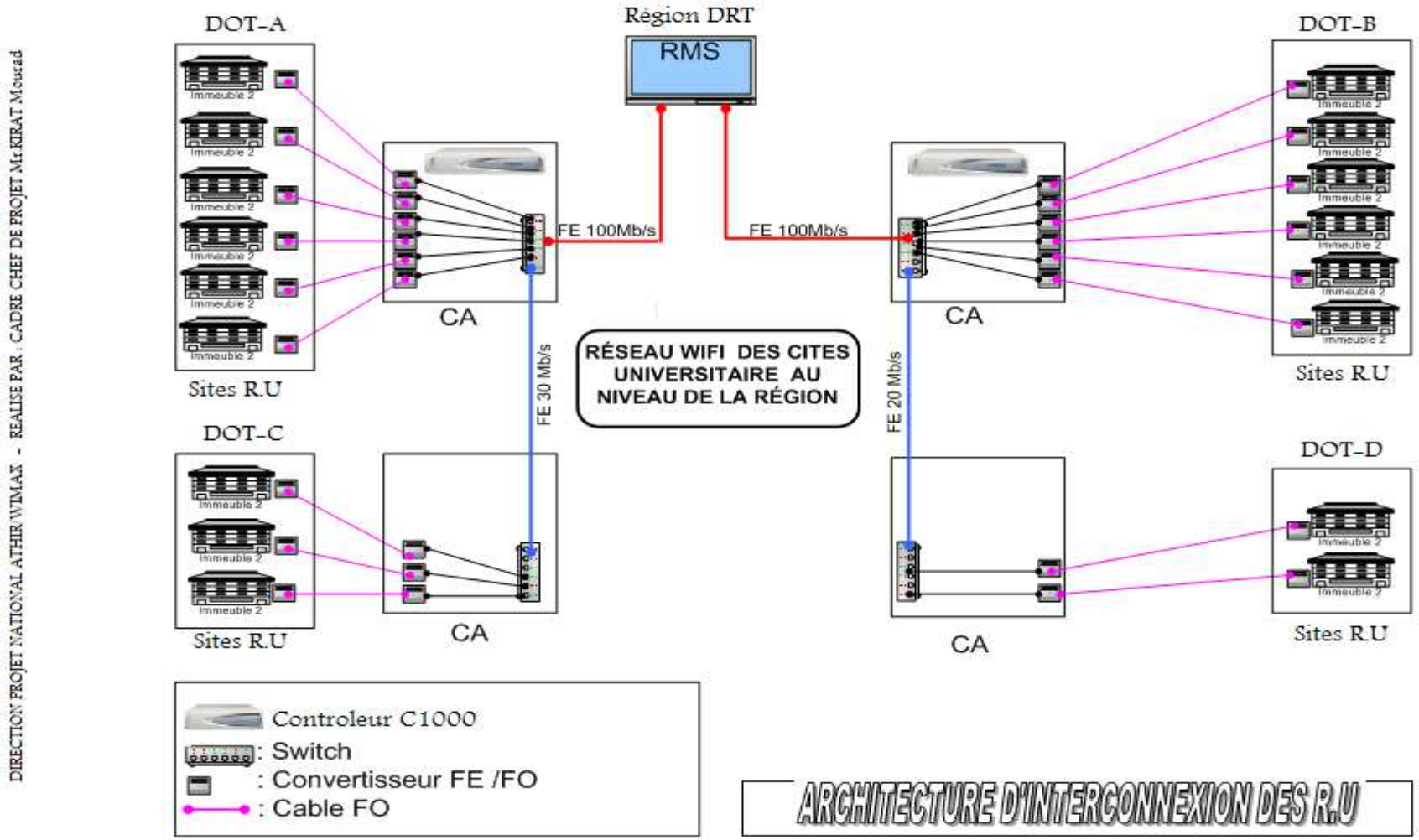
Le C1000 avec la licence attribuée selon l'adresse de management supporte et gère 200 points d'accès synchronisables et permet 4096 accès, possédant deux ports optique Gigabit Ethernet et un port de management 10/100BaseT.

Les caractéristiques du contrôleur :

- Configuration, gestion, rapports et maintenance centralisée.
- Sécurité élevée.
- Flexibilité en fonction entreprise.
- Evolutive et souple en déploiements et contrôle des centaines des points d'accès.

Le contrôleur HWC est construit dans la capacité d'organiser et gérer le point d'accès :

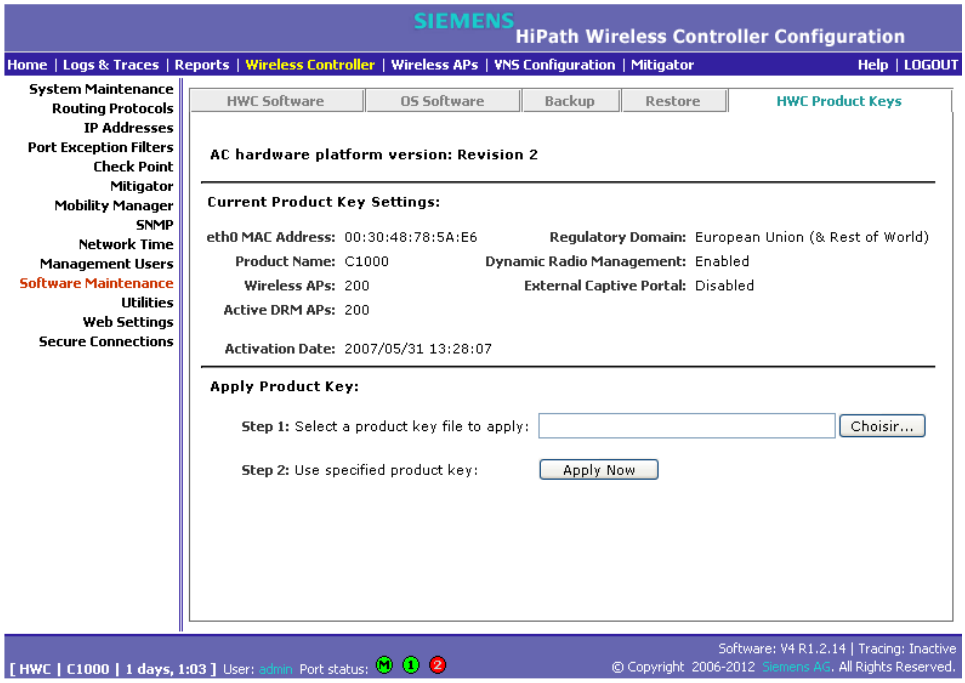
- Active les points d'accès.
- Autorise le point d'accès à recevoir le trafic.
- Processus de trafic des données des points d'accès.
- Transporte et route le processus trafic de données dans le réseau.
- Authentifié les demandes et applique les droits d'accès.


DOT-A
Région DRT
RMS
DOT-B
Immeuble 2
FE 100Mb/s
FE 100Mb/s
CA
CA
Sites R.U
Sites R.U
FE 30 Mb/s
FE 20 Mb/s
RÉSEAU WIFI DES CITES UNIVERSITAIRE AU NIVEAU DE LA RÉGION
DOT-C
DOT-D
CA
CA
Sites R.U
Sites R.U
Controleur C1000
: Switch
: Convertisseur FE /FO
: Cable FO
ARCHITECTURE D'INTERCONNEXION DES R.U
DIRECTION PROJET NATIONAL ATHIR WIMAX - REALISE PAR : CADRE CHEF DE PROJET Mr KIRAT Mourad

III.7. Configuration et Paramétrage du Contrôleur

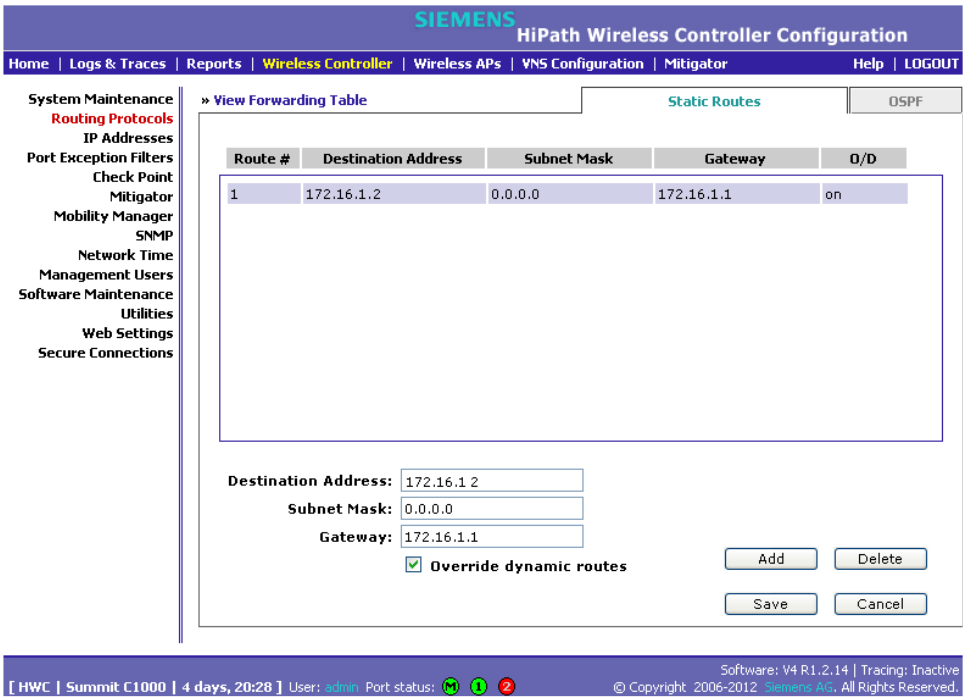
III.7.1. Activation licence

Dans le menu « Software Maintenance », la licence est sélectionnée selon l'adresse Mac du produit et y activée afin de permettre la gérance du quota des points d'accès autorisés.



III.7.2. **Routage** (Statique & Protocole)

Le Routage est utilisé dans le Contrôleur afin de supporter les définitions VNS.

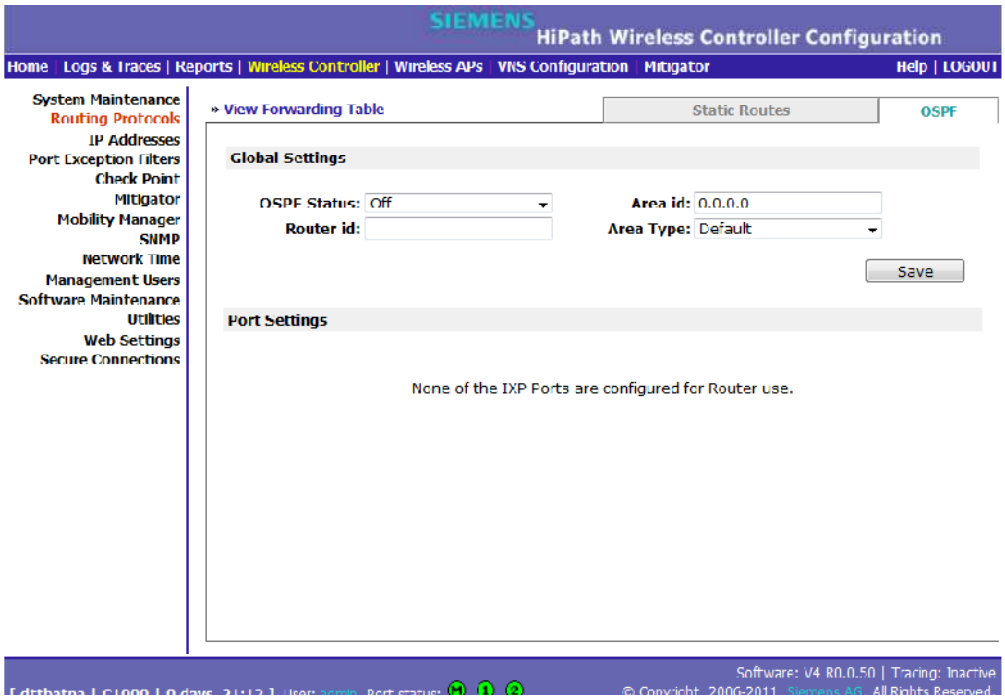


À travers l'interface utilisateur, on peut configurer le « Routing Protcols » à utiliser l'un des techniques de routage :

●**Static routes :** afin de définir un routage par default du contrôleur, par conséquent le trafic des équipements sans fil approuvés peuvent se connecter à la passerelle par défaut.

●**Open Shortest Path First** (OSPF, v2) : permettre au contrôleur à participer à la sélection dynamique route. Ce protocole est désigné pour moyen et large réseaux IP avec habilité à segmenter les routes (voies) dans les différents domaines de routage par un résumé d'informations et propagation.

Remarque : en sélectionnant l'option « Override dynamic routes » la priorité est donné au protocole OSPF de lire les routes incluant la route définie par défaut ; par conséquent en décochant la priorité est affiliée au routage statique.



Remarque: la définition de routage statique et la dynamique peuvent être combinés, mais la statique route prendra du privilège et priorité par rapport à la dynamique.

III.7.3. Plans d'adressage

On procédera en point de vue sécurité à modifier les paramètres par défaut de management et accès au contrôleur comme suite:

Dans « IP Addresses » :

- Hostname
- IP management
- Subnet mask

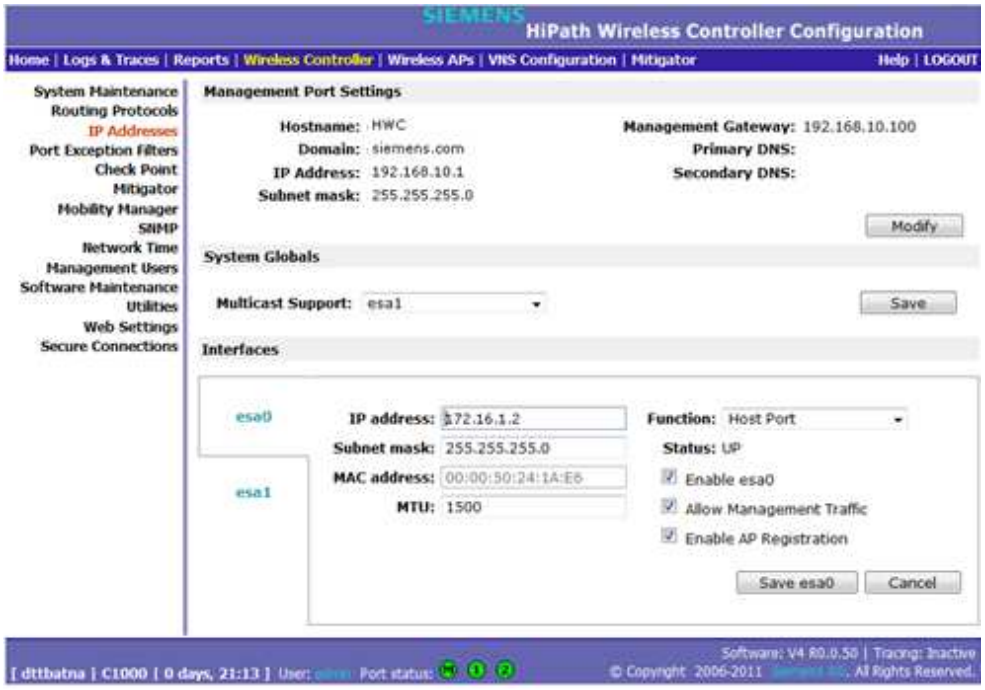
Dans « Management Users » :

- Admin
- User Password

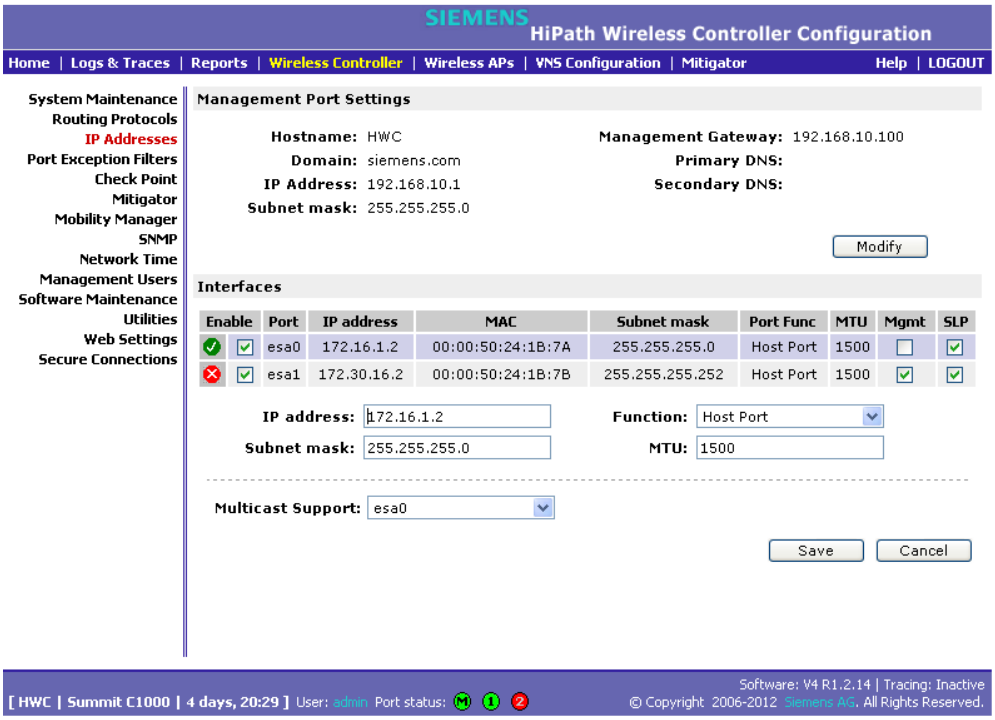
Le prochain initial paramètre à configurer est le port physique de données selon trois types de fonctionnement:

- Host Port
- Third-Party AP Port
- Router Port

Host Port : cette fonction doit être utilisée avec la définition du routage statique pour le non connexion des points d'accès avec la dynamique route qui est désactivé par défaut afin de s'assurer qu'il ne participe pas avec le protocole OSPF.



Remarque: la fonction « Router Port » sera utilisé si on veut se connecter en routeur next-hop dans le réseau, en protocole de routage dynamique à condition que OSPF est ‘’On’’.



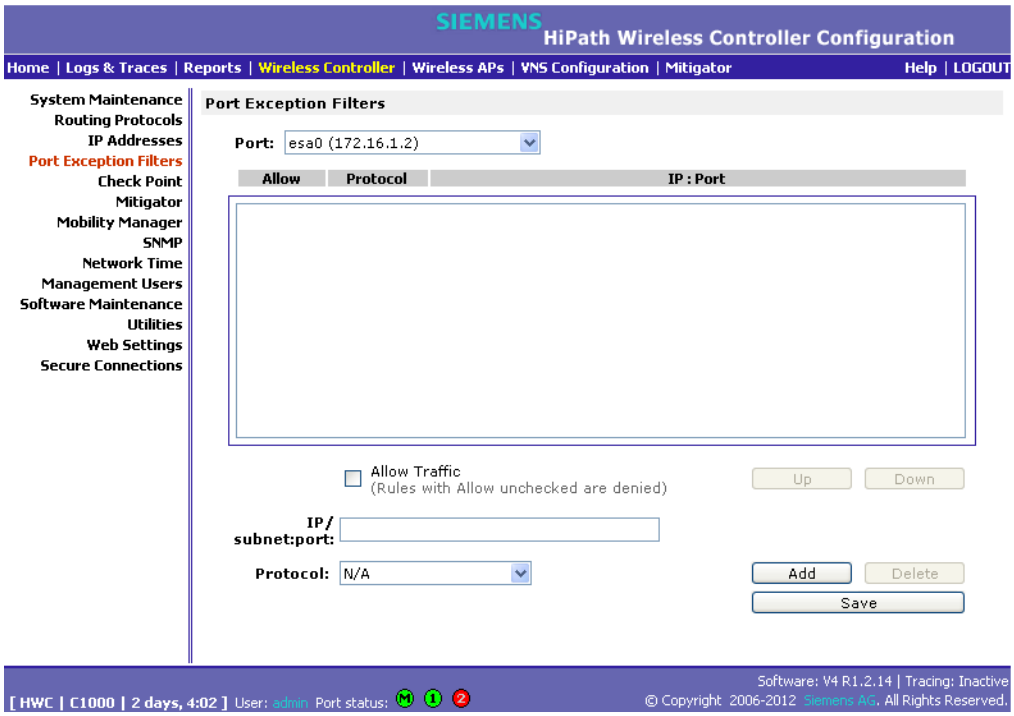
Le contrôleur C1000 possède deux interfaces (ports optique) esa0 et esa1 qui devront être coché pour permettre le flux de données en réception et émission, et saisir le plan d’adressage IP des ports Ethernet.

Mgmt : permet l’accès aux services de management via les interfaces (HTTPs:port-SSH-SNMP)

SLP : protocole utilisé par les points d’accès pour la découverte et l’enregistrement.

III.7.4. Port Exception Filters

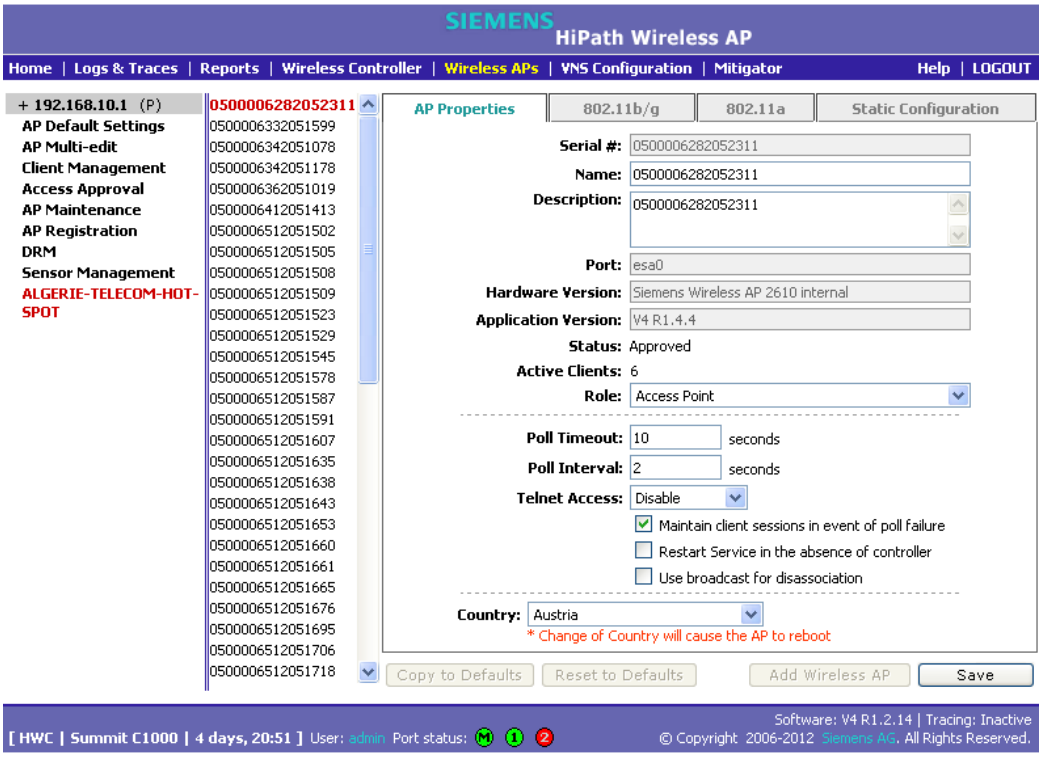
Ces filtres protègent le contrôleur d’accès du trafic non autorisé aux services et fonctions de gestion à travers les ports.



III.8. Configuration et Paramétrage des Points d'Accès

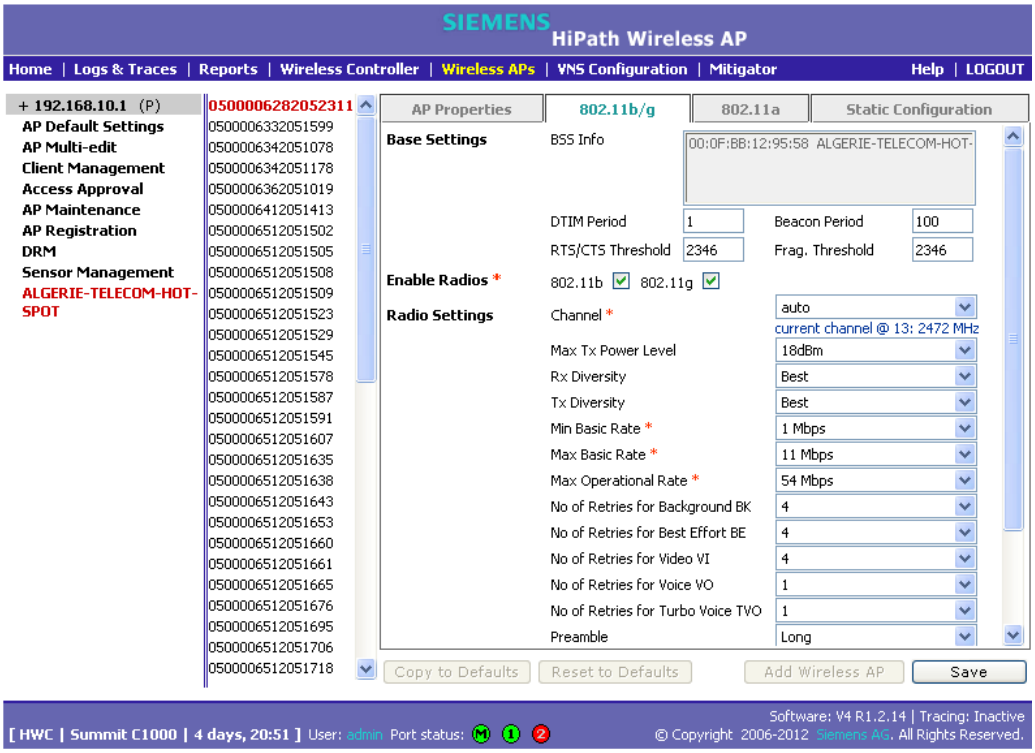
III.8.1. dentification et registration des points d'accès

Le point d'accès 2610/20 est démuni d'interface utilise le standard 802.11b/g/a est connecté en infrastructure au réseau local en établissant une connexion IP avec le contrôleur.



Toute communication avec ce dernier est effectuée grâce au protocole UDP, qui encapsule le trafic IP du point d'accès et le redirige vers le contrôleur C1000.

Une liste des adresses IP est mise en service par différents méthodes sont envoyées au point d'accès qui attend et recherche celles-ci, et lorsqu'il découvre ces adresses il envoi des requêtes simultanément à chacune d'elles et attendra pour s'enregistrer dés qu'il reçoit une première réponse. Lorsque la connexion et l'enregistrement sont établis avec le contrôleur en envoyant le numéro de série et recevant d'autre part un port d'adresse IP et une clé.



Le point d'accès sans fil Siemens a deux radios :

- 2.4 GHz supportant le standard 802.11b/g opérant respectivement à une transmission de 11/54 Mbps et ces deux normes peuvent coexister dans le même réseau sachant que la 802.11g utilise la même plage de fréquence.
- 5 GHz supportant le standard 802.11a opère à 54 Mbps utilisant la modulation OFDM, FHSS ou DSSS, cette radio ne sera pas configurée dans notre réseau WiFi car le point d'accès jouera le rôle de couverture et non pont (antenne).

III.8.2. Procédures d'identification

1- Utilisation d'une adresse IP de la dernière bonne connexion au contrôleur.

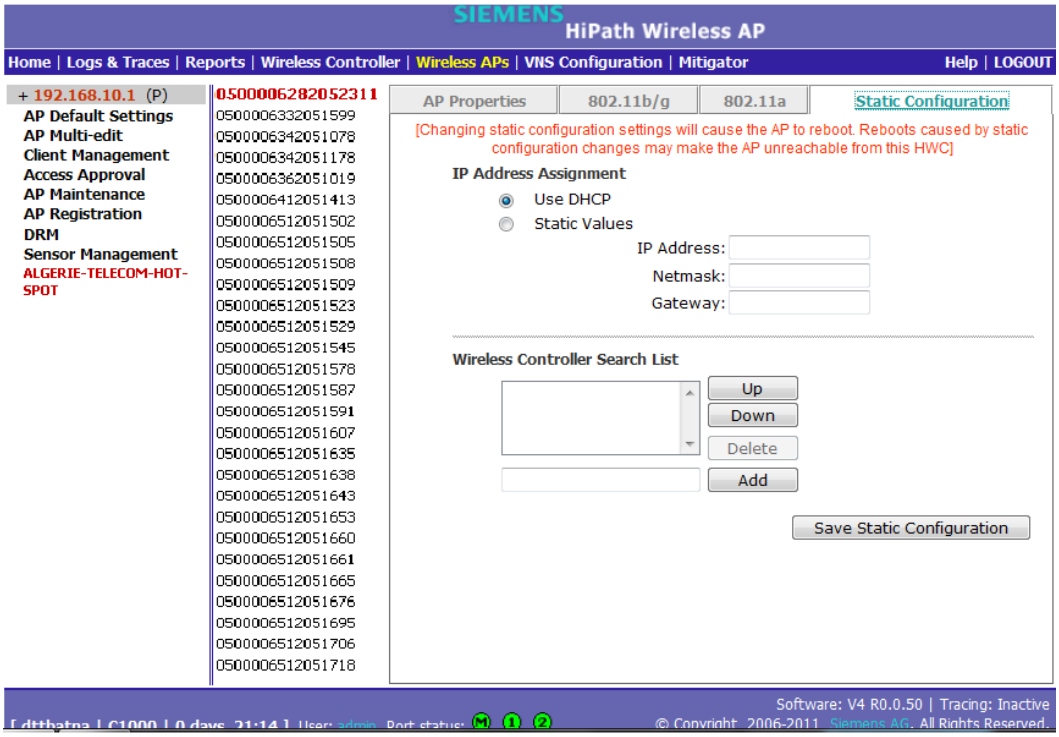
2- Utilisation des adresses IP statiques prédéfinis dans le réseau pour le contrôleur (Wireless Controller Search list).

3- Utilisation du protocole DHCP (Dynamic Host Configuration Protocol) pour l'attribution des adresses IP aux périphériques dans le réseau.

4- Utilisation du protocole SLP (Service Location Protocol).

5- Utilisation du DNS (Domain Name Server) à chercher le nom hôte du contrôleur.

6- Utilisation Multicast SLP requête pour trouver SLP Service Agent.

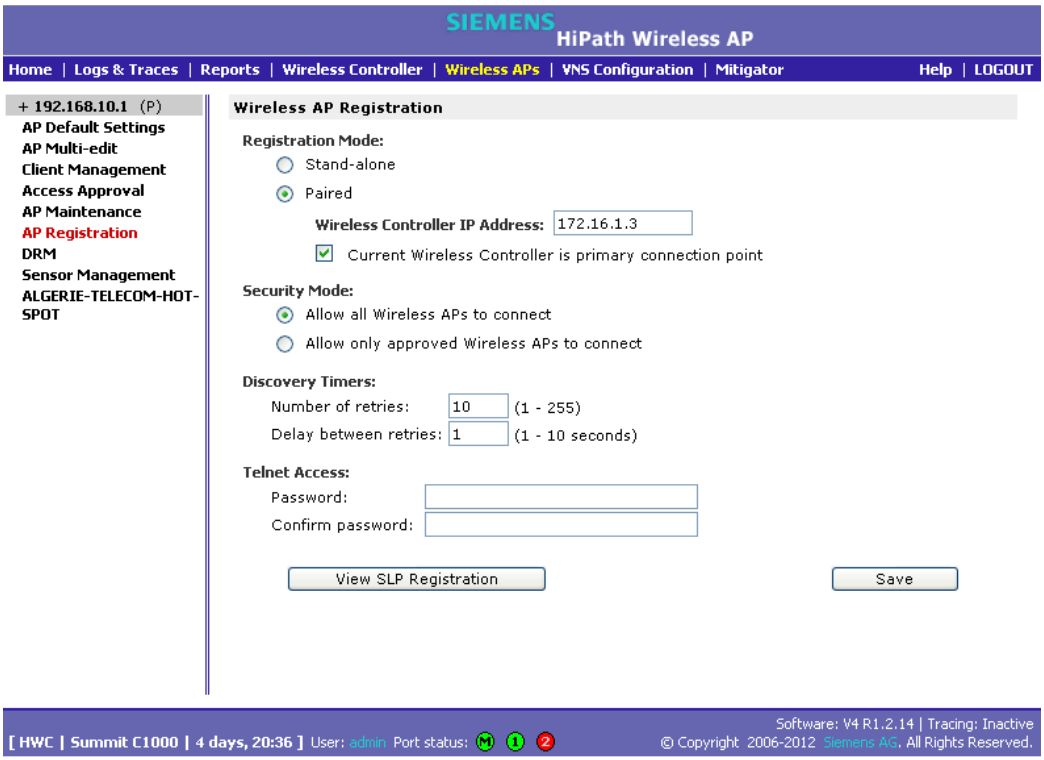


III.8.3. AP Registration

Dans ce mode, le contrôleur peut fonctionner seul en sélectionnant l'option « Stand-alone » pour le maximum des points d'accès (200), ou « paired » en continuité avec un second contrôleur avec spécification de l'adresse de management ou en redondance.

Deux propriétés à définir après la configuration du point d'accès sans fil :

- Security Mode.
- Discovery Timers.



Durant l'initialisation et l'enregistrement du maximum des points d'accès, il est recommandé de sélectionner l'option **Allow all Wireless APs to connect**

Une fois l'opération est complétée, il est suggéré en point de vue sécurité de basculer vers l'option **Allow only approved Wireless Aps to connect** afin de s'assurer aucun autre point d'accès non approuvé n'est autorisé à se connecter.

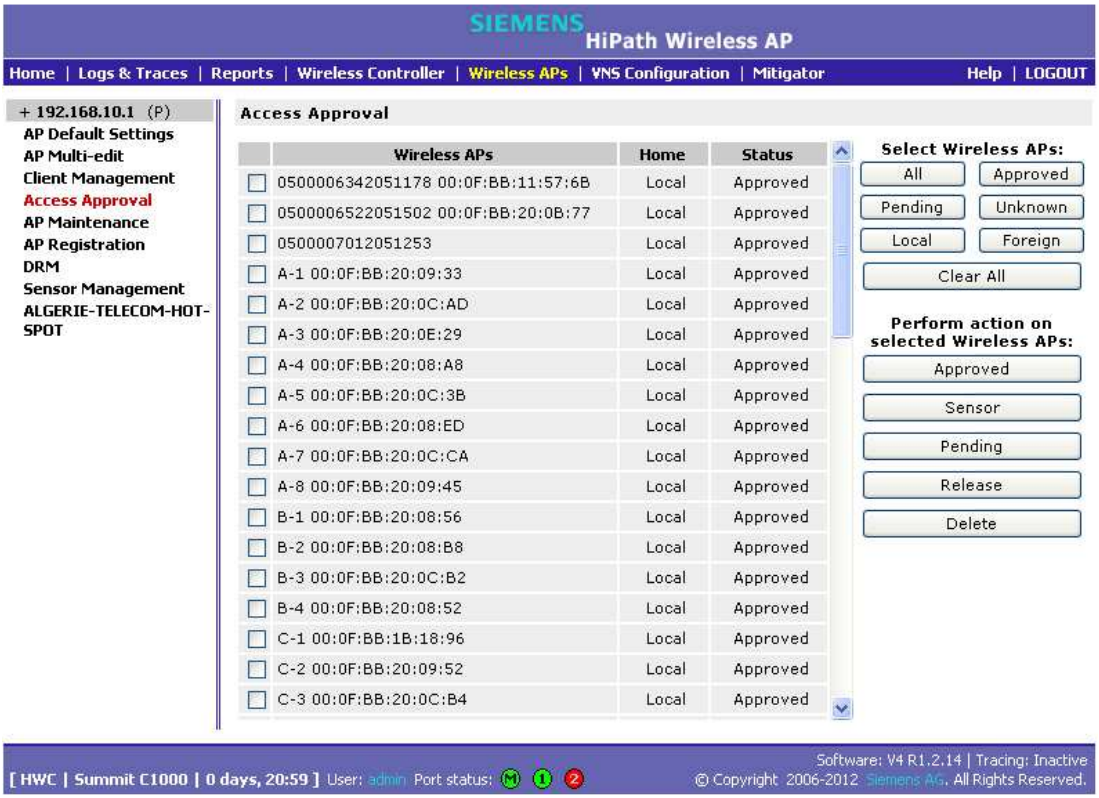
Pour définir les paramètres du processus de découverte, les valeurs en secondes sont tapées définissant le nombre de tentatives et l'intervalle de délai entre chaque test.

DRM : Offres de gestion dynamique de RF
Sélectionne automatiquement les canaux et ajuste la radiofréquence de propagation de signal (RF) et les niveaux de puissance sans intervention de l'utilisateur.

III.8.4. Access Approval

Une fois les AP sont identifiables et configurables en normes et en DRM dans la partie « Wireless APs » et pris leur adresses IP par le serveur DHCP même les APs en Pending, il

est plus judicieux pour la performance et la sécurité d'approuver ces périphériques réseau sans fil en « Approved » afin d'éviter une éventuelle intrusion ou ajout des rogues.



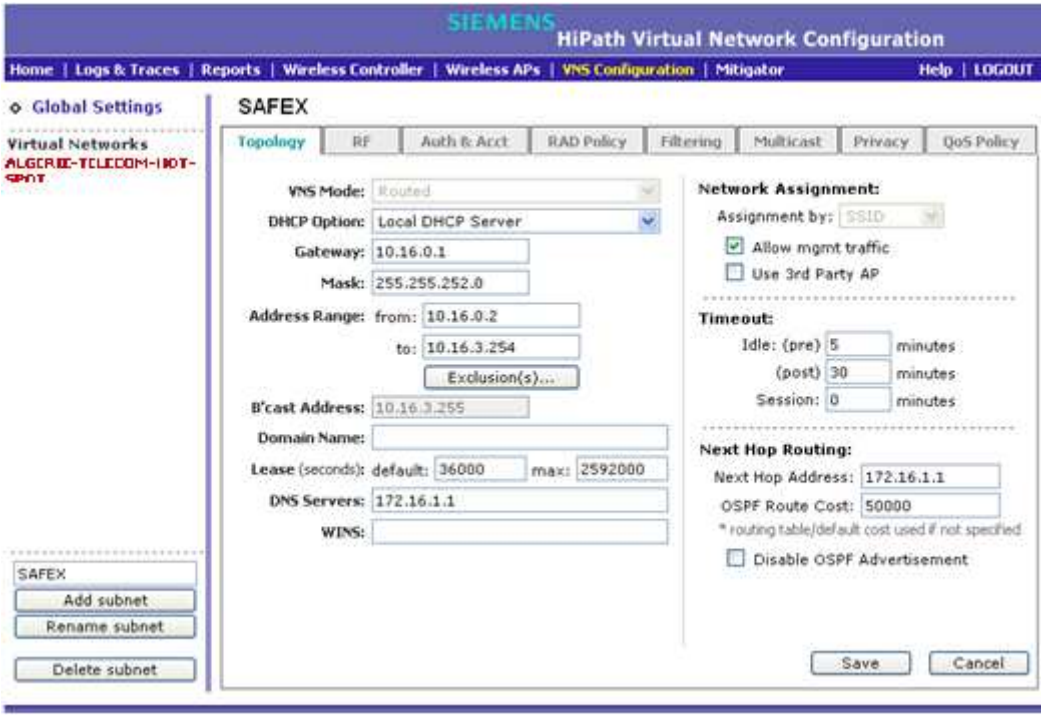
III.9. Configuration VNS

Le contrôleur C 1000 supporte 50 VNS

III.9.1. Configuration du DHCP

Après que le Wireless AP est enregistré et configuré, y est assigné au VNS (Virtual Network Segment) pour traiter le trafic sans fil.

D'abord, il faut créer un sous-réseau (subnet) sur le réseau avec un mode Routed où le trafic d'utilisateur est dirigé en tunnel vers le contrôleur.



Le DHCP des clients doit être DHCP Server (dans le cas contraire chaque périphérique réseau doit y avoir une adresse IP statique) avec un masque sous réseau dans une plage /254 - /248 - /240. Si on utilise le DHCP relay, cela forcera le contrôleur à transmettre avant les requêtes à un DHCP externe dans le réseau d'entreprise qui manage les adresses IP.

Next-hop routing : dans le but de spécifier une unique gateway ou le trafic en VNS est transporté. Définir le « Next hop routing » pour le VNS force tout le trafic dans le VNS à être transporté vers le réseau indiqué par l'adresse IP par passage de toutes les configurations de routage définies dans la table de routage.

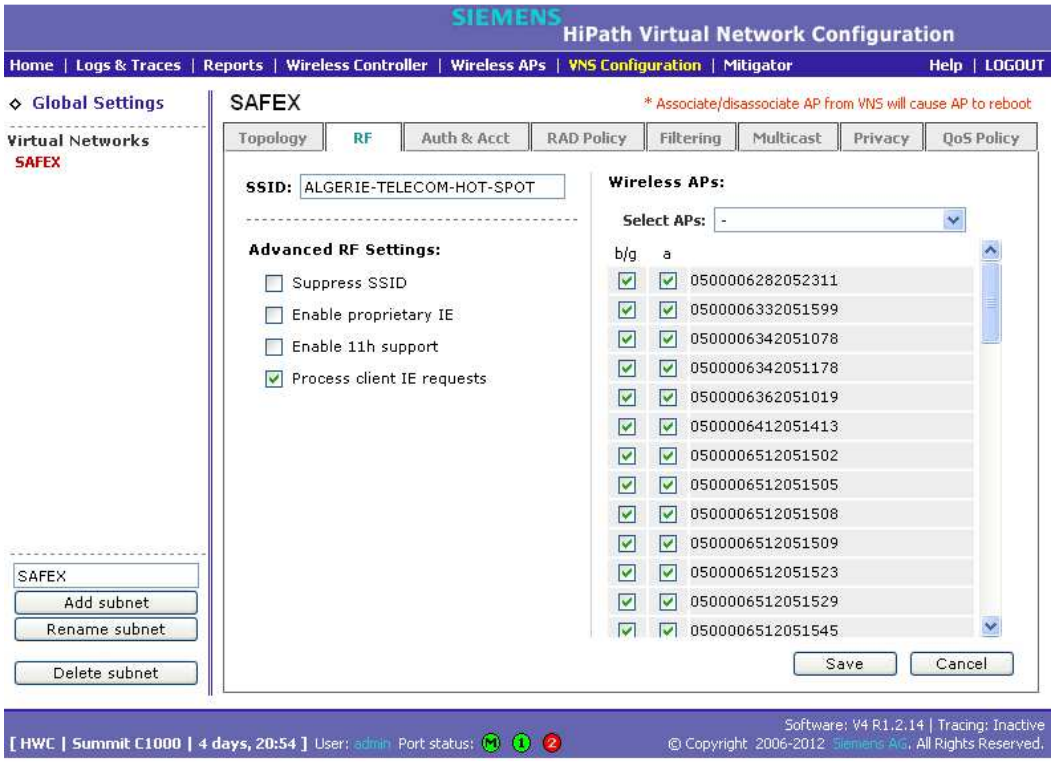
Network Assignement : la sélection de SSID dans cette topologie a pour conséquence le déploiement du contrôleur et les points d'accès sans le serveur Radius, c.à.d. sans authentification des utilisateurs dans le réseau.

Auth & Acct : dans cet onglet, sélectionné **No Captive Portal** radio signifiera qu' il n'y aura pas d'authentification des utilisateurs mais le contrôleur et les points d'accès sont opérationnels.

Remarque : si le VNS mode est sur « Bridged at the AP VNS » le trafic d'utilisateur est directement lié par pont au VLAN vers le point d'accès sur le réseau pour accès via le port Switch.

III.9.2. Affectation AP au VNS (SSID)

Dans la variable RF, tous les points d'accès seront paramétrés sur la radio b/g (et non en même temps afin d'éviter l'atténuation du signal) en couverture et affectés au SSID prédéfini pour la connexion et accès des AP sur le réseau.



Le RF décri où vous attribuez les AP à VNS.

Il est recommandé de cocher les paramètres avancés suivantes :

1- Suppress SSID : prévoit l'apparence de SSID dans le message envoyé par AP.
2- Enable proprietary IE : active les rapports du canal radio à envoyer à l'AP.
3- Enable 11h support : active les rapports sur le TPC (transmission power control)
4- Process client IE requests : active AP à accepter les requêtes IE envoyés par le client via Probe Request frames et répondre en incluant les requêtes IE dans la correspondance Probe Response frames.

III.10. Plate Forme

La plate forme du réseau WLAN de l'opérateur d'Algérie Telecom se constitue des parties intégrales suivantes :

1- Serveur à base de système Linux version RedHat Server entreprise 5.
2- Application Garderos de Siemens (DNS-RADIUS).
3- Serveur DHCP.
4- MPAG.
5- Contrôleur C1000 Siemens.
6- Firewall (NAT).

Le HiPath Wireless Controller est une application de l'équipementier Siemens intégrée comme système d'exploitation (OS : AC-HR-4_0_14.tar) dans le contrôleur qui fournit une authentification en utilisant :

1- Captif portal : mécanisme basé sur un navigateur qui force les utilisateurs vers une page Web sécurisée.
2- RADIUS (IEEE 802.1x).

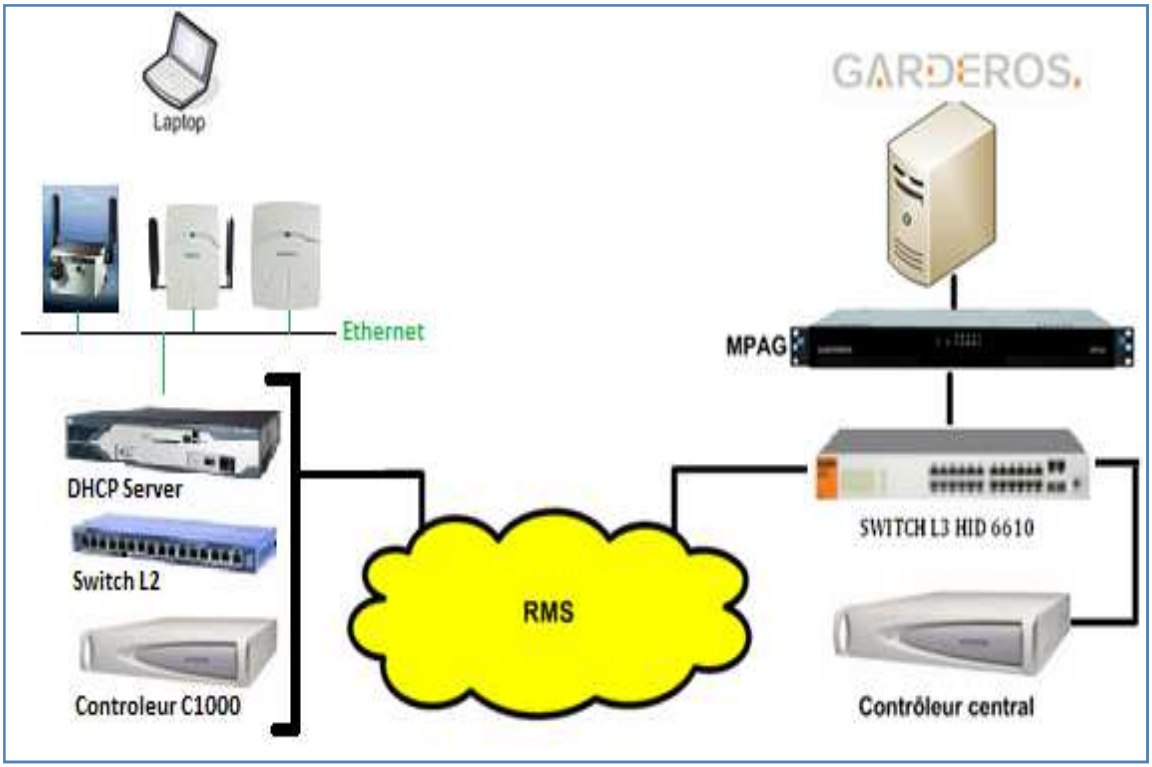


Figure.III.30 : Architecture simplifiée de la plate forme

III.11. Configuration sur MPAG

Le Garderos MPAG (Multi Protocol Access Gateway) est un produit, désigné comme un routeur de périphérie à commande distant configurable à faible cout d'arrêt, aussi un contrôleur d'accès pour les réseaux de pointe ou des réseaux hotspots publics.

Figure.III.31 : MPAG.

Fondamentalement le Garderos MPAG (BRAS) est un routeur avec interfaces réseau à deux ports Ethernet 10/100/1000BT.

1-> WAN, interface Internet (10/100/1000BT), l'interface IP peut être configurée en statique IP address ou en DHCP ou PPPoE. Le routeur définit automatiquement la route par défaut via cette interface.

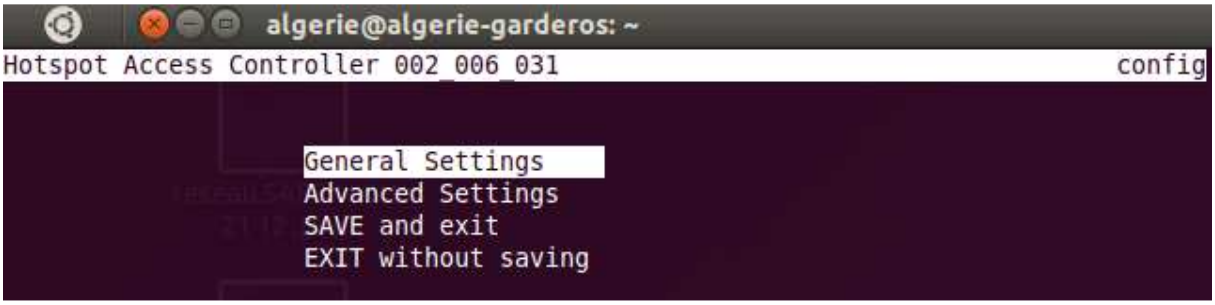
2-> Access Network, interface client (10/100/1000 BT) qui offre un accès payant à Internet pour les clients. Les soi-disant « zones » sont configurées sur cette interface. Chacune de ces zones représente une zone d'accès de l'endroit où les utilisateurs peuvent accéder à Internet. Si plus d'une zone est configuré sur l'interface, le marquage VLAN est nécessaire pour séparer les zones d'accès.

La connexion à MPAG pour une éventuelle configuration est possible via :

- l'interface WAN par un cordon RJ45 direct à l'aide d'un navigateur Web
- Le port série DB9 par un câble console à l'aide de SSH Secure (Putty)

En utilisant le câble console raccordé au PC et à l'aide de l'utilitaire SSH, en spécifiera l'adresse de management par défaut (10.0.0.1) et le nom d'utilisateur (root) en tapant le mot de passe une fois confirmé la liaison.

#config



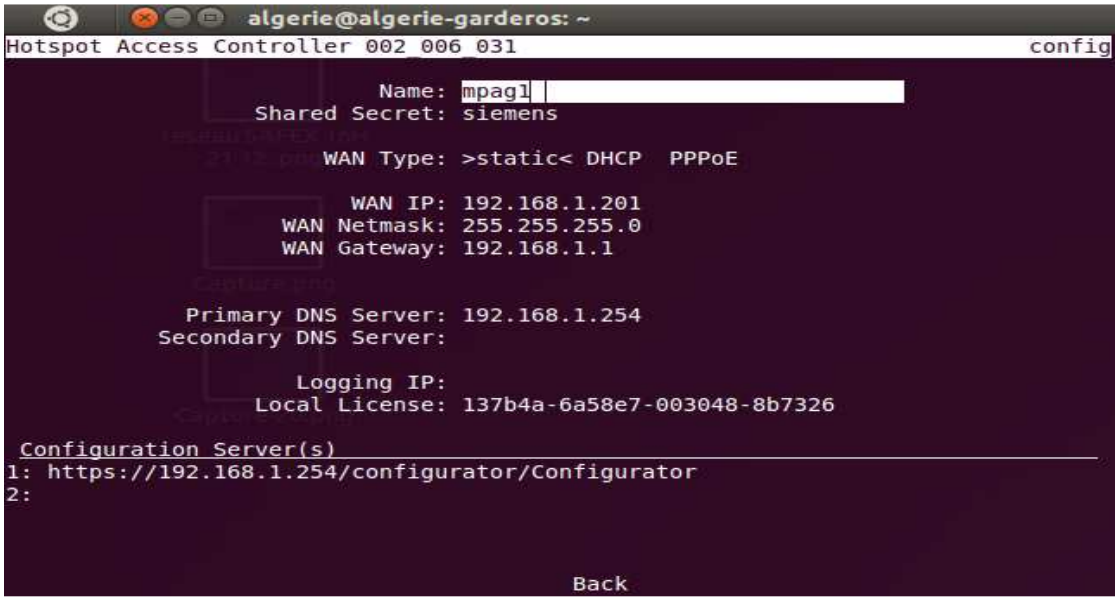
Le MPAG Garderos fournit uniquement les fonctionnalités dont on a réellement besoin dans la zone d'accès local.

Toutes les fonctions qui sont plus faciles à gérer à partir d'un emplacement central sont attendus sur un système de back-end, Garderos C-OSS, qui a déjà mis en œuvre toutes les interfaces MPAG.

Généralement les fonctions dans le backend inclus:

- Configuration management.
- Portal page server.

III.11.1. Interface MPAG



Une méthode de base pour la désignation et la définition des MPAG est comme suite :

- Les noms des MPAG sont crées de la façon alphanumérique : mpag1, mpag2,…
- Les adresses de management des MPAG sont choisi de la façon où x représente le MPAG correspondant : 192.168.1.201, 192.168.1.201,…, 192.168.1.X.
- Chaque MPAG est lui affiliée une adresse IP de la classe C à chaque zone ou x représente le nom de celle-ci : 10.X.0.1.

III.11.2. Débogage réseau

Pour analyser ces erreurs, le MPAG fournit des outils de débogage réseau parmi :

- Ifconfig : montre la configuration du réseau de l'MPAG et connaitre ces paramètres devrait montrer au moins les interfaces lo, eth0 et eth1.
- Ping : utilisé pour tester l'accessibilité à une autre machine.
- Traceroute : Pour savoir où un ping est échoué, et nous dire si le saut est disponible.
- Tcpdump : utilisée pour afficher la communication sur les interfaces MPAG.
- Ip tunnel : montre la configuration des tunnels GRE configurés sur le MPAG.
- Ip route : affiche les règles actuelles de routage sur le MPAG.

Utilitaire ac : L'outil fournit plusieurs fonctions utiles pour tester le MPAG

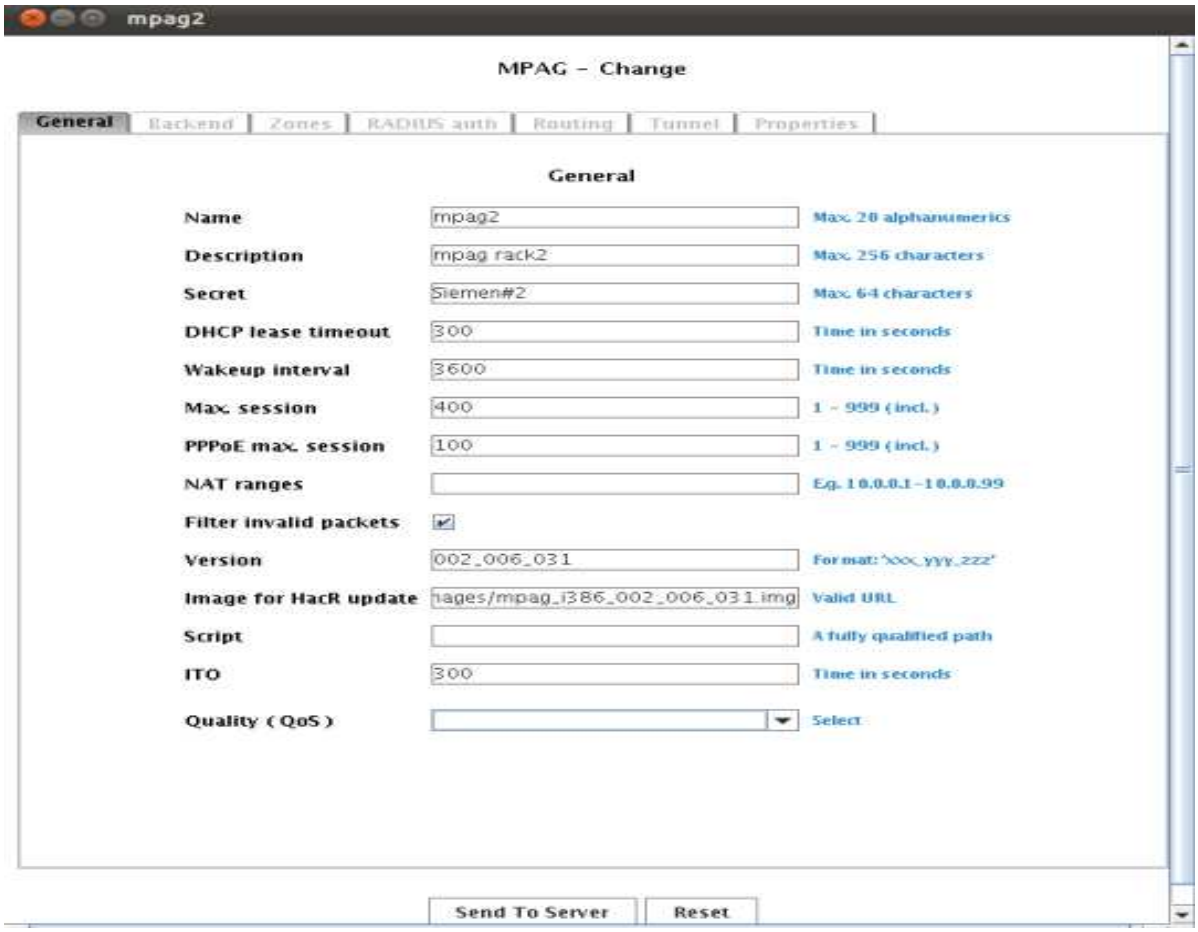
- Show wan.
- Show users.
- Login/logout users.
- Reconfigure.
- Acsatd.
- Reboot.

III.12. Configuration sur GARDEROS

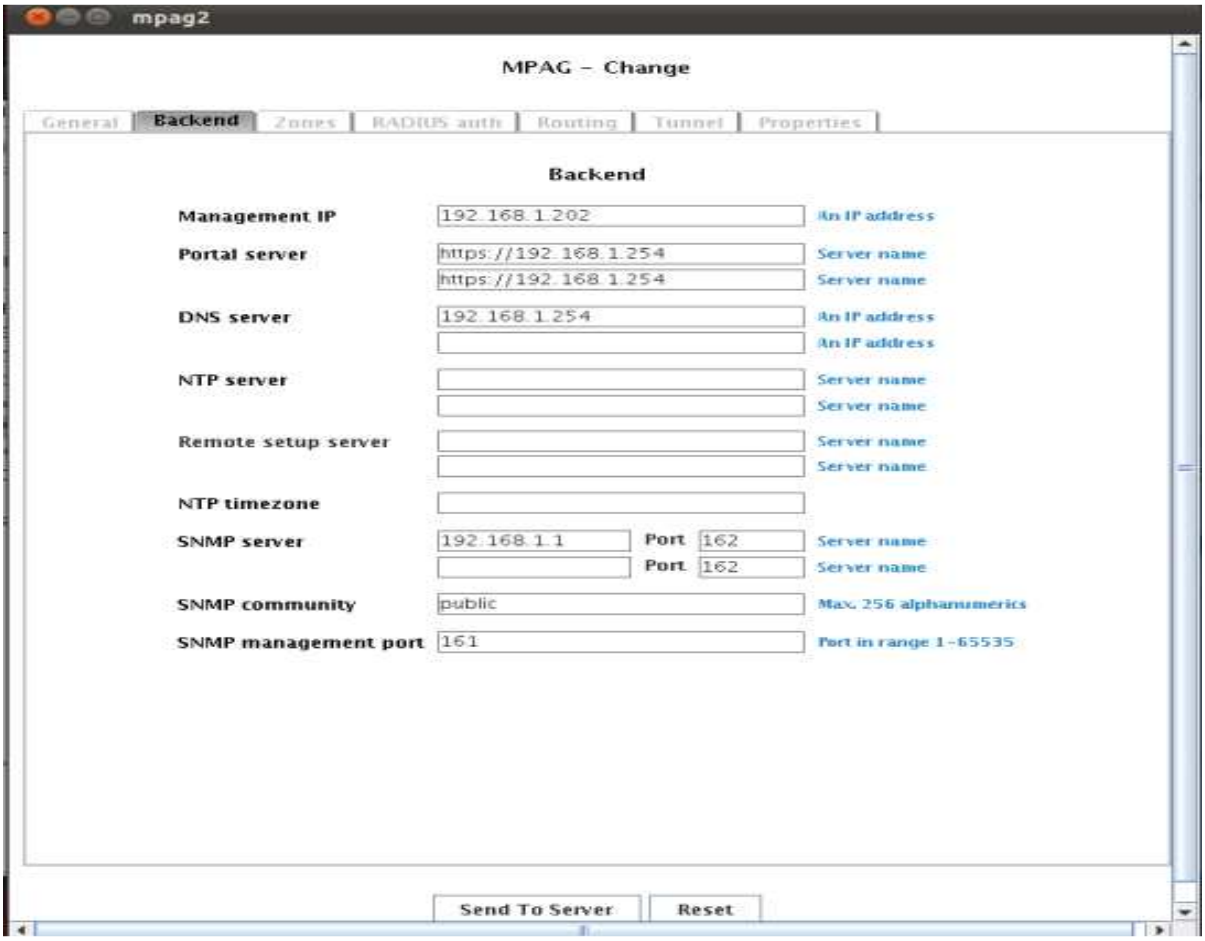
Dans le but d'assurer la bonne configuration et la mise en service du réseau Wifi déployé dans le campus, certains aspects techniques et étapes de configurations doivent être respectées dans la norme d'une administration afin de permettre le service de connexion Internet et établissement d'une liaison de bout en bout réalisé en transmissions via un lien en fibre optique de dix Méga.

Le Garderos C-OSS fournit une interface graphique d'administration, ce qui permet de créer des fichiers de configuration pour la MPAG dynamiquement, la configuration est stocké dans la base de données de Garderos.

La capacité de Garderos pour gérer les accès utilisateurs en administration et authentification est de 65.000, et de 10.000 accès simultanés pour les MPAG (ce qui limite les MPAG et les zones en 10).



Le C-Garderos OSS est utilisé comme un système Back-end pour le MPAG

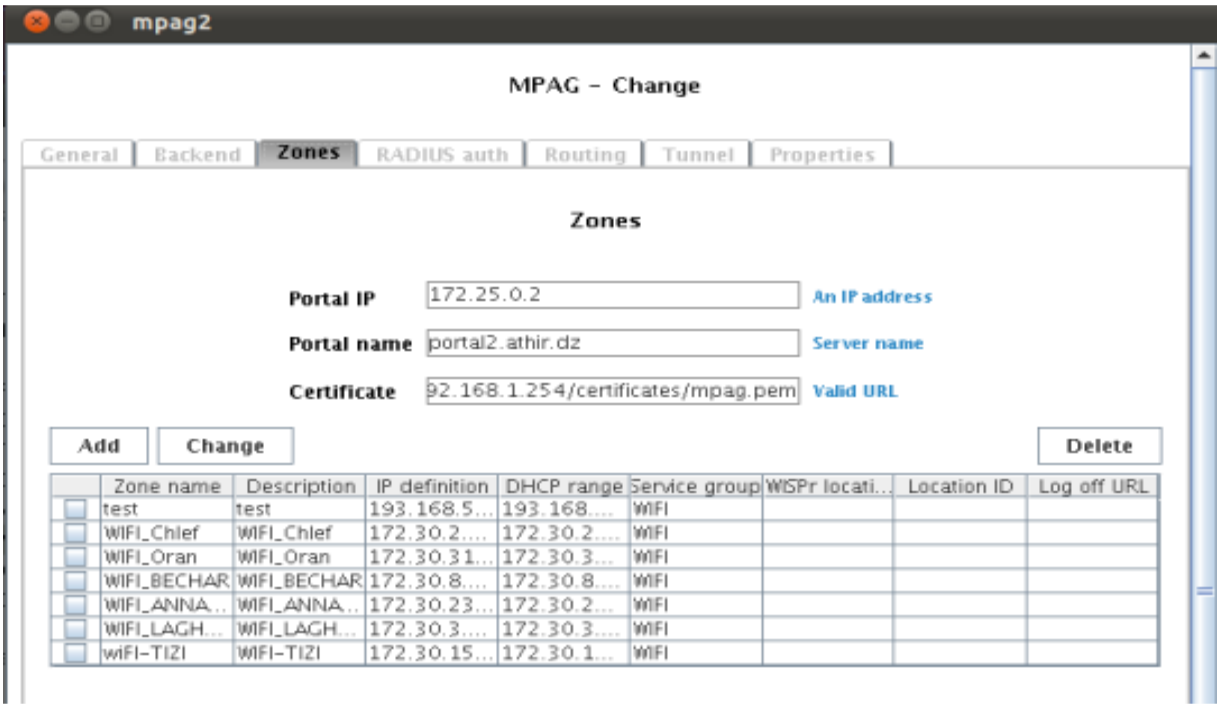


Généralement les fonctions dans le backend inclus:

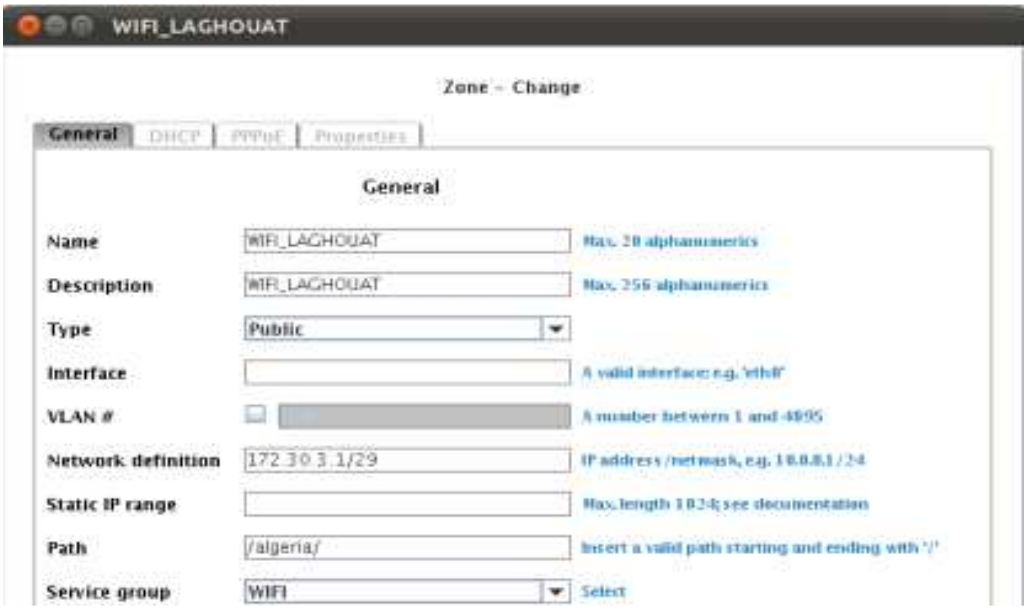
- Configuration management
- Portal page server
- Authentication server
- User database
- Service management
- Billing

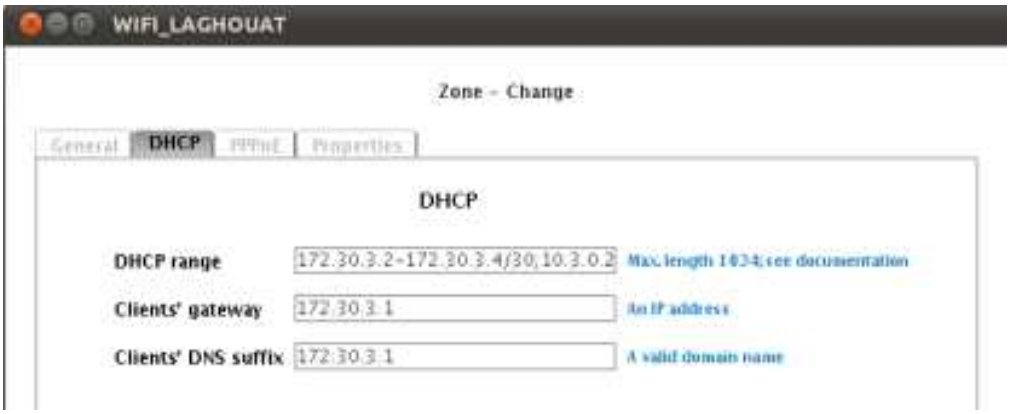
III.12.1. Les zones

Cette page définit le portal des zones enregistrées et informe les utilisateurs courant dans quelles zones se retrouvent avec attribution et allocution des adresses IP pour chaque zone et leur DHCP plages correspondantes.



III.12.2. Définition des zones





III.13. Partie Radius

Le client RADIUS du MPAG est utilisé pour authentifier et envoyer des données comptables à un serveur RADIUS Back-end qui doit appeler le chemin (/ admin) sur le MPAG pour vous connecter ou déconnecter un utilisateur.

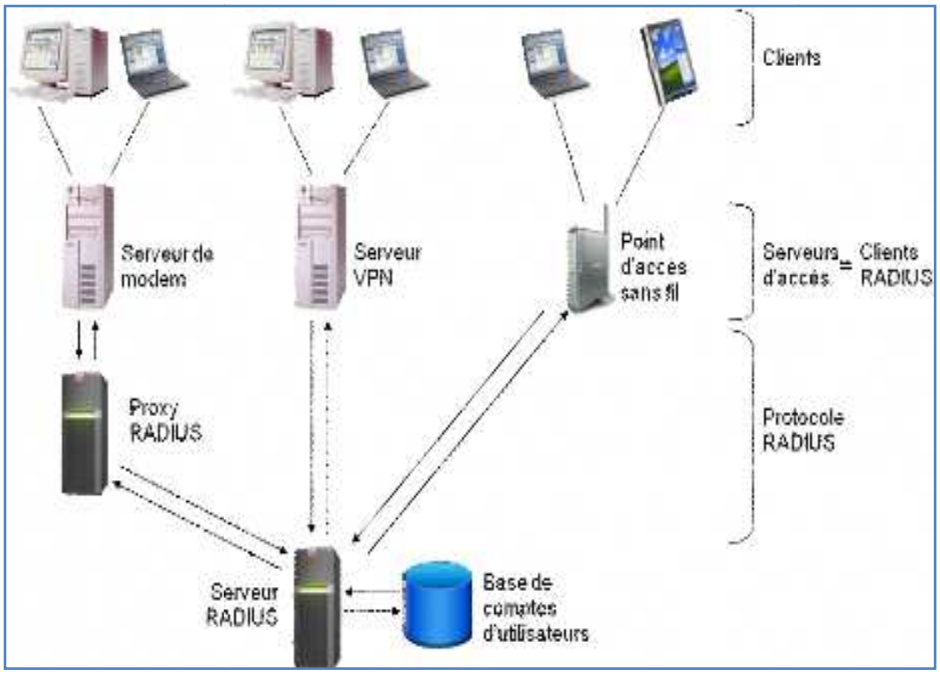


Figure.III.32 : Authentification Radius.

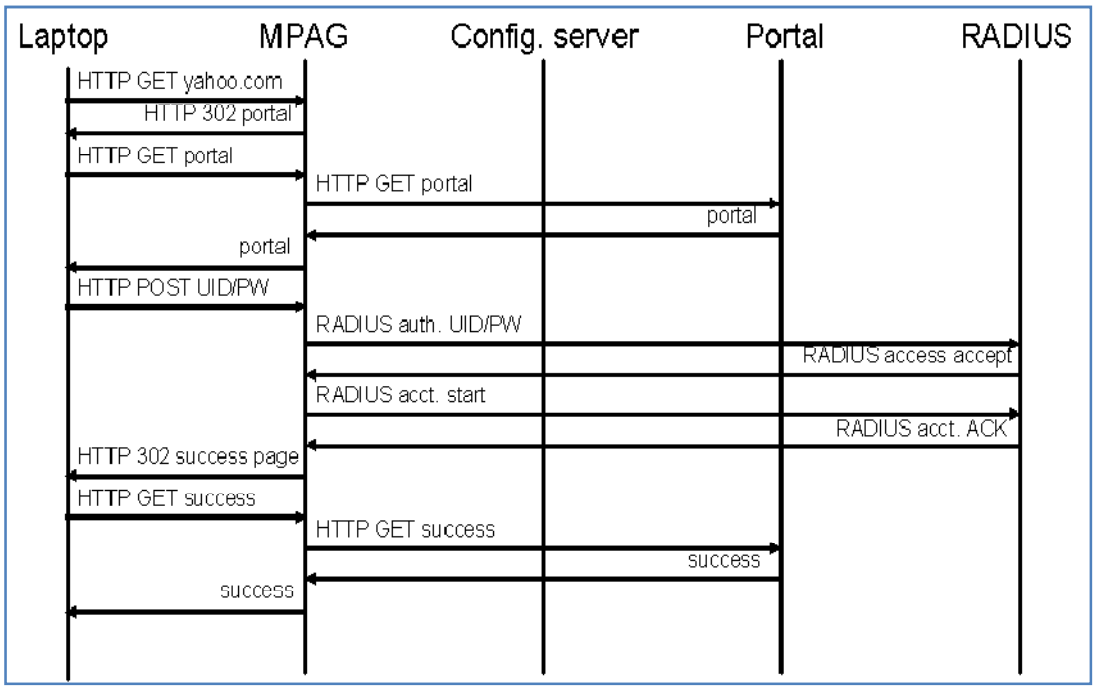


Figure.III.33 : Processus d'Authentification et Autorisation.

La procédure de connexion est comme suite :

a. L'utilisateur tente d'atteindre n'importe quelle page sur Internet. La requête HTTP est redirigée vers l'intérieur Serveur proxy MPAG (le port 80, puis le port 4444).

b. Le serveur proxy MPAG redirige l'utilisateur (code d'erreur HTTP 302) vers le port sécurisé 443 sur sa propre adresse IP portail. C'est sa propre adresse IP interne, où il produit des pages Web.

c. Lorsque l'utilisateur appuie sur le portail IP de MPAG, le serveur proxy MPAG reconnaît qu'il doit répondre à la demande avec une page tirée d'un serveur principal Back-end.

d. Le proxy ajoute des paramètres de l'entête HTTP à la requête HTTP et l'envoie au Back-end serveur du portail principal.

e. Le serveur de portail Back-end examine les paramètres d'en-tête HTTP, découvre que l'utilisateur n'est pas encore connecté (paramètre d'en-tête X-AC-User Logged-In: no) et crée le cas échéant la page de connexion. La page du portail est renvoyée au serveur proxy de la MPAG.

f. Le serveur proxy MPAG reçoit la page de connexion et la livre ou fournit au terminal de l'utilisateur.

g. L'utilisateur entre son nom d'utilisateur et mot de passe et appuie sur le bouton de connexion. La connexion est envoyée sur le serveur proxy de l'MPAG.

h. Le MPAG serveur proxy achemine la demande au serveur web Back-end, qui extrait le nom d'utilisateur et mot de passe à partir de la demande de connexion. Il va maintenant authentifier l'utilisateur.

i. Si l'utilisateur a été correctement authentifié (en utilisant RADIUS), le serveur Web envoie une requête HTTP vers le chemin / admin / login.cgi sur le MPAG.

j. Le MPAG détecte que la demande doit déclencher une connexion de l'utilisateur. Il va extraire le nom d'utilisateur et mot de passe à partir de la demande de connexion et va déclencher une demande d'authentification RADIUS pour un serveur RADIUS.

k. Si le serveur RADIUS envoie un accès accepter le message, l'utilisateur sera connecté à MPAG.

l. Le MPAG répond à la requête HTTP du serveur Back-end avec un message de réussite.

m. Le serveur principal Back-end envoie une redirection vers une page de succès comme une réponse à la requête HTTP provenant du serveur proxy MPAG

n. Le serveur proxy MPAG envoie en http une redirection de message à l'utilisateur, qui pointe vers le la page de connexion de succès comme une réponse à la demande de l'utilisateur http.

o. Le terminal de l'utilisateur envoie une requête HTTP à la page prévue dans la redirection HTTP, avec généralement aller au serveur proxy de l'MPAG à nouveau.

p. Le serveur proxy va chercher la page sur le serveur web Back-end avec la même, en ajoutant cette fois paramètres de l'entête à la requête HTTP demandant au serveur Web que l'utilisateur Back--end est déjà connecté.

q. Le serveur proxy envoie la page de connexion réussie vers le dispositif de l'utilisateur.

III.14. Script Switch L3

```
<Switch_Controleur_ORAN>dis cur
!Software Version V100R005C01SPC100
sysname Switch_Controleur_ORAN
vlan batch 131
cluster enable
ntdp enable
ntdp hop 16
ndp enable
dhcp enable
undo http server enable
drop illegal-mac alarm
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default
domain default_admin
local-user admin password simple admin
local-user admin service-type http
interface Vlanif1
ip address 192.168.31.3 255.255.255.0
dhcp select interface
dhcp server option 78 ip-address 192.168.31.1
interface MEth0/0/1
interface GigabitEthernet0/0/1
port link-type access
port default vlan 131
ntdp enable
```

```
        ndp enable
        bpdu enable
        undo negotiation auto
        speed 100
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 131
 ntdp enable
 ndp enable
 bpdu enable
        interface GigabitEthernet0/0/3
         ntdp enable
         ndp enable
         bpdu enable
interface GigabitEthernet0/0/4
 ntdp enable
 ndp enable
 bpdu enable
        interface GigabitEthernet0/0/5
         ntdp enable
         ndp enable
         bpdu enable
interface GigabitEthernet0/0/6
 ntdp enable
 ndp enable
 bpdu enable
        interface GigabitEthernet0/0/7
         ntdp enable
         ndp enable
```

```
 bpdu enable
interface GigabitEthernet0/0/8
 ntdp enable
 ndp enable
 bpdu enable
 interface GigabitEthernet0/0/9
 ntdp enable
 ndp enable
 bpdu enable
interface GigabitEthernet0/0/10
 ntdp enable
 ndp enable
 bpdu enable
 interface GigabitEthernet0/0/11
 ntdp enable
 ndp enable
 bpdu enable
interface GigabitEthernet0/0/12
 ntdp enable
 ndp enable
 bpdu enable
 interface GigabitEthernet0/0/13
 ntdp enable
 ndp enable
 bpdu enable
interface GigabitEthernet0/0/14
 ntdp enable
 ndp enable
 bpdu enable
```

```
interface GigabitEthernet0/0/15
 ntdp enable
 ndp enable
 bpdu enable
interface GigabitEthernet0/0/16
 ntdp enable
 ndp enable
 bpdu enable
interface GigabitEthernet0/0/17
 ntdp enable
 ndp enable
 bpdu enable
interface GigabitEthernet0/0/18
 ntdp enable
 ndp enable
 bpdu enable
interface GigabitEthernet0/0/19
 ntdp enable
 ndp enable
 bpdu enable
interface GigabitEthernet0/0/20
 ntdp enable
 ndp enable
 bpdu enable
interface GigabitEthernet0/0/21
 ntdp enable
 ndp enable
 bpdu enable
 port media type fiber
```

```
 undo negotiation auto
 combo-port auto
interface GigabitEthernet0/0/22
 port link-type access
 port default vlan 131
 ntdp enable
 ndp enable
 bpdu enable
 port media type fiber
 undo negotiation auto
 combo-port auto
 interface GigabitEthernet0/0/23
 ntdp enable
 ndp enable
 bpdu enable
interface GigabitEthernet0/0/24
 ntdp enable
 ndp enable
 bpdu enable
 interface NULL0
 snmp-agent
 snmp-agent local-engineid 000007DB7F0000010000601E
 snmp-agent sys-info version v3
 user-interface con 0
 idle-timeout 0 0
 user-interface vty 0 4
 user privilege level 15
 set authentication password cipher F@&U-=E^:@#Q=^Q`MAF4<1!!
return
```

III.15. Partie Sécurité

III.15.1. Réseau et Sécurité

1. VLAN 802.1Q.
2. VLAN 802.1Q.
3. Serveur DHCP.
4. NAT.
5. Client IPSEC intégré (interconnexion de sites).
6. Bridging d'interfaces.
7. Firewall intégré (state full inspection).
8. VPN Pass-through.
9. Secure Socket compliant (SSL) b.
10. Load balancing sur plusieurs liens WAN.
11. Répartition de charge entre plusieurs LMB.
12. Proxy transparent (http, https,…).
13. Détection d'attaques et contres mesures.

III.15.2. Authentification et Comptabilité

1. Authentification via support HTTPS/SSL.
2. Authentification 802.1x (EAP TLS, TTLS, PEAP).
3. Authentification par adresse MAC.
4. Autorisations en fonction du profil d'utilisateur.
5. Interface vers bases LDAP et Active Directory.
6. Interface vers bases RADIUS.

III.16. Partie Portail Captif WEB

III.16.1. Portail captif personnalisable et contrôle d'accès

L'Appliance se positionne entre le réseau d'accès de l'utilisateur nomade et l'accès Internet de l'operateur. La solution Radius avec le contrôleur oblige le visiteur à s'authentifier via une interface web personnalisable selon la charte graphique de l'entreprise et sa politique d'accès Internet.

L'accès à Internet est paramétrable en fonction du profil de l'utilisateur et de sa localisation il est alors possible de restreindre l'accès pendant un certain temps, à certaines heures, à certaines applications et avec une bande passante limitée. Il peut définir des ressources (tel qu'un serveur financier, un routeur ou un sous réseau d'adresses IP), des services (tels que http, FTP, POP3) et contrôler leur accès suivant les utilisateurs.

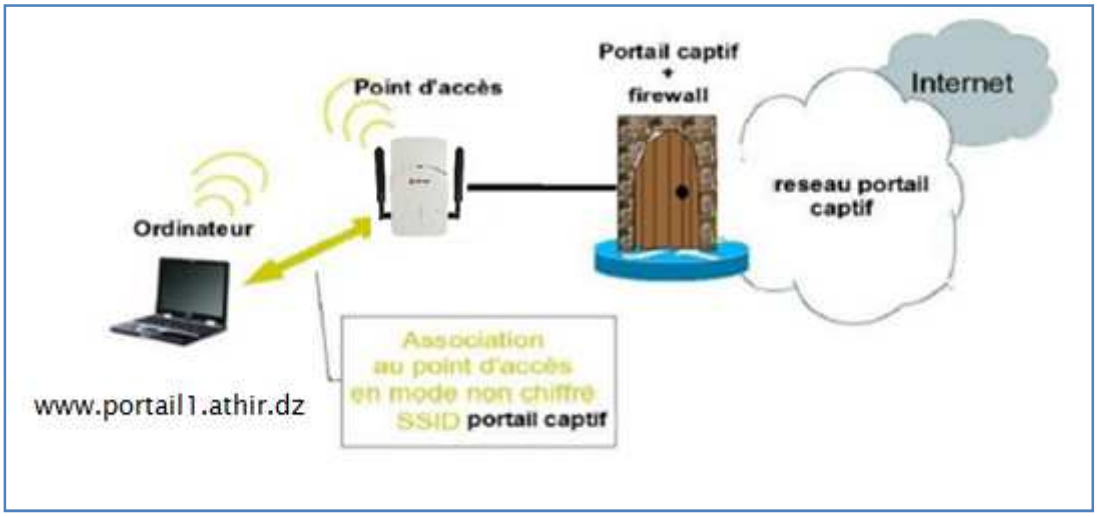


Figure.III.34 : Portail captif WEB.

L'utilisateur s'authentifie via une page Web dédiée de l'opérateur d'Algérie Telecom sécurisée par le SSID open en tapant son identifiant et son mot de passe.

III.17. Création des Comptes

III.17.1. Gestion des comptes

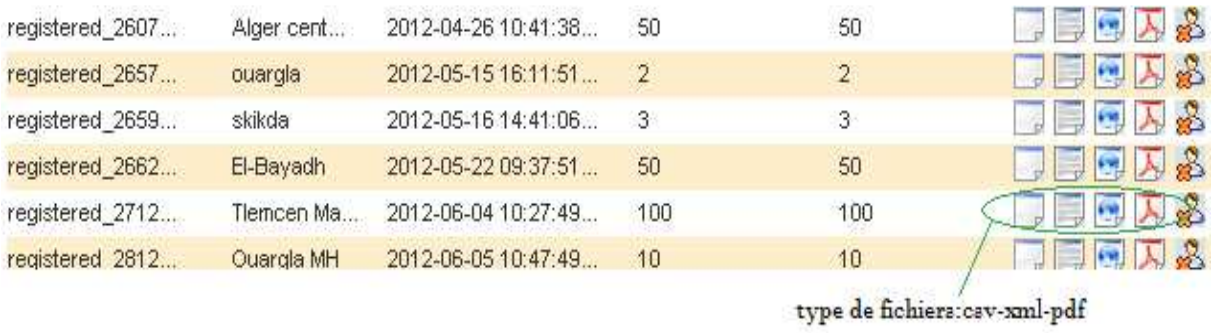
Pour répondre aux politiques de connexion les plus diverses, et permettre une gestion des comptes la plus appropriée, une grande variété de mécanismes nécessitera d'être disponible sur les solutions proposées au travers d'une interface Web sécurisée : création de comptes par lots, création et impression de compte a la volée, autocréation de compte par l'utilisateur, envoi de SMS et/ou email, importation via fichier csv, et même création par des applications externes via l'API WEB Services.

D'autre part, tout ou partie de la gestion des comptes peuvent être déléguée à un personnel non technique sans installation de logiciel sur le poste de l'accueil. L'interface de création de comptes est entièrement personnalisable par l'administrateur.

III.17.2. Création des comptes

La création des comptes pour accès Internet aux utilisateurs se fera de deux manières différentes par le système OSS-GARDEROS à savoir par ajout manuel un par un, ou par la technique Voucher automatiquement.

Les fichiers crées par la technique voucher sont définis aprioris selon la classe (connexion limitée par les horaires, dates ou open) et les identifiants et les mots de passe sont indiqués par leurs tailles de caractères. Les fichiers sont générés en pdf, csv ou xml.



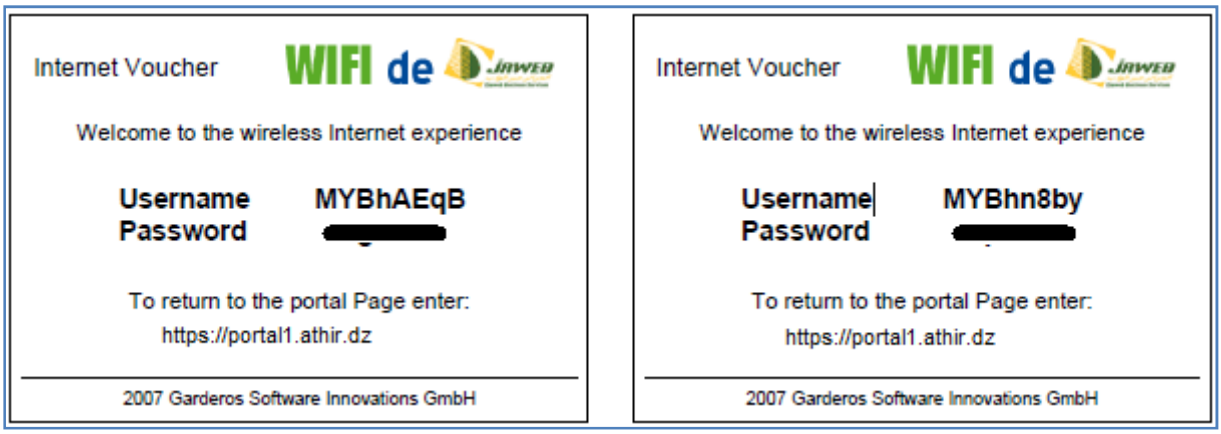
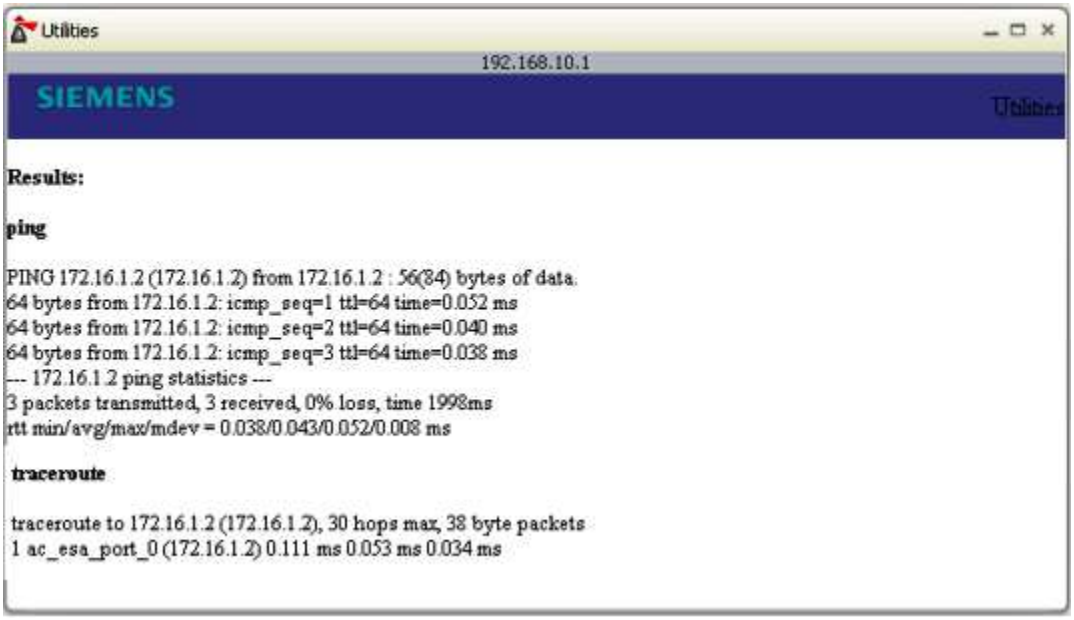


Figure.III.35 : Modèle de carte d'accès au réseau.

III.18. Test – Repporting – Supervision

III.18.1. Test de mise en service

Une fois la configuration est finalisée sur tous les équipements de la plate forme, sachant le contrôleur C1000, le MPAG et le serveur Garderos, on procède aux tests de la mise en service du réseau Wifi déployé par les utilitaires ping et trace route afin de vérifier la continuité et la traçabilité des trames.



III.18.2. Outil de test (1)

Le test de débit ou bande passante pourra aussi se faire par les outils gratuits se trouvant sur Internet permettant la mesure de haut gain comme le speedtest.net qui donnera des résultats voisinant et approximatifs.

III.18.3. Outil de test (2) :

Un autre outil de test très fiable physique réalisé par l'appareil de mesure JDSU 3000 pour la mesure de débit de bout en bout sur un port RJ45 génère un rapport illustré comme suite :

```
****************************************
** Test Instrument: HST-3000 ACE II    **
** Serial Number: ac871b010000          **
** Software Revision: 7.30.12           **
** Eth10/100/1G Electrique  Terme       **
** Couche 2 Trafic                      **
****************************************
[Sommaire Port 1 Results]
   ALL SUMMARY RESULTS OK

[Statistiques Port 1 Results]
% d'utilisation Total, Courant     34.003
% d'utilisation Total, Min          0.000
% d'utilisation Total, Moy         32.518
% d'utilisation Total, Pic         34.071
Débit Trame, Courant                 7990
Débit Trame, Min                        0
Débit Trame, moy                     7654
Débit Trame, Pic                     8005
Taille de trame, Min                   64
Taille de trame, Moy                  512
Taille de trame, Max                  594
Mbps Act en C1 en Rx                34.00
Mbps Act en C2 en Rx                32.72
Mbps Tx, Act C1                     34.00
Mbps Tx, Act C2                     32.72
Délais Min (us)                 Non dispo
Délais Moy (us)                 Non dispo
Délais Max (us)                 Non dispo
Svc Disruption (us)            > 60000000
Gigue de Paquet, Moy (us)             0.00
Gigue de Paquet, Moy Max (us)        65.54
Gigue de Paquet, Pic (us)            86.02
Gigue de Paquet, InstantanÃ©e (us)    6.14
```

ID VLAN	Non dispo
Priorité VLAN	Non dispo
ID SVLAN	Non dispo
Priorité SVLAN	Non dispo
SVLAN Trame DEI	Non dispo

[Compteur Lien Port 1 Results]

Toutes Trames en Rx	4125307
Toutes Trames en Tx	2511623
Trames Rx	4125307
Octet de Trame en Rx	2112262126
Octet de Trame en Tx	1285949679
Trames Acterna en Rx	4122926
Trames Acterna en Tx	2511616
Trames Pause	0
Trames VLAN Rx	0
Trames QinQ en Rx	0
Trames Unicast	4122926
Trames Multicast	10
Trames de Broadcast	2371
Trame Span tree	0
Trames 64 Octets	60
Trame de 65-127 Octets	103
Trame de 128-255 Octets	9
Trames 256-511 Octets	1
Trames 512-1023 Octets	4125134
1024-1518/1526	0
>1518/1526	0

[Stats d'auto Neg Port 1 Results]

Link Advt. Status	OK
ACK de config du lien	Oui
Vitesse (Mbps)	100
Duplex	Full
Supporte les Trames Pause	Aucune
Contrôle de Flux	Arrêt
10Base-TX FDX	Oui
10Base-TX HDX	Oui
100Base-TX FDX	Oui
100Base-TX HDX	Oui
1000Base-TX FDX	Non
1000Base-TX HDX	Non
Faute Distante	Non

[BERT Port 1 Results]

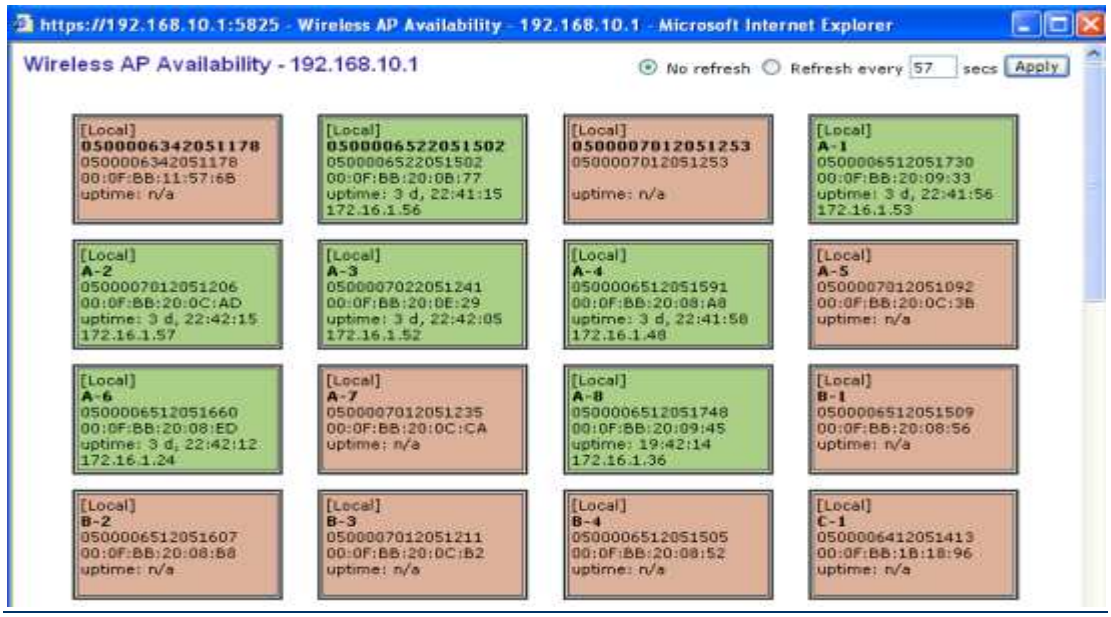
Erreurs bin.	Non dispo
Taux d'Erreur Bit	Non dispo
Secondes Bits Erronées	Non dispo
Nbre Total de Bits reçus	Non dispo
Seconde sans erreur	Non dispo
Seconde sans erreur, %	Non dispo

[Erreurs Port 1 Results]

Trame trop longue	0
Runts	0
Jabbers	0

III.18.4. Rapports

Afin de prendre en charge la partie suivi et maintenance préventive et curative du réseau déployé, par exemple les ponts d'accès seront ainsi visualisés en UP (verte) ou Down (rouge)



III.18.5. Supervision

La supervision concerne les MPAG et les contrôleurs C1000 via les interfaces graphiques GUI et terminal (SSH).

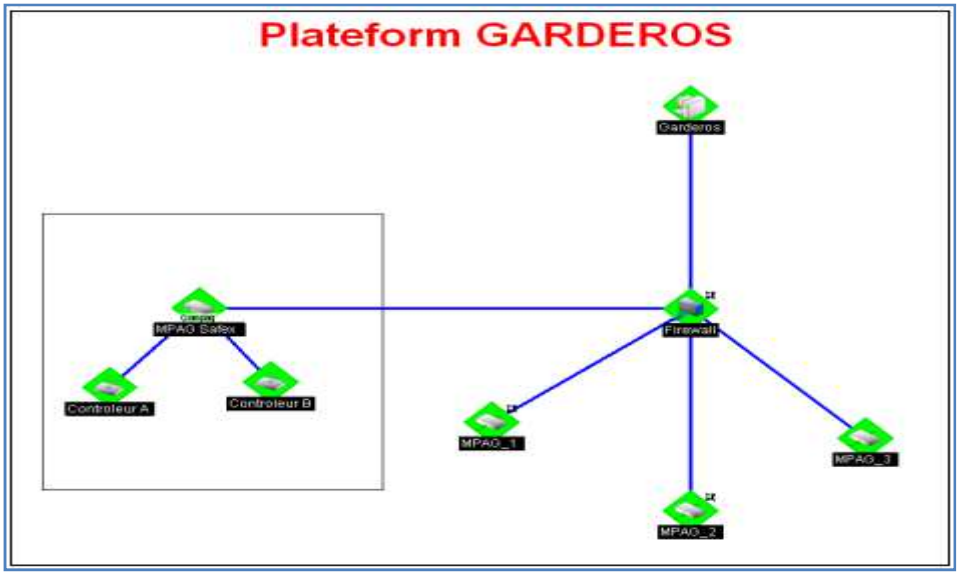


Figure.III.36 : Plate forme Garderos.

La partie supervision comme étalée dans la figure ci-dessus est réalisée et exploitée par le logiciel IpSwitch où les icones représentant les équipements de la plate forme à chacune sont définis des adresses IP lui correspondent dans l'architecture du réseau Wifi.

Cette opération est réalisé sur un poste administrateur installé au niveau de la direction dans le but de prendre en charge l'accès à distance de ladite plate forme pour manipuler et faciliter les interventions en cas de panne et perturbations ou coupures des connexions, sur toutes les équipements actifs tel que les contrôleurs qui synchronisent les points d'accès et les MPAG qui assurent la passerelle à la page Web au niveau des régions authentifié par la partie Radius de Garderos.

Ici, quelques commandes avec l'outil 'ac' sur le MPAG afin de visualiser le trafic et les utilisateurs connectés identifié par l'adresse IP du terminal et son compte attribués.

Garderos Access Controller

```
mpag3[~]# ac show wan
WAN is UP
  WAN type is static IP
  WAN interface eth0
  system MAC is 00:30:48:8b:3c:9a
  WAN address is 192.168.1.203
  traffic:
    10 second rates:      10528.0 kbit/s in    942.0 kbit/s out
     1 minute rates:      10646.3 kbit/s in   1094.4 kbit/s out
    10 minute rates:      10075.9 kbit/s in    689.5 kbit/s out
mpag3[~]# ac show users
   110.10.20.230  00:00:00:00:00:00  MYBTdH77 (4m:28s)
   110.10.18.211  00:00:00:00:00:00  djaweb5 (5m:56s)
   110.10.21.103  00:00:00:00:00:00  MYBmaet9 (11m:46s)
   110.10.16.254  00:00:00:00:00:00  MYBNQHe5 (16m:18s)
   110.10.17.204  00:00:00:00:00:00  algBgLba3alg (16m:24s)
   110.10.20.166  00:00:00:00:00:00  4324m2 (26m:20s)
    110.10.23.67  00:00:00:00:00:00  MYBm2p8N (28m:07s)
   110.10.22.172  00:00:00:00:00:00  MYBn8qFR (38m:48s)
    110.10.16.81  00:00:00:00:00:00  MYDYFLeq (39m:04s)
   110.10.22.106  00:00:00:00:00:00  MYBrfdA8 (45m:07s)
    110.10.20.26  00:00:00:00:00:00  algBbrYAhalg (55m:03s)
   110.10.17.102  00:00:00:00:00:00  algBg4Df8alg (1h:18m:35s)
   110.10.21.114  00:00:00:00:00:00  MYBh3WPg (1h:22m:31s)
    110.10.18.84  00:00:00:00:00:00  djaweb8 (1h:22m:32s)
    110.10.18.63  00:00:00:00:00:00  djaweb3 (1h:31m:48s)
    110.10.18.56  00:00:00:00:00:00  MYDgKE5g (1h:45m:32s)
   110.10.19.178  00:00:00:00:00:00  algBa7dDyalg (1h:49m:17s)
   110.10.22.125  00:00:00:00:00:00  MYBmS3Re (1h:56m:01s)
   110.10.23.125  00:00:00:00:00:00  MYDaqnrr (1h:57m:36s)
   110.10.20.108  00:00:00:00:00:00  MYBNZ49S (2h:02m:12s)
    110.10.17.19  00:00:00:00:00:00  MYBS57Ye (2h:05m:00s)
   110.10.21.144  00:00:00:00:00:00  algBd6HaDalg (2h:11m:51s)
   110.10.17.170  00:00:00:00:00:00  algBdXR2Walg (2h:12m:39s)
   110.10.20.125  00:00:00:00:00:00  49BKqb (2h:12m:45s)
   110.10.18.179  00:00:00:00:00:00  MYBm9XXn (2h:12m:54s)
    110.10.19.79  00:00:00:00:00:00  MYBSpdnr (2h:13m:17s)
   110.10.22.211  00:00:00:00:00:00  MYDfABrd (2h:14m:35s)
     110.10.21.7  00:00:00:00:00:00  MYBhAEqB (2h:14m:55s)
   110.10.19.125  00:00:00:00:00:00  MYDe4AgZ (2h:15m:22s)
   110.10.16.183  00:00:00:00:00:00  algBbEeN4alg (2h:15m:24s)
   110.10.17.173  00:00:00:00:00:00  MYBYaDB3 (2h:17m:34s)
   110.10.22.110  00:00:00:00:00:00  bek1234 (2h:18m:07s)
   110.10.19.134  00:00:00:00:00:00  algBeqBY5alg (2h:18m:20s)
     110.10.17.1  00:00:00:00:00:00  MYBna4Zh (2h:18m:25s)
    110.10.23.66  00:00:00:00:00:00  algBbfpfLalg (2h:18m:54s)
   110.10.21.181  00:00:00:00:00:00  MYDb5XML (2h:18m:55s)

36 Users.
```

III.19. Partie Supervision

III.19.1. Administration et Supervision

1. Gestion via interfaces Web sécurisées (HTTPS, SSH).
2. Gestion via interfaces Web sécurisées (HTTPS, SSH).
3. Gestion du réseau local ou à distance.
4. Statistiques et reporting.
5. Gestion des incidents, relèves d'incidents.
6. SNMP.
7. SYSLOG distant.
8. Authentification administrateurs dans bases LDAP et Active Directory.
9. Authentification administrateurs dans bases RADIUS.

III.19.2. Provisioning et Facturation

1. Portail pour création de comptes.
2. Hiérarchie d'operateur de comptes.
3. Vouchers *(*date de départ – de fin, durées limitées, après première utilisation, connections limitées).
4. Prépaye (cartes à pavées).
5. Import de fichier.
6. Autocréation de compte par l'utilisateur.
7. Interface Web Services.
8. Interface vers logiciels externes via API Web Services.
9. Interface avec logiciels de facturation (PMS).
10. Création et impression de comptes en volume.

III.19.3. Gestion évoluée des utilisateurs

1. Aucun logiciel supplémentaire requis.
2. Aucun logiciel supplémentaire requis.
3. Support IP Zéro configuration :

- IP fixe et DHCP.
- SMTP zéro configuration.
- Proxy et DNS zero configuration.

4. Accès public et prive (profil, priorité).

5. Popup de suivi des connections.
6. Proxy transparent (y compris https, FTP,…).
7. Redirection de sites web personnalisable (par profil utilisateur).
8. Portail d'accueil personnalisable (par Point d'Accès, par VLAN, par Site).
9. Limitation des connexions suivant profil utilisateur par :

- Sites, Zone, VLAN.
- Plage horaire, Jours de la semaine.

10. Limitation des protocoles et des IP en fonction du profil utilisateur.
11. Filtrage URL en fonction du profil utilisateur.
12. IP publique suivant profil utilisateur.

Conclusion Générale

A la fin de ce projet de fin d'étude ou il était question de regarder de prés le déploiement, la mise en service et les problèmes rencontrés lors des exercices pratiques dument sur la connectivité c.à.d. couverture et de sécurité dans les réseaux sans fil.

Vu la mobilité qu'il offre par rapport à celui filaire, le réseau Wifi est largement sollicité de nos jours malgré les contraintes observées lors du déploiement sur le campus.

Certes, durant tout le parcours de notre stage au siège de la direction du projet national Athir/Wimax des connaissances importantes sont acquises y sont très bénéfiques pour notre futur intégration dans le domaine de travail et nous avons appris :

- La technologie sur le Wifi (connaissances de base, normes, contraintes)
- Etude de faisabilité d'un réseau Wifi (avec simulateur et estimation)
- Connaissances des équipements informatiques et leurs fonctionnalités telles que les points d'accès, les Switch et les hubs, convertisseurs FO/FE, etc.…
- Maitrise des systèmes d'exploitation Linux et administration réseau (DHCP, DNS)
- Installation et configuration des réseaux IP et leur déploiement
- Configuration des Points d'accès, contrôleurs, routeurs, Switch L3

Il existe des technologies récentes Mesh purement Wifi (pas de la connectique) assurant le coût et le temps avec des mesures de sécurités complémentaires utilisant un système de contrôleurs des contrôleurs avec des points d'accès travaillant en couverture et pont garantissant un gain et débit suffisant en qualité de service, avec le portail captif également demeurera une bonne solution pour offrir des connexions instantanée aux utilisateurs d'Internet. Sûr, la sécurité dans les réseaux n'est toujours pas une valeur absolue et que les failles et les vulnérabilités ont tendance à se minimiser et contrôler.

Annexes

1) . Hipath Werless Controller Supported Feutures

	Feature	C10	C100	C1000
Manageability	Centralized Management over Layer 3 (CAPWAP)	Yes	Yes	Yes
	Branch Office Support over WAN	Yes	Yes	Yes
	Auto-discovery of new APs	Yes	Yes	Yes
	CDR/RADIUS Accounting	Yes	Yes	Yes
Capacity	Network Interfaces	4x10/100 BaseT	4x10/100 BaseT	2xGigE (Fiber)
	APs Supported per Controller	30	75	200
	Simultaneous Users per Controller	512	2048	4096
	Number of VNS User Segments per Controller	8	32	32
Performance	Automatic Failover to Redundant Controller	Yes	Yes	Yes
	Dual, Hot Swappable Power Supply	No	Yes	Yes
	Premium Radio Frequency Management Support	Yes	Yes	Yes
Mobility	Roaming Between IP Subnets	Yes	Yes	Yes
	Roaming Between Multiple Controllers	No	Yes	Yes
Security	Enhanced 802.11i security with fast roaming	Yes	Yes	Yes
	Captive Portal (URL Redirect) and Walled Garden (unauthenticated access to URL)	Yes	Yes	Yes
Voice	HiPath Premium Voice Support	Yes	Yes	Yes
	Enhanced 802.11e quality of service features	Yes	Yes	Yes
	Simultaneous Voice Calls per Controller (802.11b, G.711, R > 80)	75	200	1000

2) .Power Over Ethernet (POE)

TECHNICAL SPECIFICATIONS	
Output Voltage	48VDC @0.5A
Input Voltage	90-260VAC @47-63Hz
Input Current	0.3A @120VAC, 0.2A @230VAC
Inrush Current	<15A peak @120VAC, <30A peak @230VAC
Efficiency	70+%
Output Ripple	1% Max
Switching Frequency	200kHz
Line Regulation	+/- 0.5%
Load Regulation	+/- 1%
Operating Temperature	-10C to +60 deg C
Storage Temperature	-20 to +85 deg C
Operating Humidity	5% to 90% non condensing
Size (LxWxH)	85x43x30 mm
Weight	4oz
AC Ceonnector	IEC-320 C6
Data IN / POE	RJ45 Shielded Socket
80% Current Indicator	Power LED will change color
Surge Protection	Common Mode
Clamping Protection	11V Data, 77.5V Power
Max Surge Discharge	1200A (8/20uS) Power
Peak Pulse Current	36A (10/1000uS) Data
Shunt Capacitance	<5pf data
Response Time	<1nS
Compliance	UL, EN55022 (CISPR22) class B, Meets CE

3) .Enterasys Wireless Access Points

Supported Features – 802.11a/b/g	AP2605	AP2610/2620	AP2630/2640	AP2650/2660
Management				
Plug'n Play Installation • Automatic Controller Discovery • Centrally deployed configurations and upgrades	√	√	√ Thin mode only	√
Web Management and Configuration	√	√	√	√
Secure Remote Management	√	√	√	√
Number of SSIDs Supported	16	16	8 – standalone 16 – thin mode	16
Security				
Security via WEP, WPA (TKIP), WPA2 (AES), 802.11i, 802.1X	√	√	√ Does not support 802.1X	√
VPN Support: IPSec, PPTP, L2TP	√	√	√	√
Rogue AP Detection mode	√	√	√ Thin mode only	√
Rogue AP Sensor mode	-	√	√ Thin mode only	-
Performance				
Intelligent thin AP (Encryption, blacklisting, QoS and RF Management done by the AP)	√	√	√ Thin mode only	√
Bridging at AP (tagged and untagged traffic forwarding at AP)	√	√	√	√
Filtering at AP (policy enforcement and rate limiting at AP)	-	√	√ Thin mode only	√
Wireless Distribution System (WDS)	-	√	√ Thin mode only	√
Fast failover and Session Availability	√	√	√ Thin mode only	√
Dynamic RF Management	√	√	√ Thin mode only	√
Flexible Client Access (airtime fairness)	√	√	√ Thin mode only	√
Multicast Rate Control	√	√	√ Thin mode only	√
Dual concurrent, Dual band 802.11a (5GHz) and 802.11b/g (2.4GHz) connectivity	√	√	√	√
Voice				
Quality of Service (WMM, 802.11e)	√	√	√	√
Call Admission Control (TSPEC)	√	√	√	√
Power Save (U-APSD)	√	√	√	√
Fast secure roaming and handover between APs	√	√	√	√
Pre-Authentication (Pre-Auth)	√	√	√ Thin mode only	√
Opportunistic Key Caching (OKC)	√	√	√ Thin mode only	√
Capacity				
Simultaneous Voice calls (802.11b, G711, R>80)	12	12	6 – standalone 12 – thin mode	12
Simultaneous users per radio	128	128	128	128

4) .Surpass hiD 6610 – S212 Highlights

Switch L3

General:

24 ports 10/100 base TX
2 Uplink ports
256 VLANs
8K MAC Addresses
13Gbps Switch Fabric*
8.8Gbps Maximum bandwidth*
6.5Mpps Forwarding rate
Non-blocking
AC/DC power (RPU available)
LED indicators

Availability:

Spanning tree (802.1d)
Rapid Spanning Tree (802.1w)
Link Aggregation (802.1ad)
GE Cascading

Multicast:

IGMP v1/v2
IGMP Snooping
IGMP Report Suppression
IGMP Static join, Fast Leave

Quality of Service (QoS)

Classification:

Port based
L2 based (MAC, IEEE 802.1p, Ether type, VLAN)
IP based (ToS/DSCP, IP DA, IP SA)
L4 based (TCP/UDP)

Queuing and scheduling:

4 queue per port
Strict priority (SP)
Weighted Round Robin (WRR)
Random Early Detection (RED)

Management:

Traffic statistics
RMON 4 Groups (Stats, History, Alarms & Events)
SNMP v1/v2
Secure shell (SSH v2)
Access Integrator Element (ACI-E)
Command Line Interface (CLI)

Security:

Port / MAC based authentication based on 802.1x
MAC address limitation
DHCP filtering/snooping
DHCP snooping
IP Source Guard
DHCP Server/Relay agent option82
Storm control
Anti spoofing mechanism
TACACS+ / Radius

Access control List (ACL) based on:

Port
MAC Address - List
Ether type
IP Multicast Address (Multicast Filtering)
Destination and source IP address
L4 (TCP/UDP)

5) .Convertisseur FO/FE SC

- Marque : Trendnet
- Modèle : TFC 100
- Vitesse de transfert : 100 Mbps (half-duplex), 200 Mbps (full-duplex).
- Protocol réseau : CSMA/CD
- Alimentation : 7,5VDC /1,5A (7,2Watts max). Components of the product

6) .Pigtail SC

- Fibre optique multimode 62,5 / 125 (OM1).
- Atténuation maximale (db/km) : 850 / 1300 nm | 3,2 / 0,9.
- Bande passante (Mhz-km) : 850 / 1300 nm | 200 / 500.
- Fibre optique multimode 50 / 125 (OM2).
- Atténuation maximale (db/km) : 850 / 1300 nm | 2,7 / 0,7.
- Bande passante (Mhz-km) : 850 / 1300 nm | 400 / 1 200.
- Fibre optique monomode 9 / 125 (OS1).
- Atténuation maximale (db/km) : 1 300 / 1500 nm | 0,45 / 0,28.
- Chaque Pigtail est testé individuellement et garanti sur 15 ans dans des conditions normales d'utilisation

7) .Jarretière MTRG MM

COLOR	Blue
CONNECTOR1	LC
CONNECTOR2	MTRJ
INSERTION LOSS	<0.3dB
LENGTH	5m
MATERIAL	LSZH
MAXIMUM ATTENUATION	0.4/0.3 dB/KM(1310/1550)
MIN BANDWIDH	200/500 MHZ.Km
MIN BENDING RADIUS	6cm(loaded), 4cm(unloaded)
MODE TYPE	OM3
OP TEMP	-40~+85?
PACKING	Neutral
POLISH	PC-PC
Size	CAT
STORAGE TEMPERATURE	-40~+85?
TEST	100% tested
Garantie	25 Ans

8) .Scalance W788- 1pro

Components of the product

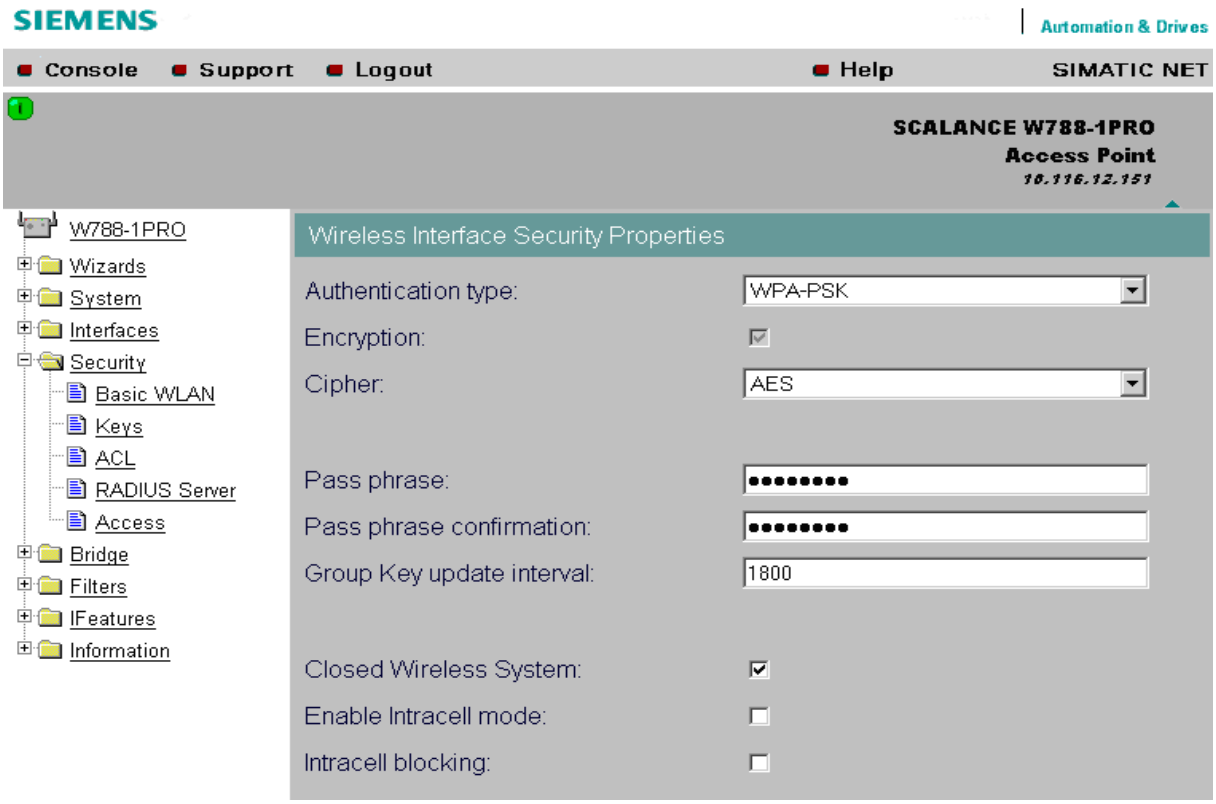
- SCALANCE W788-xPRO/RR or W74x-1PRO/RR
- 2 OMNI antennas ANT795-4MR
- 1 IE IP 67 hybrid plug-in connector
- 1 protective cap for the M12 socket
- 2 (or 4 with SCALANCE W788-2PRO or SCALANCE W788-2RR) sealing plugs for the R-SMA sockets
- 1 SIMATIC NET Industrial Wireless LAN CD with these Configuration Manual for SCALANCE W-700
- 1 Operating Instructions (compact) SCALANCE W788-xPRO/RR or W74x-1PRO/RR in printed form

Properties of the SCALANCE W788

- The Ethernet interface supports 10 Mbps and 100 Mbps, both in full and half duplex as well as autocrossing and autopolarity.
- The wireless interface is compatible with the IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g standards. In the 802.1a- and 802.1g mode, the total transmission rate is up to 54 Mbps. In the turbo mode, the transmission rate is up to 108 Mbps (not permitted in all countries and modes).
- Operation in the 2.4 GHz and 5 GHz frequency bands.
- Support of the authentication standards WPA, WPA-PSK and IEEE 802.1x and WEP, AES and TKIP encryption schemes.
- Suitable for inclusion of a RADIUS server for authentication.
- Device-related and application-related monitoring of the wireless connection.
- The interoperability of SCALANCE W78x devices with WiFi devices of other vendors was tested thoroughly.

Paramétrage de base	
Mode	G
SSID	PCS 7
Wireless Mode	2,4 GHz 54 Mbps (IEEE 802.11g)
	DHCP
Paramétrage de sécurité	
Authentification réseau	WPA-PSK
Cryptage des données	AES
Clé réseau	<un mot de passe>
Confirmez la clé réseau	<répéter mot de passe>

9) .Configuration de l'Access Point (AP) SCALANCE W788-1PRO



Références Bibliographique

Références Bibliographique

- A. Tanenbaum, « Réseaux », 4eme Edition 2009.
- D. Dhoutant, « étude du standard IEEE 802.11 dans le cadre des réseaux ad-hoc de la simulation à l'expérimentation », thèse de doctorat, institut national des sciences appliquée, Lyon, décembre 2003.
- F. LEMAINQUE, « Tout sur les Réseaux sans fil », DUNOD 2009.
- J. Wiley & Sons Ltd; Networking Bible Edition Original-1, Sept 2009.
- J. Antoine Mantagnon, « Les réseaux d'entreprise », Dunod 2011.
- Rapport réalisé par J. DUTREIGE et T. TIMMERMANS, Université Clause Bernard Lyon 1 Département Informatique, MPSIR, Année 2006/2007.

Sites Web

- Httt:/ /www.commentcamarche.net
- Httt://www.isi.edu/nsnam
- http://rubb.free.fr
- http://www.cisco.com
- WWW.futura-sciences.com-hotspot