TABLE DES MATIERES

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABREVIATIONS

AES	Advanced Encryption Standard
AP	Access Point, borne d'un réseau sans-fil
BLR	Boucle Locale Radio
BSS	Basic Service Set
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DES	Directory Entry Service
DIT	Directory Information Tree
DS	Distribution System
DSE	Directory Specific Entry
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol [RFC2284]
FHSS	Frequency Hopping Spread Spectrum
GPRS	General Packet Radio Service
IBSS	Independant Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IR	Infra Red
ISM	Industrial, Scientific and Medical
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format
LEAP	Lightweight Extensible Authentication Protocol
LLC	Logical Link Control
MAC	Medium Access Control
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open System Interconnection
PEAP	Protected Extensible Authentication Protocol
SASL	Simple Authentification and Security Layer
SSID	Service Set Identifier
SSL	Secure Socket Layer

TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security protocol
U-NII	Unlicensed-National Information Infrastructure
VLAN	Virtual Local Area Network
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPA	Wi-Fi Protected Access
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network

INTRODUCTION

L'évolution de la technologie surtout dans le domaine des systèmes réseaux se retrouve désormais au zénith du XXI^{ème} siècle. La technique la plus utilisée actuellement est la liaison sans-fil qui nous offre une solution liée aux problèmes de la liaison filaire : une bande passante limitée, une saturation de ligne, et une limitation géographique. Les avantages des réseaux sans-fil ne sont plus à démontrer surtout à une génération de plus en plus habituée à la mobilité. Le marché des produits munis d'une telle technologie est en plein essor : les ordinateurs portables, un nombre croissant de téléphones mobiles et les consoles de jeux.

Le Wi-Fi est une technologie intéressante permettant la facilité d'accès à Internet haut débit. La mise à disposition de cette technologie dans notre établissement l' « Ecole Supérieure Polytechnique d'Antananarivo » peut certes servir à surfer sur Internet, mais pas seulement, il autorise aussi l'échange de fichiers, de données, etc... Ce ne sont là que quelques exemples de ses usages possibles.

Toutefois, le point crucial lors d'une installation réseau, quelle soit filaire ou sans-fil, est la mise en place d'éléments de protection. La sécurité a toujours été le point faible des réseaux Wi-Fi, à cause principalement de sa nature physique : les ondes radio étant un support de transmission partagé, quiconque se trouvant dans la zone de couverture peut écouter le support et s'introduire dans le réseau. On peut même, grâce à des antennes amplifiées, se trouver hors de portée de la couverture radio pour pénétrer ce réseau. Ces problèmes de sécurité se posent aussi pour des réseaux câblés nécessitant une intrusion physique. C'est ce qui nous a orienté dans le choix de ce mémoire qui s'intitule : « SECURISATION D'UN RESEAU Wi-Fi AU CAMPUS UNIVERSITAIRE DE VONTOVORONA ».

Pour présenter notre étude, ce mémoire est organisé en trois chapitres :

- le premier chapitre consiste à exposer brièvement les réseaux sans fils, en particulier les réseaux Wi-Fi,
- le second chapitre analyse la sécurité du réseau,
- le dernier chapitre montre un modèle de configuration et le déploiement du réseau.

Chapitre 1 : **RESEAU Wi-Fi**

Ce premier chapitre est consacré à l'étude de la transmission sans-fil. Il permet de comprendre les différentes caractéristiques du réseau Wi-Fi, en particulier ses spécificités et ses modes d'opérations.

1.1 GENERALITES

a. Réseaux sans fils

i) Présentation des réseaux sans fils

Un réseau sans-fil est un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire. Grâce aux réseaux sans fils, un utilisateur a la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu. Les réseaux sans fils sont basés sur une liaison utilisant des ondes radioélectriques (radio et infrarouges). Il existe plusieurs technologies se distinguant par la fréquence d'émission utilisée, le débit et la portée des transmissions. Ils permettent de relier très facilement des équipements distants, d'une dizaine de mètres à quelques kilomètres. [1]

ii) Classification des réseaux sans fils

On distingue plusieurs catégories de réseaux sans fils, selon le périmètre géographique offrant une connectivité (appelé zone de couverture) :

- **Réseaux personnels sans fils (WPAN)**

Le réseau personnel sans-fil (appelé également réseau individuel sans-fil ou réseau domotique sans-fil et noté WPAN pour Wireless Personal Area Network) concerne les réseaux sans fils d'une faible portée : de l'ordre de quelques dizaines de mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, ...) à un ordinateur sans liaison filaire ou bien à permettre la liaison sans-fil entre deux machines très peu distantes. [1] [2]

Il existe plusieurs technologies utilisées pour les WPAN telles que :

- Bluetooth ou 802.15.1 qui a une portée de base de 10 à 30 mètres et un débit de 2Mbps
- HomeRF ou Home Radio Frequency, propose un débit théorique de 10 Mbps avec une portée d'environ 50 à 100 mètres sans amplificateur.
- ZigBee ou 802.15.4 qui permet d'obtenir des liaisons sans fils avec une très faible consommation d'énergie.
- Infrarouges qui est une technologie largement utilisée pour la domotique (télécommandes) mais souffre toutefois des perturbations dues aux interférences lumineuses.

– **Réseaux locaux sans fils (WLAN)**

Le réseau local sans-fil (WLAN pour Wireless Local Area Network) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre eux les terminaux présents dans la zone de couverture. Il existe plusieurs technologies concurrentes telles que :

- Wi-Fi (ou *Wireless Fidelity*) offre des débits allant jusqu'à 54Mbps sur une distance de plusieurs centaines de mètres.
- HiperLAN (High Performance Radio LAN), est une norme européenne, permet d'obtenir un débit théorique de 54Mbps sur 100 mètres.

– **Réseaux métropolitains sans fils (WMAN)**

Le réseau métropolitain sans-fil (WMAN pour Wireless Metropolitan Area Network) est connu sous le nom de Boucle Locale Radio (BLR). Les WMAN sont basés sur la norme IEEE 802.16. Le WiMax (Worldwide Interoperability for Microwave Access.) est l’un des réseaux métropolitains le plus connu avec un débit utile de 1 à 70 Mbps pour une portée de 4 à 50 kilomètres.

– **Réseaux étendus sans fils (WWAN)**

Le réseau étendu sans-fil (WWAN pour Wireless Wide Area Network) est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fils les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans-fil. Les principales technologies sont les suivantes :

- GSM (Global System for Mobile communication ou Groupe Spécial Mobile)
- GPRS (General Packet Radio Service)
- UMTS (Universal Mobile Telecommunication System)

Voici la représentation graphique d'une classification des réseaux sans fils:

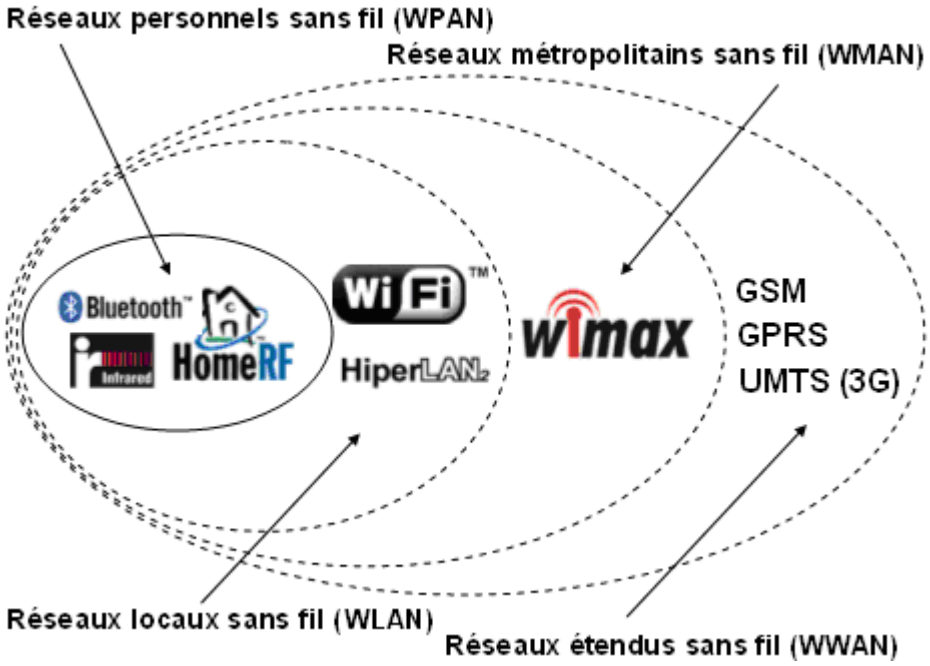

Figure 1.1 : **Classification des réseaux sans fils [1]**

b. Wi-Fi

i) Présentation du Wi-Fi

Le Wi-Fi est une transmission sans-fil permettant de relier des ordinateurs portables, des machines de bureau ou tout type de périphérique à une liaison haut débit sur un rayon de plusieurs dizaines de mètres en intérieur à plusieurs centaines de mètres en environnement ouvert. Il est basé sur une liaison utilisant des ondes radio.

Le terme Wi-Fi est une contraction de *Wireless Fidelity (fidélité sans-fil)* qui correspond au nom donné à la certification délivrée par la WI-FI Alliance. Cet organisme est chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11.

Le Wi-Fi regroupe tout le matériel 802.11a, b, g. Ainsi, lorsqu'un matériel a été certifié Wi-Fi, il doit avoir un logo comme celui-ci :

Figure1.2 : **Logo Wi-Fi [1]**

Le nom de la norme se confond aujourd'hui avec le nom de la certification. Ainsi un réseau Wi-Fi est en réalité un réseau répondant à la norme 802.11.

ii) Standard 802.11

En 1997, la première version du standard a été apparue, il définit trois couches physiques différentes (noté PHY) et une couche de contrôle de l'accès au médium de transmission (MAC). Une des couches PHY utilise les ondes infrarouges (IR) permettant des débits allant jusqu'à 2 Mbps et les deux autres couches utilisent les ondes radio à 2,4 GHz : l'une avec l'étalement de spectre à séquence directe DSSS (Direct Sequence Spread Spectrum) et l'autre avec l'étalement de spectre par saut de fréquence FHSS (Frequency Hopping Spread Spectrum) permettant l'une comme l'autre d'atteindre des débits allant jusqu'à 2 Mbps.

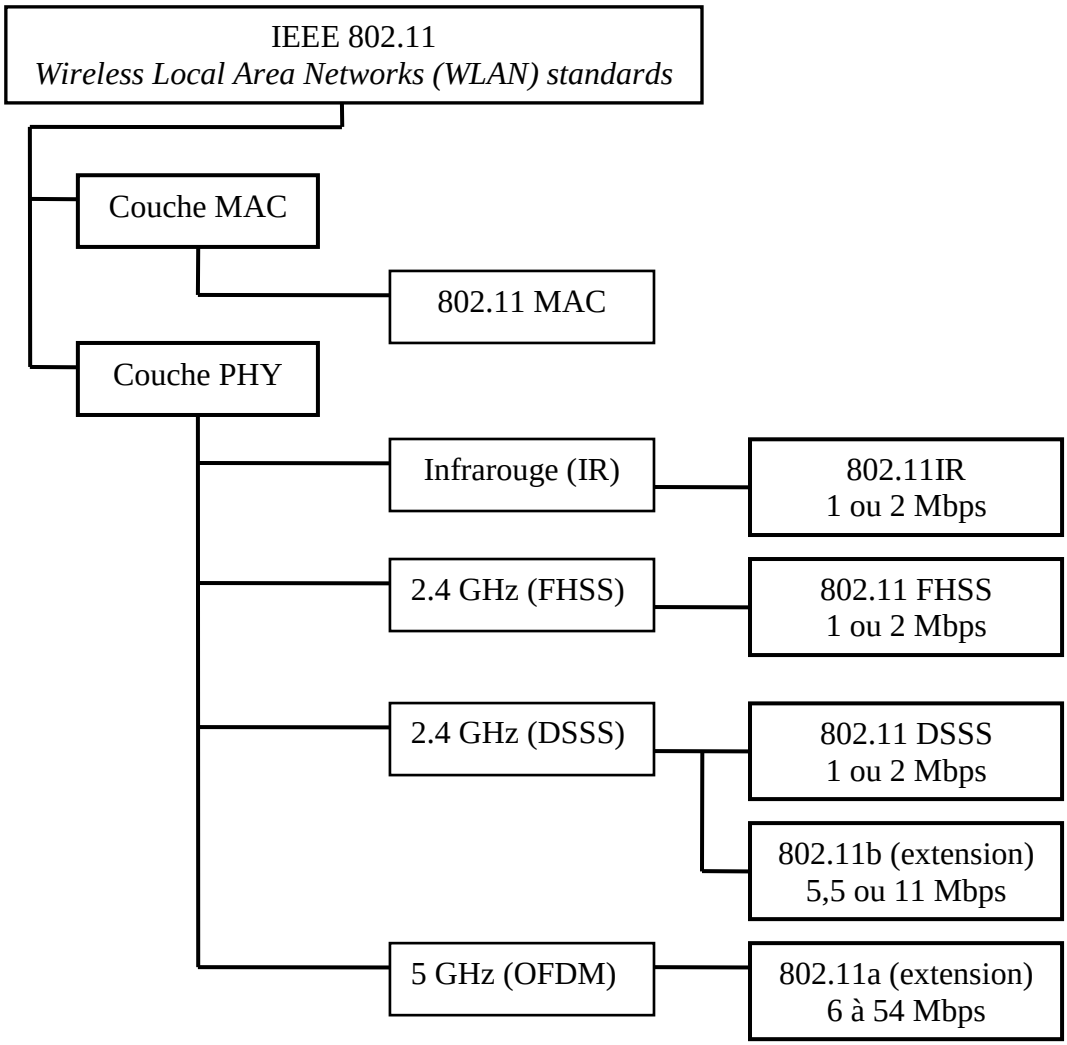

Figure 1.3 : **Récapitulatif des détails du standard 802.11 [3]**

iii) La normalisation 802.11

Pour la normalisation des réseaux sans fils, c'est principalement le groupe de travail IEEE 802.11 de l'IEEE qui s'en charge aux Etats-Unis tandis que le groupe HiperLAN (High Performance Radio LAN) s'en occupe en Europe.

La norme IEEE 802.11 est en réalité la norme initiale offrant des débits de 1 ou 2 Mbps. Des révisions ont été apportées à la norme standard d'origine afin d'optimiser le débit

(c'est le cas des normes 802.11a, 802.11b et 802.11g, appelées **normes 802.11 physiques**) ou bien préciser des éléments afin d'assurer une meilleure sécurité ou une meilleure interopérabilité.

- **802.11b**

Cette norme utilise la bande des 2,4GHz ou la bande ISM. Elle utilise comme technique de transmission l'étalement de spectre à séquence directe ou DSSS (Direct Sequence Spread Spectrum). Pour cette norme, on ne peut utiliser que 3 réseaux sur une même cellule et elle offre un débit maximal de 11 Mbps brut (5,6 Mbps net). La norme 802.11b spécifie 14 canaux radio dans la bande des 2,4GHz ou ISM (Industrial, Scientific and Medical). C'est avec cette norme que le Wi-Fi s'est imposé.
Le tableau suivant montre le débit et la portée de 802.11b :

Débit théorique	**Portée (en intérieur)**	**Portée (à l'extérieur)**
11 Mbps	50 m	200 m
5,5 Mbps	75 m	300 m
2 Mbps	100 m	400 m

Tableau1.1 : **Débit et portée de 802.11b [1]**

- **802.11g**

La norme 802.11g offrira un haut débit (54 Mbps théoriques, 32 Mbps réels) sur la bande de fréquence des 2,4 GHz. La norme 802.11g a une compatibilité ascendante avec la norme b. Ce qui signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b. Le tableau 1.2 indique le débit et la portée de 802.11g.

Débit théorique	Portée (en intérieur)	Portée (à l'extérieur)
54 Mbps	27 m	75 m
48 Mbps	29 m	100 m
36 Mbps	30 m	120 m
24 Mbps	42 m	140 m
18 Mbps	55 m	180 m
12 Mbps	64 m	250 m
9 Mbps	75 m	350 m

Tableau1.2 : **Débit et portée de 802.11g [1]**

Il y a plusieurs normes pour la technologie 802.11 mais ce sont les 802.11b et 802.11g qui sont les plus utilisées actuellement, surtout dans les réseaux de types WLAN. Les différentes normes sont récapitulées dans le tableau 1.3.

Groupe	Description
802.11a	Ajout d'une nouvelle couche physique : jusqu'à 54 Mbps dans la bande U-NII.
802.11b	Ajout d'une nouvelle couche physique : jusqu'à 11Mbps dans la bande ISM.
802.11c	Incorporation des fonctionnalités de 802.1d.
802.11d	Utilisation de 802.11 dans de nouveaux pays.
802.11e	Travaux sur la Qualité de Service.
802.11f	Travaux sur l'interopérabilité entre les points d'accès.
802.11g	Ajout d'une nouvelle couche physique : jusqu'à 54Mbps dans la bande ISM.
802.11h	Harmonisation de 802.11a avec le standard européen.
802.11i	Amélioration de système de sécurité et d'authentification.
802.11IR	Utilisation des signaux infrarouges.
802.11j	Harmonisation de 802.11a avec le standard japonaise.

Tableau1.3 : **Les groupes de travail du groupe 802.11 [4]**

1.2. SPECIFICITE DE 802.11

La figure 1.4 précise les couches du modèle OSI spécifiées par le 802.11. La couche MAC fonctionne avec la couche LLC IEEE 802.2 également utilisée au dessus du standard pour un réseau local Ethernet.

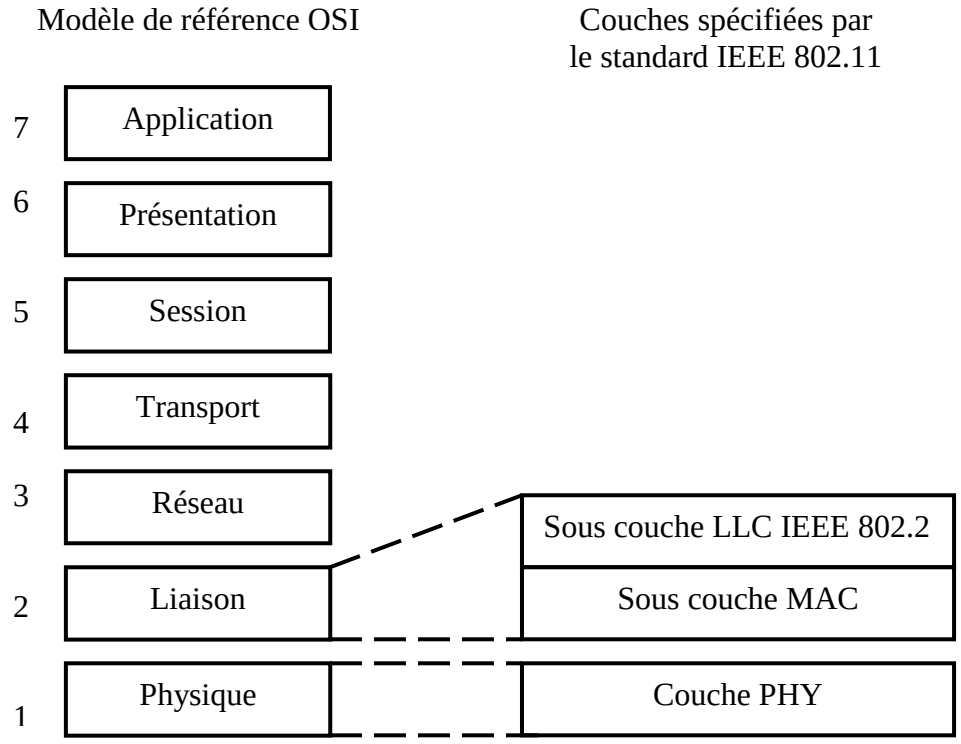

Figure1.4 **: Couches du modèle OSI spécifiées par le standard 802.11 [3]**

a. Couche liaison de données

Cette couche assure la transmission des données ou informations entre deux ou plusieurs systèmes immédiatement adjacents. Elle détecte et corrige dans la mesure du possible les erreurs issues de la couche inférieure. Les objets échangés sont souvent appelés « trames ».

Elle se compose de deux sous-couches :

- le contrôle de liaison logique (LLC)
- le contrôle d'accès au support (MAC)

i) La sous-couche LLC

Le standard 802.11 utilise la sous-couche LLC 802.2 et l'adressage sur 48 bits, tout comme les autres LAN 802, ce qui simplifie le pontage entre les réseaux sans fils et filaires. Par contre, le contrôle d'accès au support est propre au WLAN.

ii) La sous-couche MAC

La couche MAC utilise des primitives fournies par la couche PHY. Elle propose par ailleurs une interface standard à la couche LLC qui peut ainsi utiliser toutes les fonctionnalités de transmission de données sans en connaître les spécificités. La sous-couche MAC définit comment un utilisateur obtient un canal de transmission lorsqu'il en a besoin. Il utilise le **mécanisme d'accès au médium CSMA/CA.**

La CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) ou méthode d'accès multiple à détection de porteuse et évitement de collision est basée sur une fonction de détection de porteuse pour déterminer si le médium est occupé ou non. Avant qu'une station ne décide d'émettre, elle vérifie au préalable que le canal de transmission n'est pas déjà occupé par une émission. [3]

b. <u>Couche physique</u>

La couche physique a pour rôle principal d'établir et de maintenir le lien radio pour permettre la transmission de données sans-fil entre les stations constituant le réseau.

i) Transmission par ondes radio

La transmission par ondes infrarouge (850 à 950 nm) souffre de plusieurs défauts qui limitent son usage à des cas bien précis. Les diodes infrarouges transmettent de manières quasi directionnelles. Pour qu'un couple émetteur/récepteur puisse communiquer, il est indispensable que l'émetteur de l'un soit en vue du récepteur de l'autre. Cette restriction est embarrassant lorsqu'il s'agit de connecter des stations mobiles. Les ondes infrarouges ne peuvent pas traverser des surfaces opaques. Elles souffrent également d'une portée plutôt faible (environ 10 mètres).

Par contre, la transmission par ondes radio ne souffre pas des inconvénients évoqués précédemment. Elles sont omnidirectionnelles et s'accommodent de la présence d'obstacles opaques dans sa trajectoire. Les ondes radio souffrent néanmoins des interférences, des problèmes de trajets multiples surtout en milieu clos et des atténuations dues aux propriétés plus ou moins absorbantes des matériaux.

ii) Les bandes de fréquence : ISM et U-NII

L'utilisation des bandes de fréquences est régie par des organismes propres à chaque pays telles que : la FCC (USA), l'ART (France), MKK (Japon), l'OMERT (Madagascar), ETSI (Europe). Les bandes sans licence utilisées dans 802.11 sont la bande ISM et la bande U-NII :

- La bande ISM (Industrial, Scientific and Medical) correspond à trois sous couches de fréquences : 902-928 MHz ; 2.4-2.4835 GHz et 5.725-5.825 GHz. C'est la bande des 2.4 GHz qui est utilisée dans 802.11 avec une largeur de bande de 83.5 Mhz

- La bande U-NII est située dans les 5GHz. Elle offre une largeur de bande plus importante, de 300 MHz au lieu de 83.5 MHz pour l'ISM. La bande U-NII n'est pas continue, et est divisée en trois sous bandes distinctes de 100MHz, qui utilisent chacune une puissance de signal différente. [4]

iii) Technique de transmission des signaux

- **OFDM**

La modulation OFDM permet d'avoir des débits importants (allant jusqu'à 54Mbps). On la trouve à la fois dans le 802.11g et 802.11a. Il utilise le principe de multiplexage, ce qui permet la transmission simultanée de plusieurs communications sur une même bande de fréquences.

– **FHSS**

La technique d'étalement de spectre par saut de fréquence est utilisée pour éviter les interférences. A des instants donnés, l'émetteur et le récepteur se mettent d'accord pour transmettre sur une fréquence différente de celle utilisée précédemment. Le choix de la fréquence suivante est déterminé par une fonction pseudo aléatoire.

– **DSSS**

La technique utilisée dans le DSSS consiste à répartir la transmission sur une plus large bande pour atténuer les effets d'un pic de puissance localisée. La chance pour qu'à un instant donné tout le signal transmis soit brouillé par une transmission parasite est presque nulle. La perturbation résultante du signal parasite est beaucoup plus faible. La probabilité de reconstruire le message initial est plus forte. [4]

1.3. MODES D'ASSOCIATIONS

Le mode d'association configuré sur un module Wi-Fi détermine ses possibilités de connexion avec les autres. En général, on utilise deux modes : **Ad hoc** et **Infrastructure**.
Mais nous allons voir qu'il existe d'autres configurations possibles pour un point d'accès ou bien pour une carte qui fonctionne en un point d'accès.

a. Mode Infrastructure

En mode infrastructure, chaque ordinateur station se connecte à un point d'accès (en anglais AP ou Access Point) via une liaison sans-fil. L'ensemble formé par le point d'accès et les stations situés dans sa zone de couverture est appelé ensemble de services de base BSS et constitue une cellule. Chaque BSS est identifié par un BSSID à 48 bits qui correspond à l'adresse MAC du point d'accès. Il est possible de relier plusieurs points d'accès entre eux c'est-à-dire plusieurs BSS par une liaison appelée système de distribution ou DS afin de constituer un ensemble de services étendu ESS. Le système de distribution peut être aussi bien un réseau filaire qu'un câble entre deux points d'accès ou bien un réseau sans-fil. Un ESS est repéré par un ESSID qui est un identifiant de 32 caractères de long (au format ASCII) servant de nom pour le réseau. L'ESSID, souvent abrégé en **SSID**, représente le nom du réseau et représente en quelque sorte un premier niveau de sécurité dans la mesure où la connaissance du SSID est nécessaire pour qu'une station se connecte au réseau étendu. [3] [4]

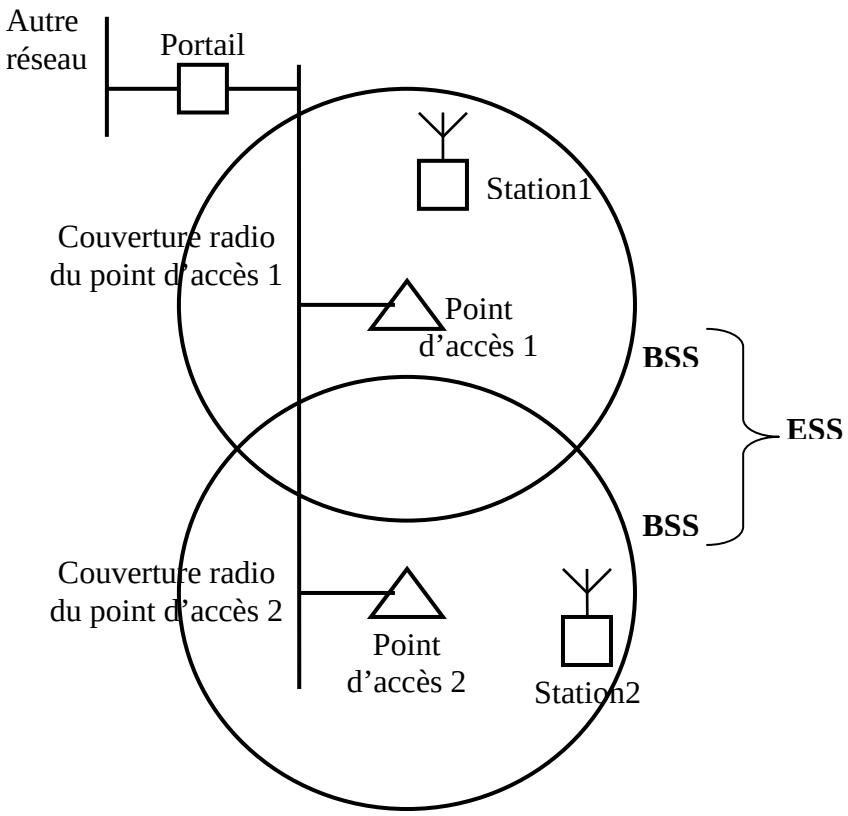

Figure 1.5 : **Mode Infrastructure [3]**

b. Mode Ad –hoc

En mode ad hoc, les machines sans fils clientes se connectent les unes aux autres afin de constituer un réseau point à point, c'est-à-dire un réseau dans lequel chaque machine joue à la fois le rôle de client et le rôle de point d'accès. L'ensemble formé par les différentes stations est appelé IBSS ou ensemble de services de base indépendants. Un IBSS est ainsi un réseau sans-fil constitué au minimum de deux stations et n'utilisant pas de point d'accès. Il est identifié par un SSID, comme l'est un ESS en mode infrastructure. [3] [4]

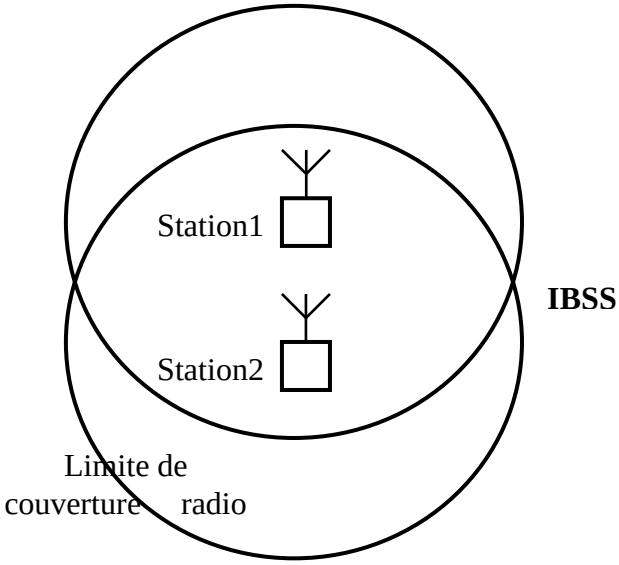

Figure 1.6: **Mode Ad hoc [1]**

c. Mode Répéteur

Ce mode permet à un point d'accès de transmettre les communications provenant des clients vers un autre point d'accès au lieu de les transmettre vers le réseau câblé. Donc un point d'accès en mode répéteur n'a pas besoin d'être connecté au réseau local via un câble RJ45. Un client peut se connecter sur un point d'accès en mode « Répéteur ».

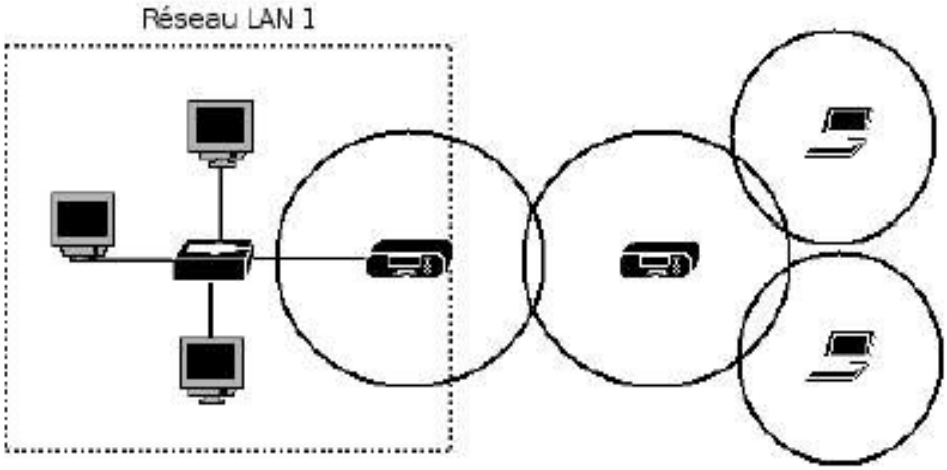

Figure1.7: **Mode Répéteur [5]**

Chapitre 2 : SECURITE RESEAU

En dehors de la destruction et du vol de document ou des données privées qu'on possède sur un ordinateur, un éventuel pirate pourrait vouloir se servir du système réseau comme d'une passerelle. Au cas où un système est piraté, une solution convenable est de réinstaller entièrement le système, cela implique une perte de temps et de finance.

Il est donc nécessaire de comprendre les méthodes d'attaques utilisées par les pirates afin de pouvoir lutter contre ce danger. Puis, il faut appliquer une politique de sécurité à chaque fois qu'on met en place un système pour éviter le plus possible le risque de piratage.

2.1. PROBLEMATIQUES DES RESEAUX WI-FI

Nous allons brièvement évoquer ci-dessous les inconvénients des réseaux Wi-Fi.

a) Complexité

Le premier problème auquel l'administrateur réseau est confronté est la diversité des compétences nécessaires à la mise en œuvre d'un réseau Wi-Fi. Il faut prendre en considération les problèmes de transmission radio, un éventuel audit du site, l'intégration de l'existant (réseau câblé,…), le respect de la régulation, le support effectif des standards actuels et à venir, l'administrateur de ce futur réseau,….

b) Attaques et intrusions

On peut classifier les attaques en deux groupes principaux : les attaques passives et les attaques actives, qui sont bien évidemment plus dangereuses.

i) Attaques passives

Dans un réseau Wi-Fi, il s'agit tout simplement d'écouter le trafic radio dans l'air. L'écoute passive est d'autant plus facile que le média air est difficilement maîtrisable. Bien souvent, la zone de couverture radio d'un point d'accès déborde du domaine privé d'une entreprise ou d'un particulier.

ii) Attaques actives

Les différentes attaques connues dans les réseaux filaires et qui touchent le monde du Wi-Fi sont : [6]

- Attaques DoS (Denial of Service) qui a pour but de bloquer des points d'accès Wi-Fi.
- Attaque par force brute qui consiste à tester toutes les combinaisons possibles afin de récupérer un mot de passe ou une clé de chiffrement utilisée dans un réseau.
- Attaque par dictionnaire qui est utilisée pour récupérer un mot de passe ou une clé en utilisant une base de données contenant un grand nombre de mots.
- Spoofing (usurpation d'identité) est une technique permettant à un pirate d'envoyer à une machine des paquets, semblant provenir d'une adresse IP autre que celle de la machine du pirate.

iii) Intrusions

Les intrusions dans l'environnement sans-fil peuvent être classifiées comme suit : [6]

- Surveillance : elle consiste à observer et décoder le trafic effectif du réseau.
- Impersonation : ce type consiste à prendre la place d'un client ou d'un AP valide en utilisant son adresse (BSSID et ESSID pour un AP), dans l'objectif d'accéder au réseau ou aux services.
- Intrusion Client : consiste à exploiter une vulnérabilité du client pour accéder au réseau.
- Intrusion Réseau : qui vise à prendre le contrôle des ressources réseau d'une entreprise.

c) Multiplicité des méthodes d'attaques et d'intrusions

Du fait des faiblesses des solutions standard, de nombreux risques existent en Wi-Fi. Il s'agit typiquement des Fake AP, Rogue AP, Honey Pot, dont on parle le plus souvent. [6]

i/ Fake AP

Le Fake AP n'est pas un véritable AP. Des logiciels permettent de faire apparaître l'interface Wi-Fi d'un poste client (généralement sous Linux) comme un AP, et de configurer son ESSID (nom symbolique du WLAN) et BSSID (adresse MAC de l'AP) dans un objectif d'impersonation.

ii/ Rogue AP

La faille de sécurité dite Rogue AP est la plus redoutée en entreprise (nous traduirons Rogue par indésirable ici). Elle survient quand un utilisateur du réseau connecte un AP sur la prise Ethernet murale, lui permettant d'avoir une certaine mobilité avec son ordinateur à l'intérieur de la cellule ainsi créée. Ces installations pirates, pas nécessairement malveillantes, sont particulièrement dangereuses parce qu'elles ouvrent le réseau de l'entreprise au monde Wi-Fi.

iii/ Honey Pot

Le pot de miel est un AP qui cherche à apparaître comme faisant partie intégrante du réseau de la société pour attirer les postes clients (utilisation du même ESSID), et les laisser se connecter (au niveau WLAN). De cette façon, l'Honey Pot espère pouvoir espionner la phase de connexion, pour en déduire les paramètres utiles, quitte à effectivement reproduire simultanément la phase de connexion vers le réseau réel.

2.2 MESURES DE SECURITE

Un réseau sans-fil est beaucoup plus sensible qu'un réseau filaire car les données circulent librement dans l'air. Il est essentiel de protéger un réseau sans-fil, même si on considère que les données qui circulent n'ont rien de confidentiel. En effet, un réseau sans-fil non protégé peut permettre à n'importe quel utilisateur du voisinage d'utiliser une connexion Internet et éventuellement lancer un certains nombre d'attaques.

a. Cryptage et Firewall

i) Le cryptage

Le cryptage ou chiffrement garantit la confidentialité des données. Le cryptage consiste à prendre un message, dit « en clair », et à le soumettre à une fonction ou algorithme mathématique pour produire un texte « crypté ». Le déchiffrement est la transformation inverse. Les algorithmes de cryptage se servent le plus souvent d'une valeur, appelée clé, qui sert à chiffrer et à déchiffrer les données. [7]

ii) Le Firewall

Le Firewall ou pare-feu est un processus qui analyse le trafic entrant, sortant et traversant. C'est une machine qui a pour rôle principal de protéger le réseau. Le Firewall filtre l'entrée de trafic externe, par exemple l'Internet, vers le réseau local et inversement.

Le filtrage de paquet consiste à regarder l'en tête d'un paquet qui traverse une machine et à décider de l'avenir de ce paquet. Celui-ci peut être rejeté, accepté ou modifié suivant des règles plus ou moins complexe. Dans de nombreux cas, on utilisera le filtrage pour contrôler et/ou sécuriser l'intérieur du réseau local du monde extérieur. [8]

b. Authentification RADIUS

L'authentification est une procédure qui permet de vérifier et de valider l'authenticité d'une entité tandis que l'identification permet de connaître l'identité d'une entité en question. En ce qui concerne l'authentification réseau, il s'agit d'authentifier une machine lorsqu'elle se branche sur le réseau afin d'autoriser ou refuser l'usage du réseau [2]

RADIUS (*Remote Authentication Dial-In User Service*) est un protocole d'authentification standard. Le protocole RADIUS repose principalement sur un serveur (le serveur RADIUS par exemple), relié à une base d'identification (annuaire LDAP, ...) et un client RADIUS (c'est le point d'accès pour un réseau Wi-Fi), appelé **NAS** (*Network Access Server*) faisant office d'intermédiaire entre l'utilisateur final et le serveur. L'ensemble des transactions entre le client RADIUS et le serveur RADIUS est chiffré et authentifié grâce à un secret partagé. [9]

i) Les paquets RADIUS

Le protocole RADIUS utilise 4 types de paquets pour faire les transactions :

- Access-Request : c'est le premier paquet envoyé par le NAS. Il contient l'identité de l'utilisateur qui se connecte (username/password ou CN ou adresse MAC).
- Access-Accept : c'est le paquet renvoyé par le serveur Radius pour accepter la requête du client après l'interrogation de sa base d'authentification.
- Access-Reject : un paquet émis par le serveur Radius pour spécifier au client que sa requête est rejetée.
- Access-Challenge : ce paquet est émis par le serveur Radius soit pour émettre une nouvelle fois un access-request, soit pour demander des informations complémentaires.

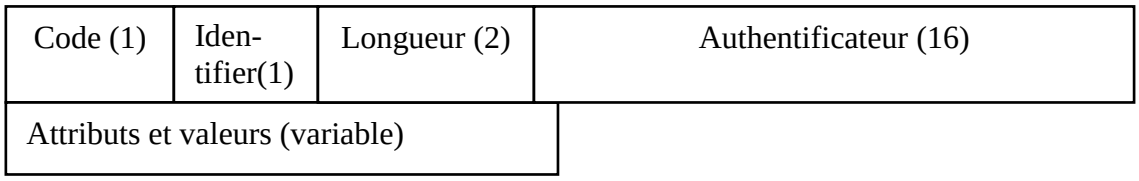

Figure2.1 : **Format des paquets du protocole Radius [10]**

Code : contient le type du paquet (il a comme valeur 1 - access-request, 2 - access-accept, 3- access-reject, 4- accounting-request, 5- accounting-response, 11- access-challenge).
Identifier : utilisé pour associer les requêtes et les réponses.
Authentificateur : utilisé pour que le NAS puisse authentifier les réponses du serveur.
Attributs et valeurs : Ces attributs permettent au client de communiquer des informations au serveur (password, adresse MAC…).

Voici quelques attributs nécessaires pour l'authentification 802.1x et Radius :

Called-Station-Id : contient l'adresse MAC de l'équipement NAS

Calling-Station-Id : contient l'adresse MAC de la machine de l'utilisateur.

NAS-IP-Address : Adresse IP de l'équipement NAS.

NAS-Port : Port sur lequel est connecté le supplicant.

User-Name : Nom d'utilisateur.

Password : Mot de passe utilisateur.

ii) Terminologie

Il y a plusieurs acteurs pour le protocole RADIUS:

- Le client, encore appelé « supplicant », il s'agit de l'entité qui souhaite être authentifiée de façon à avoir accès aux ressources du réseau.

- Le point d'accès sans-fil Wi-Fi encore appelé « authenticator » ou NAS (*Network Access Server*).

- Le serveur d'authentification, en général un serveur RADIUS. Ce serveur RADIUS est supporté par Windows 2003 Server et Linux.

- La méthode d'authentification : il en existe plusieurs qui, suivant les mécanismes d'authentification (login/mot de passe par exemple) mis en place côté serveur et client, apportent des niveaux de sécurité différents.

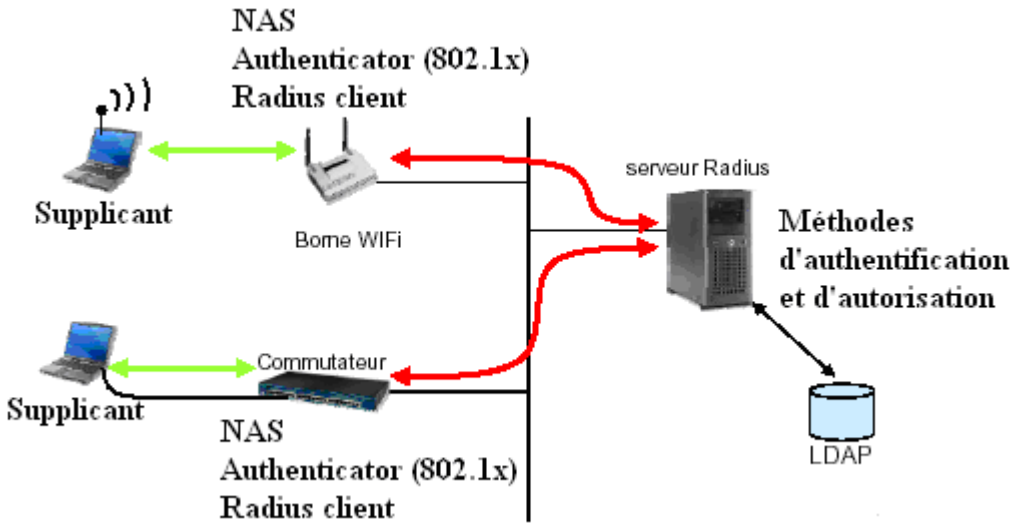

Figure2.2 : **Terminologie des acteurs [10]**

iii) Processus d'authentification 802.1x

RADIUS utilise le mécanisme d'authentification du protocole 802.1x qui se fait avec les étapes suivantes :

- La première étape est l'association physique du client avec le point d'accès (chemin 1 sur l'illustration).

- Deuxième étape : tant que le client n'est pas authentifié, il ne peut pas avoir accès au réseau, seul les échanges liés au processus d'authentification sont relayés vers le serveur d'authentification par le point d'accès (chemin 2 sur l'illustration).

- Une fois authentifié, le point d'accès laisse passer le trafic lié au client (chemin 3 sur l'illustration) et ce dernier peut avoir accès aux ressources du réseau.

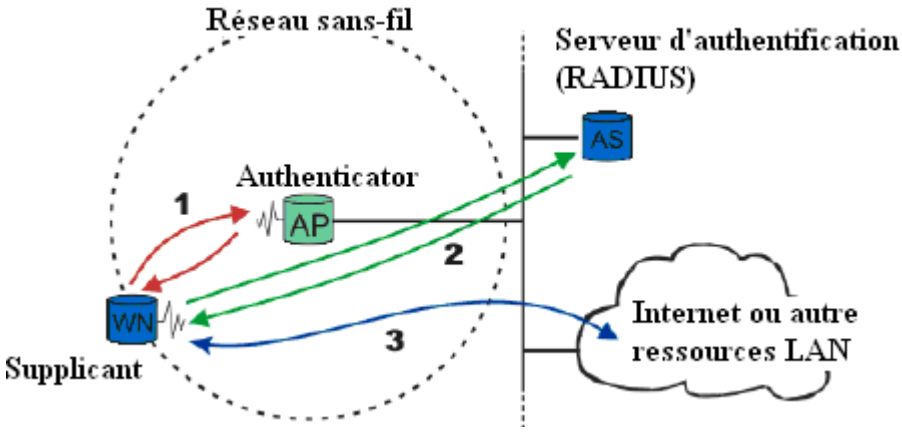

Figure 2.3 : **Processus d'authentification 802.1x [11]**

iv) Le protocole EAP

RADIUS repose sur le protocole EAP (ou **E**xtensible **A**uthentication **P**rotocol) du 802.1x pour les communications du client vers le serveur d'authentification.

EAP est un protocole de transport de protocole d'authentification. L'intérêt de l'architecture de EAP est de pouvoir utiliser divers mécanismes d'authentification sans que l'équipement réseau ait besoin de les connaître. Dans ce cas, il agit comme un tunnel transparent vers un serveur qui lui implémente les mécanismes souhaités (par exemple: mot de passe, certificats, ….). Son fonctionnement dans ses différentes variantes est décrit comme suit : [12]

– **Dialogue entre le supplicant et l'authenticator** : **EAPoL**

Le standard 802.1x spécifie un format de trame Ethernet. Le port du commutateur qui est en mode 802.1x n'acceptera que ce type de trame tant que l'authentification n'est pas accomplie.

Ces trames transportent dans leur charge utile le protocole EAP. On parle d'EAPoL pour « EAP Over LAN », utilisé pour le dialogue entre le Supplicant et l'Authenticator.

– **Dialogue entre l'authenticator et le serveur d'authentification** : **EAP in RADIUS**

L'authenticator est responsable du relayage des trames EAP entre le supplicant et le serveur d'authentification. Ce relayage prend en compte les transformations nécessaires de ces paquets pour une transmission dans le format approprié. Le serveur d'authentification que l'on utilisera sera un serveur RADIUS, l'authenticator communique alors en EAPoL avec le supplicant et en EAP in RADIUS avec le serveur d'authentification. L'authenticator est client du serveur RADIUS et peut attribuer les informations qu'il reçoit au supplicant (temps de session, ...). Dans la configuration de cette étude, toutes les autres trames EAP venant du supplicant sont converties du format EAPoL en EAP in RADIUS et inversement étant donné que le standard 802.1x n'impose pas l'utilisation de RADIUS. Lorsque l'authenticator reçoit un message EAPoL de la part du supplicant qu'il doit faire parvenir au serveur d'authentification, il le transforme en un paquet RADIUS ayant un attribut de code 79 indiquant qu'il encapsule un paquet EAP.

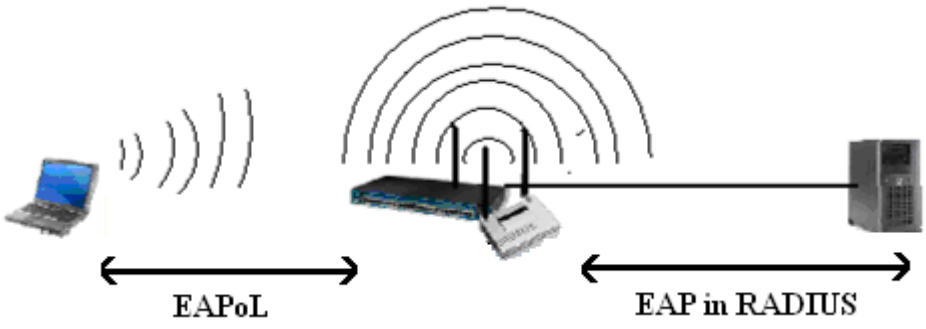

Figure 2.4: **Echanges EAP**

v) Méthodes d'authentification EAP

Le protocole EAP utilisé par RADIUS supporte plusieurs méthodes d'authentifications:

EAP-MD5 : basée sur mot de passe, jugée non sécurisée et inapte pour le sans-fil.

LEAP : basée sur mot de passe, jugée non sécurisée.

Generic Token Card – **EAP-GTC** : basée sur les données contenues dans une carte à puce.

EAP-TLS : utilisation des certificats chez le supplicant et chez le serveur d'authentification.

EAP-TTLS : utilise un tunnel TLS pour procéder à une authentification via une autre méthode EAP. Seul le serveur doit obligatoirement disposer d'un certificat.

EAP -PEAP (Protected EAP) : similaire à EAP-TTLS mais bénéficie d'une encapsulation sécurisée. Le principe de la méthode d'authentification EAP – PEAP est illustrée par la figure ci-dessous :

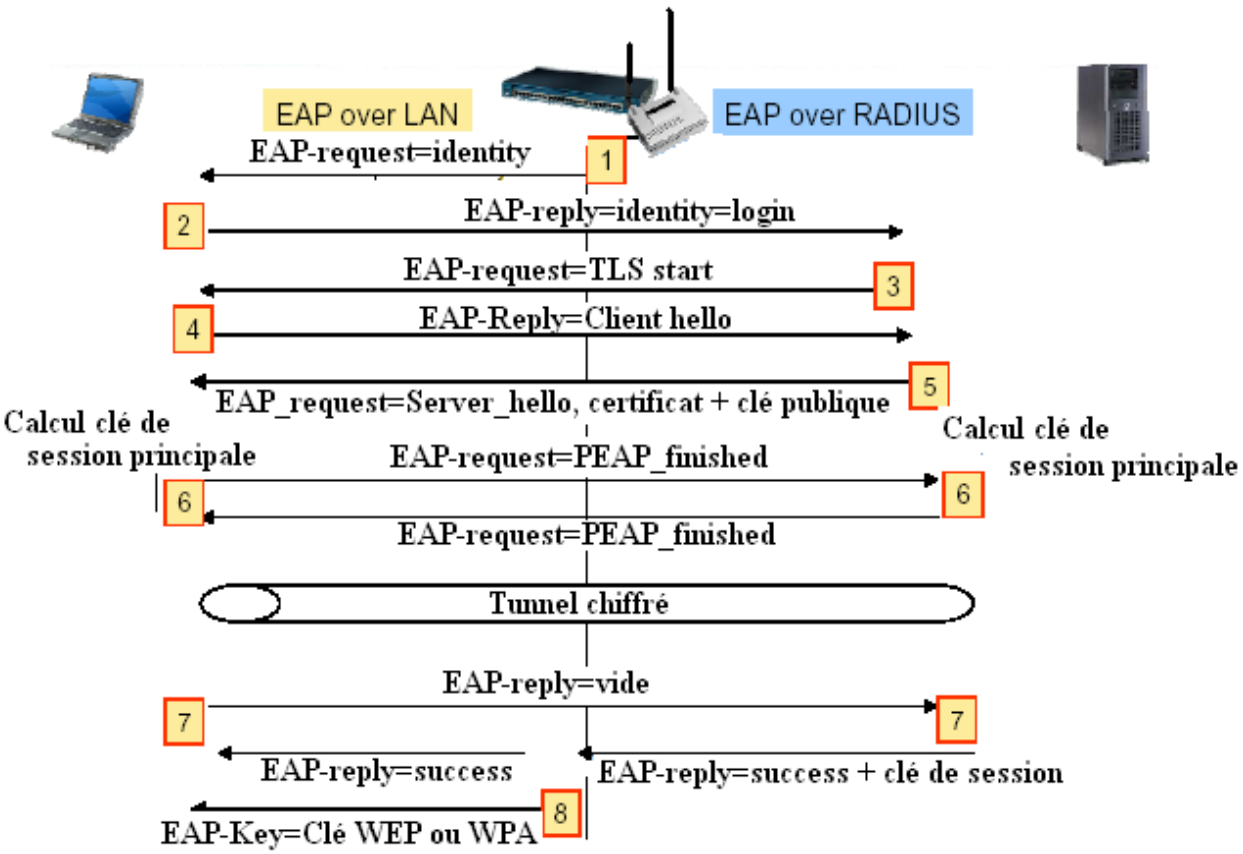

Figure2.5 : **Authentification avec login/password (PEAP) [13]**

1- Le NAS envoie au client une requête EAP lui demandant son identité.

2- Le client répond avec le User-Name comme identité.
3- Le serveur RADIUS démarre la séquence TLS par l'envoi du message TLS_start.
4- Le client répond par un message client_hello composé de : la version de TLS, un challenge (nombre aléatoire), un identifiant de session, la liste des algorithmes de chiffrement supportés par le client.
5- Le serveur répond par un message server_hello constitué de : son certificat et sa clé publique, une demande au client d'envoyer un challenge, un identifiant de session calculé à partir de celui du client, choix d'un algorithme de chiffrement en fonction de ceux connus par le client.
6- Le client et le serveur calculent une clé de chiffrement pour la session principale. Puis il y a création de tunnel chiffré pour la transmission de mot de passe.

7- Le client renvoie une réponse EAP vide et le serveur répond par un message EAP_success avec une clé de session pour la borne Wi-Fi.

8- À partir de cette clé de session, la borne calcule une clé WEP ou WPA et l'envoie au client.

c. Annuaire LDAP

LDAP (*Lightweight Directory Access Protocol*) est un annuaire utilisé par un serveur d'authentification RADIUS pour stocker et sécuriser les informations nécessaires à l'authentification des utilisateurs. [1]

i) Introduction aux annuaires

- **Définitions et caractéristiques**

Un annuaire est un recueil de données dont le but est de pouvoir retrouver facilement des ressources (généralement des personnes ou des organisations) à l'aide d'un nombre limité de critères.

L'annuaire électronique est un type de base de données spécialisée permettant de stocker des informations de manière hiérarchique et offrant des mécanismes simples pour rechercher l'information, la trier, l'organiser selon un nombre limité de critères.

Les annuaires électroniques possèdent les caractéristiques suivantes:

- **dynamiques** : la mise à jour d'un annuaire électronique est beaucoup plus simple à réaliser.
- **sûrs** : les annuaires disposent de mécanismes d'authentification des utilisateurs grâce à un mot de passe et un nom d'utilisateur ainsi que des règles d'accès.
- **souples** : ils permettent ainsi de classer l'information selon des critères multiples.

– **Différence entre annuaire et base de données**

Un annuaire est un type de base de données spécifique, c'est-à-dire qu'il s'agit d'une sorte de base de données ayant des caractéristiques particulières :

- un annuaire est prévu pour être plus sollicité en lecture qu'en écriture. Cela signifie qu'un annuaire est conçu pour être plus souvent consulté que mis à jour.
- les données sont stockées de manière hiérarchique dans l'annuaire, tandis que les bases de données dites "relationnelles" stockent les enregistrements de façon tabulaire.
- Un annuaire doit être capable de gérer l'authentification des utilisateurs ainsi que les droits de ceux-ci pour la consultation ou la modification de données.

Ainsi, un annuaire est généralement une application se basant sur une base de données afin d'y stocker des enregistrements. Il est aussi un ensemble de services permettant de retrouver facilement les enregistrements à l'aide de requêtes simples. Une base de données par contre n'est pas forcément un annuaire.

– **Normalisation d’accès**

Ainsi, un annuaire est un serveur remplissant les conditions décrites ci-dessus, mais l'implémentation peut être totalement différente d'un serveur à un autre, c'est pourquoi il a été nécessaire de définir une interface normalisée permettant d'accéder de façon standard aux différents services de l'annuaire. C'est le but du protocole LDAP (*Lightweight Directory Access Protocol*), dont le rôle est de fournir uniquement un moyen unique (standard ouvert) d'effectuer des requêtes sur un annuaire (compatible LDAP).

ii) Présentation de LDAP

LDAP (ou *Lightweight Directory Access Protocol*, traduisez *Protocole d'accès aux annuaires léger*) est un protocole standard permettant de gérer des annuaires, c'est-à-dire d'accéder à des bases d'informations sur les utilisateurs d'un réseau par l'intermédiaire de protocoles TCP/IP.

A partir de 1995, LDAP est devenu un annuaire natif (*standalone LDAP*), afin de ne plus servir uniquement à sa propre base de données mais aussi aux autres annuaires compatibles LDAP. Le protocole LDAP définit la méthode d'accès aux données sur le serveur au niveau du client.

- **Modèle d'information**

Le modèle d'information du protocole LDAP définit le type de données pouvant être stocké dans l'annuaire LDAP.

On appelle ***entrée*** l'élément de base de l'annuaire. Chaque entrée de l'annuaire LDAP correspond à un objet abstrait ou réel (par exemple une personne, un objet matériel, des paramètres, ...). Une entrée est constituée de plusieurs **objets**.

Un objet est constitué d'un ensemble de paires clés/valeurs appelées **attributs** permettant de définir de façon unique les caractéristiques de l'objet à stocker.

***Les attributs* :** chaque entrée est constituée d'un ensemble d'attributs (paires clé/valeur) permettant de caractériser l'objet que l'entrée définit.

Attribut	**Description**
c	country : Code du pays en deux lettres (respectant le standard ISO 3166)
dc	Domain Component : Suffixe d'un arbre DIT
cn	common Name : Nom de l'objet
o	organizational : Nom de l'organisation
objectClass	Classe d'objets
ou	organizational unit ou Unité organisationnelle (branche de l'organisation)
sn	surname : Nom de famille de la personne
uid	user identifier : Identifiant unique de l'objet
userPassword	Mot de passe de l'utilisateur

Tableau 2.1 **: Syntaxes d'attributs du protocole LDAP v3 [14]**

***Les classes d'objets* :** par analogie avec la terminologie objet on parle de *classe d'objet* pour désigner la structure d'un objet, c'est-à-dire l'ensemble des attributs qu'il doit

comporter. De cette façon on dit qu'un objet est une "instanciation" de la classe d'objet, c'est-à-dire un ensemble d'attributs avec des valeurs particulières. Une classe d'objet est ainsi composée d'un ensemble d'attributs obligatoires (soulignés) et éventuellement des attributs facultatifs. La figure suivante montre quelques classes d'objets LDAP standards.

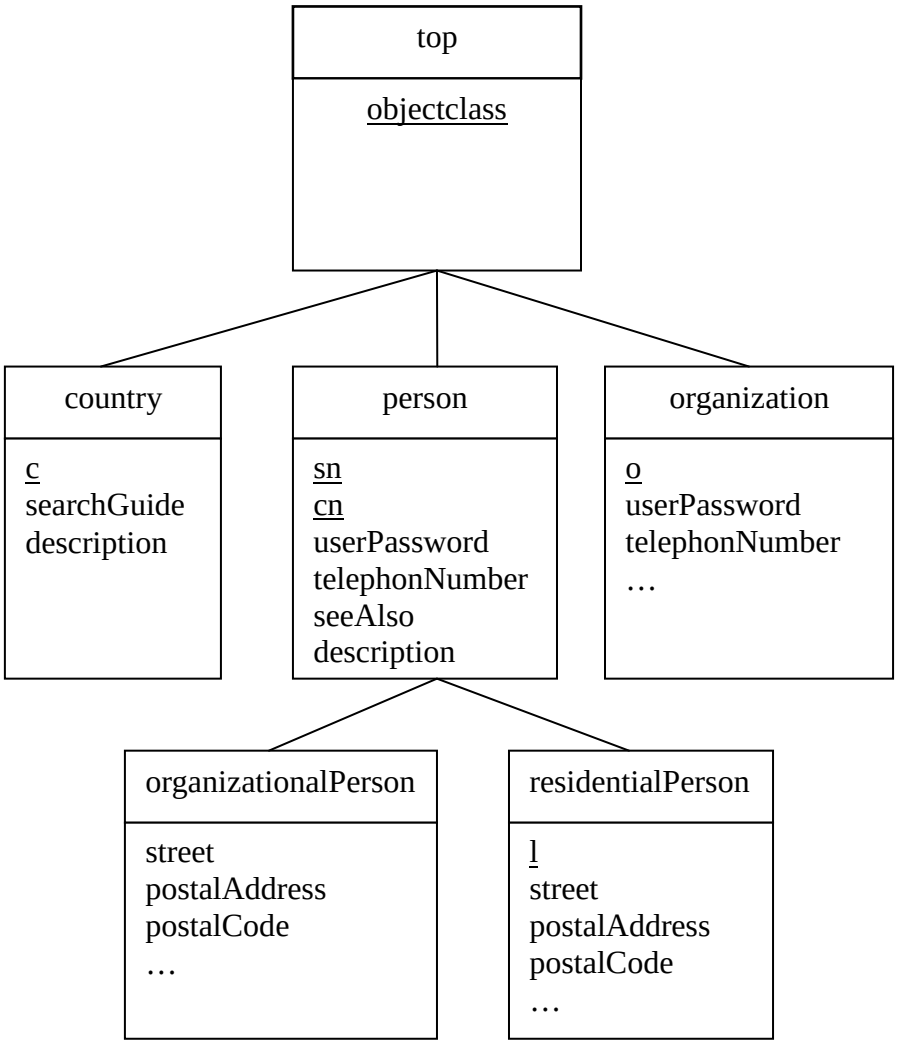

Figure2.6 : **Classes d'objets standards**

– **Modèle de nommage**

Le modèle de nommage a pour but de définir la façon selon laquelle les objets de l'annuaire sont nommés et classés. Ainsi les objets LDAP sont classés **hiérarchiquement** et possèdent un espace de nom homogène.

Le Directory Information Tree (DIT)

Les données LDAP sont structurées dans une arborescence hiérarchique sous forme d'un arbre appelé « DIT ». Chaque noeud de l'arbre correspond à une entrée de l'annuaire. Le sommet de l'arbre est appelé DIT et contient la racine ou suffixe. Les entrées correspondent à des objets abstraits ou issus du monde réel, comme une personne, une imprimante, ou des paramètres de configuration. Chaque noeud de l'arbre correspond à un objet pouvant appartenir à n'importe quelle classe d'objets à tout niveau. Cela signifie qu'il est possible d'utiliser n'importe quelle classe comme racine de l'arbre ou encore qu'une classe d'objets peut être utilisée à n'importe quel niveau de la hiérarchie.

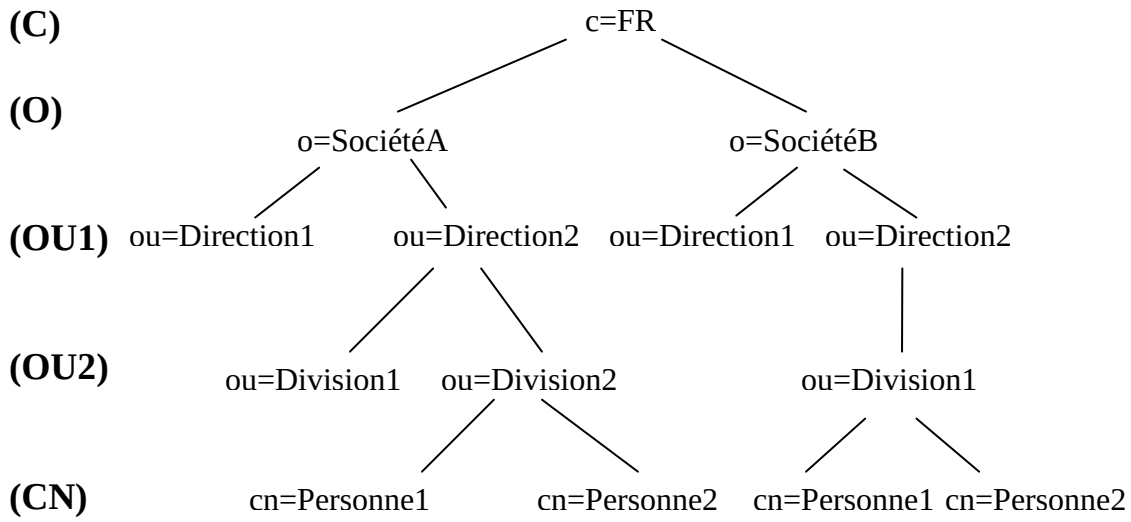

Figure2.7 : **Directory Information Tree [1]**

La désignation des entrées

La norme LDAP v3 permet de désigner un objet de deux façons : grâce à son nom relatif (**RDN** - *Relative Distinguished Name*) et grâce à son nom absolu (**DN** - *Distinguished Name*)

Un **RDN** est composé d'une (ou plusieurs) paire(s) de clé/valeur (attribut).Ainsi, un RDN sera de la forme : cn=Pillou ou bien c=fr.
Un RDN doit respecter certains critères : il doit être un nom unique dans la branche de l'objet (à un même niveau), Il peut être composé d'un ensemble d'attributs et un objet ne doit posséder qu'un et un seul RDN.

Un **DN** d'un objet est un moyen d'identifier de façon unique un objet dans la hiérarchie. C'est la concaténation de l'ensemble des RDN de ses ascendants hiérarchiques. Aussi, une entrée indexée par DN peut être identifiée de manière unique dans l'arborescence. Ainsi un *Distinguished Name* de l'objet Personne1 sera de la forme :

dn : cn=Personne1, ou=Division2, ou=Direction2, o=SociétéA, c=fr

Chapitre 3 : MODELE DE CONFIGURATION ET DEPLOIEMENT RESEAU

Il existe plusieurs stratégies de sécurité mais, pour le réseau au Campus Universitaire de Vontovorona, on estime que la sécurité des réseaux Wi-Fi s'appuie sur trois techniques: le **firewall,** le **cryptage** et l'**authentification** avec **un annuaire** sécurisé.

Pour les firewalls, on utilise deux **PC** fonctionnant sous Linux afin de protéger le réseau contre les éventuelles attaques provenant de la connexion sans-fil et celle de l'Internet.

Concernant le cryptage, on propose le protocole de sécurité **WPA2-EAP** avec l'algorithme **AES** pour protéger la communication filaire et sans-fil. WPA2 est la version de la norme IEEE 802.11i certifiée par le Wi-Fi Alliance. Il utilise le support de chiffrement AES (Advanced Encryption Standard) qui est un algorithme de cryptage très puissant. En plus de la technique de cryptage, WPA2 impose l'authentification EAP et nécessite un serveur d'authentification.

Pour le serveur chargé de l'authentification, on installe le **serveur RADIUS** (Voir le chapitre2 pour le principe RADIUS). Ce serveur authentifie les utilisateurs avec la méthode EAP-PEAP MS-CHAPv2. Le serveur d'authentification RADIUS doit être relié à une sorte de base de données sécurisée plus rapide en lecture pour trouver facilement les données nécessaires à l'authentification des utilisateurs.

Ainsi, l'utilisation d'un **annuaire LDAP** est essentielle afin de stocker, protéger et gérer les informations nécessaires à l'authentification des utilisateurs (login/mot de passe).
Le chapitre2 détaille les informations sur l'annuaire LDAP.

L'architecture réseau sécurisé au campus universitaire de Vontovorona est donc illustrée par la figure 3.1. Tous les utilisateurs du réseau filaire et sans-fil doivent être authentifiés avant l'usage du réseau. Les supplicants (clients) du réseau filaire sont authentifiés par l'intermédiaire d'un Switch ou commutateur 802.1x. L'authentification est effectuée par un serveur RADIUS utilisant un annuaire LDAP pour stocker les informations concernant les utilisateurs (login/mot de passe). On utilise la clé WPA2 avec le technique de

cryptage des trames AES et la méthode d'authentification EAP-PEAP MS-CHAPv2. On peut aussi installer un firewall comme si le point d'accès était une connexion Internet. On considère ici que tout le réseau Wi-Fi est étranger au réseau filaire local, au même titre qu'Internet. Donc, pour la protection du réseau filaire, on installe deux firewalls dont le premier protège contre les attaques venant de l'Internet et le second contre les éventuels piratages de la connexion sans-fil.

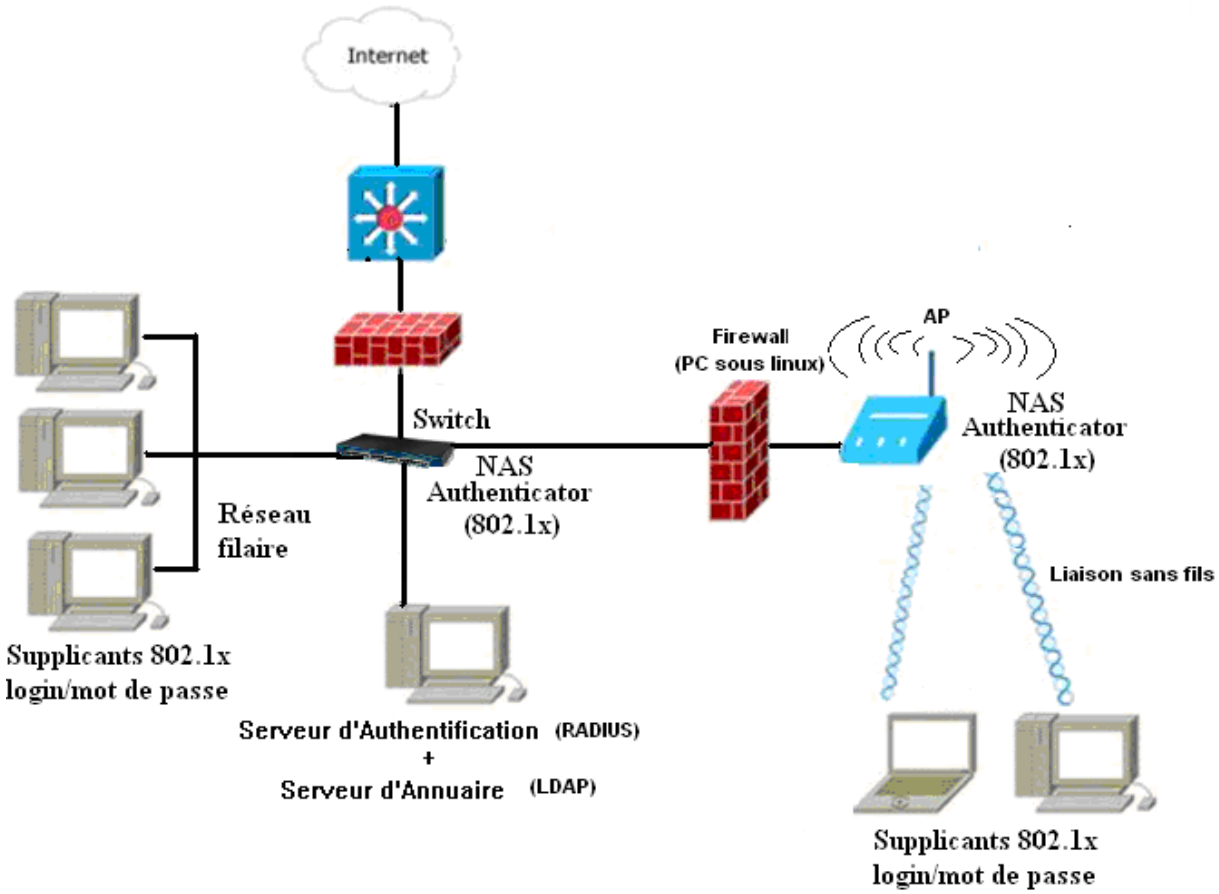

Figure 3.1 : **Réseau filaire et Wi-Fi sécurisé**

En raison de l'absence de matériels, la réalisation du Firewall et passerelle n'est pas possible pour la pratique. Néanmoins, dans le premier paragraphe, un modèle de configuration pour ces deux techniques a été déposé à titre de référence. Et dans le deuxième paragraphe se trouve la réalisation pratique pour simuler le réseau.

3.1 MODELE DE CONFIGURATION

Prenons un exemple de configuration du réseau dans le Centre Informatique Salle n°1. Cet exemple sert de modèle de référence pour la configuration des matériels dans tous les autres réseaux des départements, service administratif et le Cybercafé. La figure ci-dessous montre l'architecture du réseau dans le Centre Informatique salle n°1.

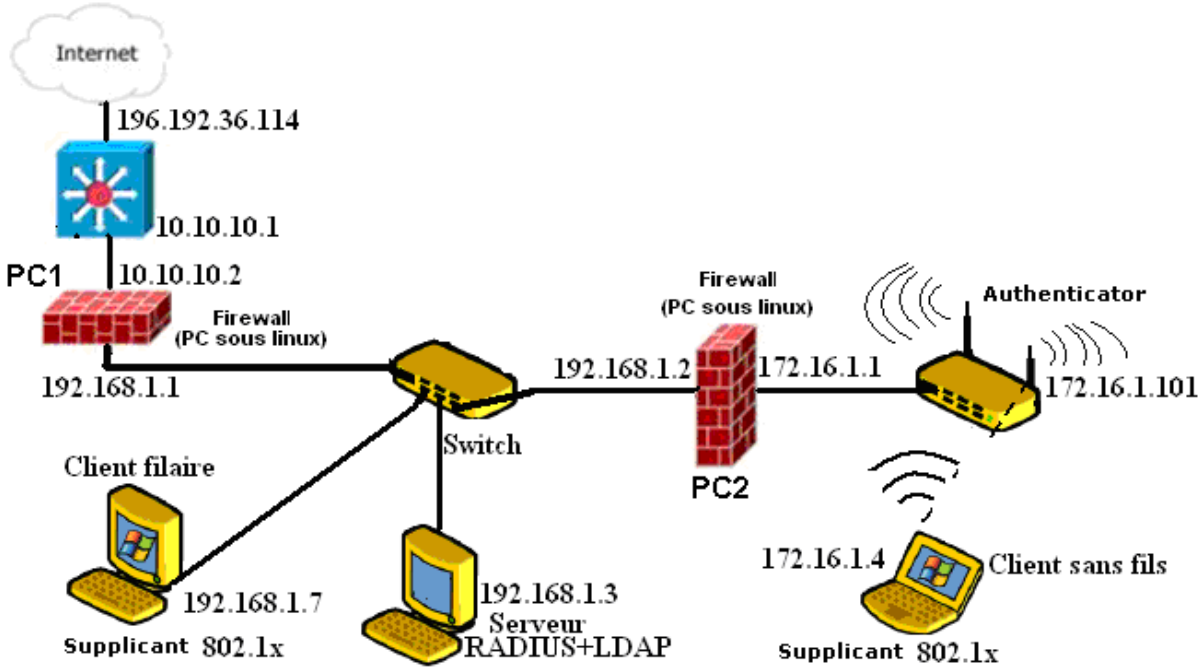

Figure 3.2 : **Architecture du réseau au Centre Informatique Salle n°1 [15]**

a. Firewall

D'après la figure 3.2, on utilise deux firewalls nommés **PC1** et **PC2**. On va fixer les politiques de sécurités suivantes:

– **Les deux firewalls sur PC1 et PC2**

- Par défaut, on refuse tout trafic qui ne correspond à aucune règle.

 # iptables –P INPUT DROP

 # iptables -P OUTPUT DROP
 # iptables -P FORWARD DROP

- On accepte tout paquet passant par le firewall à destination ou à source du port 21(port ftp), du port 80 (port d'accès au Web)

 # iptables -A FORWARD -p tcp -m multiport --dport 21,80 -j ACCEPT
 # iptables -A FORWARD -p tcp -m multiport --sport 21,80 -j ACCEPT

– **Le firewall sur PC2**

On accepte le paquet traversant la machine et qui utilise le port 1812 pour l'authentification Radius.

 # iptables -A FORWARD -p tcp --sport 1812 -j ACCEPT
 # iptables -A FORWARD -p tcp --dport 1812 -j ACCEPT

b. <u>Passerelle</u>

La passerelle est une machine possédant deux cartes réseaux (ici, on note **eth0** et **eth1**) et fonctionnant sous le système d'exploitation Linux.

– **La passerelle sur PC2**

- On attribue ainsi l'adresse IP pour les deux cartes de la passerelle :

 # ifconfig eth0 192.168.1.2 netmask 255.255.255.0 up
 # ifconfig eth1 172.16.1.1 netmask 255.255.255.0 up

- Puis activer l'IP Forwarding :

 # echo ‘‘1’’ >/proc/sys/net/ipv4/ip_forward

L'activation du Forwarding permet au réseau filaire de communiquer avec les réseaux sans-fil. Cela consiste à établir une connexion entre les deux interfaces qui se trouvent sur deux réseaux différents.

- Construction de la table de routage

 # route add default gw 192.168.1.1

Cette commande ajoute une route par défaut qui, si aucune route ne convient, sera utilisée pour envoyer les paquets vers le PC1.

– **La passerelle sur PC1**

- On attribue l'adresse IP :

 # ifconfig eth0 10.10.10.2 netmask 255.255.255.0 up

 # ifconfig eth1 192.168.1.1 netmask 255.255.255.0 up

- Activation de l'IP Forwarding :

 # echo ''1'' >/proc/sys/net/ipv4/ip_forward

- Table de routage

 # route add default gw 10.10.10.1

 # route add -net 172.16.1.0 netmask 255.255.255.0 gw 192.168.1.2

Elle permet de rejoindre l'extérieur au réseau sans-fil.

3.2 DEPLOIEMENT RESEAU

Dans ce paragraphe, en adaptant la situation suivant les matériels qui existe, on va simuler la réalisation pratique du réseau. Le but est de fournir une connexion Internet à un client sans-fil en les authentifiant avant l'usage effectif du réseau. Voici les différents matériels disponibles avec leurs fonctions pour la simulation du réseau :

- Un PC de bureau fonctionnant sous Linux (Debian3.1) pour Serveur d'authentification RADIUS avec LDAP.

- Un PC de bureau sous Windows XP SP2 hébergeant des pages Web pour jouer le rôle d'Internet.

- Un point d'accès de type D-Link DWL-2100AP pour le NAS ou Authenticator.

- Un PC portable sous Windows XP SP2 équipé d'une carte Wi-Fi joue le rôle d'un client ou supplicant 802.1x. Ci-dessous, la figure qui illustre la simulation :

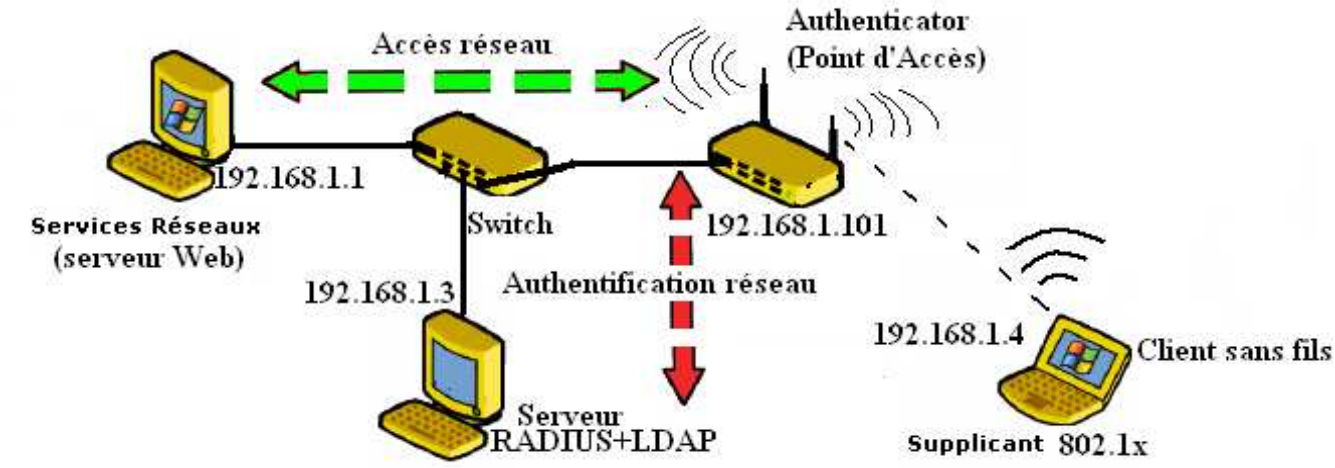

Figure 3.3 : **Simulation réseau**

a. Authenticator

Pour l'Authenticator, on va configurer le point d'accès de type DWL-2100AP en tenant compte de la sécurisation du réseau. C'est le seul AP disponible, il possède les caractéristiques suivantes :

- Standard 802.11g 2,4GHz
- Transmission ultra-rapide pouvant atteindre une vitesse de 108Mbps (en mode Turbo)

- Port 10/100BASE-TX pour connexion à Ethernet ou à DSL/câble modem
- Compatible avec les équipements 802.11b sans fil existants
- Serveur DHCP intégré
- 5 modes de fonctionnement : AP, client AP, point à point, point à multipoint, répéteur
- Encryptage de données WEP 64/128/152 bits
- Sécurité WPA avec authentification RADIUS 802.1x de l'utilisateur
- Configuration et gestion à partir du web

Cet AP dispose déjà d'une adresse IP par défaut 192.168.0.50. Il possède un port rj45 pour la mise en réseau prévue pour sa configuration. Après avoir branché en réseau cet AP avec un PC (adresse : 192.168.0.1) à l'aide d'un câble Ethernet croisé, une fenêtre apparaît. Taper « admin » pour l'utilisateur et laisser vide le mot de passe. Ensuite, un serveur web embarqué dans un AP (figure 3.4) apparaît à l'écran :

Figure 3.4 : **Serveur web embarqué dans un AP**

Voici les phases d'opération à réaliser pour sa configuration :

- Cliquer sur l'onglet « Tools », modifier le nom d'utilisateur et le mot de passe par défaut.

- Ensuite, sélectionner l'onglet « Home » puis « LAN » et modifier l'adresse IP à 192.168.1.101.

- Pour la sécurité du réseau, sélectionner l'onglet « Wireless », modifier le nom du SSID (espa dans cette pratique) et désactiver son émission. Choisir l'authentification WPA2-EAP et le type de chiffrement AES. Taper 192.168.1.3 pour le serveur RADIUS et compléter la case pour RADIUS secret.

b. Supplicant

On a installé une carte Wi-Fi au format USB et de type WG2000/R. Cette carte sans-fil possède les caractéristiques suivantes : standard 802.11g et 802.11b, sécurité WPA2 et 802.1x, débit maximum de 54Mbps. La carte Wi-Fi est livrée avec un CD d'installation fonctionnant sous Windows XP. La version de Windows sur nos PC est SP2.

Après avoir installé le CD d'installation, on branche la carte et une fenêtre de configuration (figure 3.5) apparaît à l'écran. Pour configurer le réseau sans-fil, il faut cliquer sur le bouton « Add » puis renseigner le SSID. Après il faut sélectionner l'onglet « Authentification and security ». Choisir l'authentification WPA2 et le cryptage AES. Cliquer sur le bouton « 802.1x settings» et choisir le type d'authentification PEAP et le tunnel d'authentification MSCHAP-v2 et par la suite, il faut valider toutes ces modifications.

Enfin, il faut modifier l'adresse de la carte réseau par 192.168.1.4. L'instruction pour l'affectation d'adresse pour cette carte Wi-Fi est identique à celle de la carte filaire.

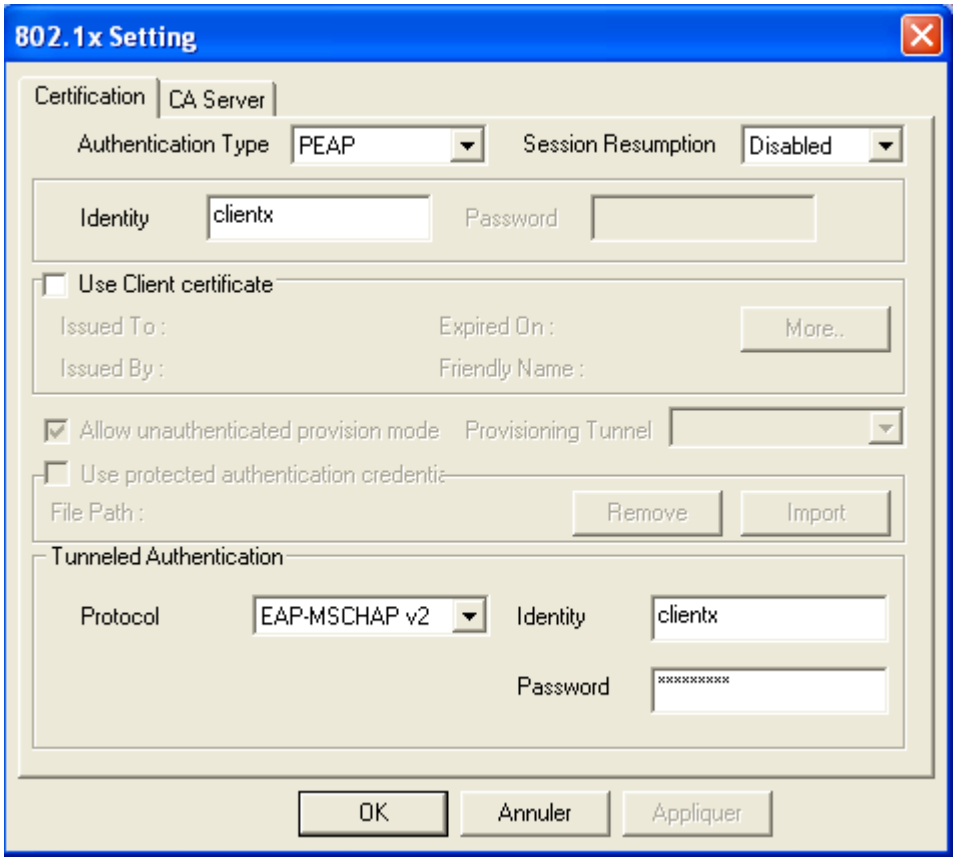

Figure 3.5 : **Paramètres du réseau sans-fil**

c. Serveur RADIUS avec LDAP

i) serveur RADIUS

- **Installation**

Sur un PC fonctionnant sous Linux Debian 3.1 sarge, on a installé un serveur RADIUS appelé FreeRADIUS. C'est une implémentation open source du protocole Radius. Elle supporte le protocole d'authentification **EAP** : PEAP, MSCHAPV2, MD5, SIM TLS TTLS, LEAP, GTC. Le serveur Freeradius peut être utilisé avec 5 types de base de données qui sont : LDAP, MYSQL, PostgresSQL, Oracle, SAMBA.

La version téléchargée est freeradius-1.0.2.tar.gz. Avant l'installation de FreeRadius, afin d'éviter des erreurs sur la compilation, il faut installer les bibliothèques Libssl-dev, Snmp et Libltdl3-dev à l'aide de la commande :

~# apt-get install libssl-dev snmp libltdl3-dev

Après, installer **openssl-0.9.7g.tar.gz** pour la génération des certificats, et il faut éditer le fichier openssl.conf qui se trouve dans /usr/local/openssl/ssl pour la configuration des certificats. Il y a plusieurs éditeurs de texte pour éditer ce fichier, comme **vi** par exemple :

~# Vi /usr/local/openssl/ssl/openssl.cnf

Pour générer les certificats, il faut chercher et exécuter le script **CA.all**. L'exécution de ce script crée 9 fichiers et un dossier qui est demoCA. Après l'installation du serveur RADIUS, ces 9 fichiers et ce dossier demoCA.all doit être copiés dans /etc/raddb/certs/.

Ensuite, on procède à l'installation du freeradius. Pour la configuration de compilation de FreeRadius, on utilise le paramètre *--sysconfdir=/etc/* qui placera tous les fichiers de configuration dans */etc/raddb*, le paramètre *--silent* permet d'afficher le debug minimum. On tape donc:

~#tar zxvf freeradius-1.0.2.tar.gz

~# cd freeradius-1.0.2

~#./configure –-sysconfdir=/etc/ --silent -–disable-shared

Après, il faut compiler et installer le serveur freeradius

~# make

~# make install

Le démarrage du serveur freeradius se fait en mode debug par :

radiusd –X -A

- **Configuration**

Les fichiers de configuration sont dans /etc/raddb. C'était le chemin précisé précédemment via le paramètre –sysconfdir lors de la compilation.

On configure les fichiers suivants :

clients.conf pour la configuration des NAS (bornes Wi-fi) autorisés à contacter le Radius.

users pour la configuration des utilisateurs autorisés.

eap.conf pour la configuration de EAP.

radiusd.conf le fichier principal de configuration de freeradius.

Les détails sur l'installation et configuration se trouvent dans l'Annexe2.

ii) Serveur LDAP

- **architecture de l'annuaire**

Le but est de mettre en place un serveur OpenLDAP afin que le serveur RADIUS puisse chercher les utilisateurs avec ses mots de passe et profiles dans un annuaire.

Les utilisateurs du réseau au campus universitaire de Vontovorona se groupent en deux organisations : les enseignants dans chaque département et les personnels des différents services. Les profiles de réseau sont WLAN (Wi-Fi) et LAN (filaire).

Pour gérer les utilisateurs via ses profiles, l'annuaire est organisé suivant la figure ci-dessous :

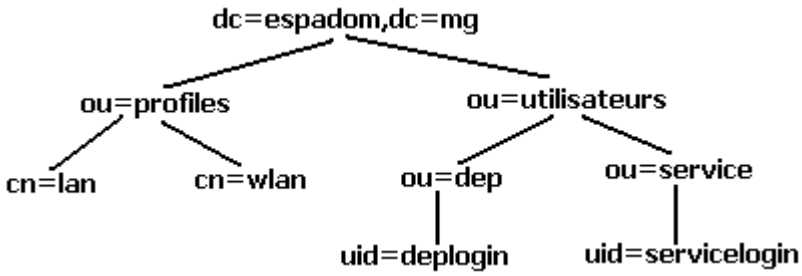

Figure 3.6 : **Organisation de l'annuaire**

Les étapes sur l'installation et création de l'annuaire LDAP sont détaillées dans l'Annexe3

– **Association LDAP avec RADIUS**

Par défaut**,** le serveur freeradius n'est pas compilé avec LDAP. Donc, on doit compiler le module **rlm_ldap :**

$ apt-get install libldap2-dev

Après il faut aller dans le répertoire /freeradius1.0.2/modules/rlm_ldap puis lancer les commandes suivantes :

$ ./configure

$ make

make instal

Et on va reconfigurer radiusd.conf :

```
ldap {
        server = "127.0.0.1"
        identity = "cn=admin,dc=espadom,dc=mg"
        password = passldap
        basedn = "dc=espadom,dc=mg"
        filter = "(uid=%{Stripped-User-Name:-%{User-Name}})"
        base_filter = "(objectclass=radiusprofile)"
        start_tls = no
        access_attr = "dialupAccess"
        ldap_connections_number = 5
        password_attribute = userPassword
        groupname_attribute = cn
```

```
        groupmembership_filter="(|(&(objectClass=GroupOfNames)
        (member=%{Ldap-UserDn}))
        (&(objectClass=GroupOfUniqueNames)(uniquemember=%{Ldap-UserDn})))"
        groupmembership_attribute = radiusGroupName
        timeout = 4
        timelimit = 3
        net_timeout = 1
    }
Authorize {
        [...]
        ldap
        checkval
        [...]
    }
```

Puis, éditer le fichier /etc/raddb/ldap.attrmap : ce fichier contient le mappage des noms de variables Radius à faire correspondre avec celle de LDAP, ce qui nous intéresse ici c'est de récupérer l'attribut LDAP userPassword et de le stocker dans la variable RADIUS Password. On met donc :

```
\begin{verbatim}
checkItem    Password                    userPassword
\end{verbatim}
```

CONCLUSION

Avec l'émergence de la technologie Wi-Fi, l'Ecole Supérieure Polytechnique d'Antananarivo bénéficie, en matière de réseaux informatiques, d'une solution très économique et simple à mettre en œuvre. Mise en application, cette technologie répond aux attentes des utilisateurs en simplifiant radicalement les problèmes de câblage, de nomadisme et de flexibilité dans l'organisation des outils de travail. En outre, la réutilisation du câblage existant reste une alternative souvent techniquement irréalisable.

Cependant, si le Wi-Fi a encore de beaux jours devant lui, il ne présente, pour autant, pas que des avantages. Son utilisation présente de gros risque au niveau de la sécurité rendant ce type de communication peu sûr. Ainsi, ce mémoire constitue, soit disant, un complément d'une étude de mise en place d'un réseau Wi-Fi au Campus Universitaire de Vontovorona, qui fait déjà objet d'une recherche menée par mon cher collègue. Il pourra contribuer à l'amélioration de la performance des réseaux Wi-Fi étant donné la prise en considération des divers risques à encourir et des solutions de mesures possibles à appliquer.

En utilisant le serveur RADIUS, on pourra centraliser l'authentification des utilisateurs et avec le serveur LDAP, on visera à gérer les annuaires qui contiennent les informations nécessaires concernant ces derniers. Dans tous les cas, l'application des techniques de cryptage semble incontournable. Pour terminer, l'ajout de firewalls (pare-feu) augmentera le niveau de sécurité en isolant le réseau des éventuelles attaques.

Annexe1: GENERATION DES CERTIFICATS

A1.1 INSTALLATION DE OPENSSL

Pour générer les certificats, on va installer OpenSSL. La version utilisée est **openssl-0.9.7g.tar.gz.** L'installation de openssl se fait via les commandes suivantes :

```
~# tar zxvf openssl -0.9.7g.tar.gz
~# cd openssl -0.9.7g
~# ./config --prefix=/usr/local/openssl shared
~# make  && make install
```

A1.2 GENERATION DES CERTIFICATS

~# Vi /usr/local/openssl/ssl/openssl.cnf

Les paramètres à modifier sont :

```
countryName_default = AF
stateOrProvinceName_default = MADAGASCAR
localityName_default = TANANARIVE
0.organizatio
nName_default = ESPA
organizationalUnitName_default = polytech
commonName_default = admin
emailAddress_default = pardefault@espa.com
challengePassword_default = whatever
```

Plusieurs méthodes permettent de générer les certificats. L'une d'entre elles est d'utiliser le script CA.all fourni par freeradius. Ce script utilise le fichier openssl.conf déjà configuré précédemment. Le fichier CA.all se trouve dans un sous répertoire nommé scripts du freeradius. Pour le trouver facilement, il faut taper la commande suivante :

~# find / -name CA.all

L'exécution du script CA.all crée 9 fichiers et un dossier qui est demoCA. Il faut copier ces 9 fichiers et ce dossier demoCA.all dans /etc/raddb/certs/.

Annexe2 : INSTALLATION DE FREERADIUS

A2.1 INSTALLATION

~# apt-get install libssl-dev snmp libltdl3-dev
~#tar zxvf freeradius-1.0.2.tar.gz
~# cd freeradius-1.0.2
~#./configure –-sysconfdir=/etc/ --silent -–disable-shared
~# make
~# make install

Il faut aller dans /etc/raddb/, puis effacer les certificats par défaut de FreeRadius, après copier notre certificat root et serveur dans le dossier certs. Enfin, générer les fichiers random & dh avec la fonction date.

radius: # cd /etc/raddb/certs/
radius:/etc/raddb/certs# rm -rf *
radius:/etc/raddb/certs# cp /root/certs/root.pem /etc/raddb/certs
radius:/etc/raddb/certs# cp /root/certs/serveur.pem /etc/raddb/certs
radius:/etc/raddb/certs# date > random
radius:/etc/raddb/certs# date > dh

A2.2 CONFIGURATION

Les fichiers de configuration sont dans /etc/raddb. Les fichiers suivants doivent être configurés : clients.conf, users ,eap.conf et radiusd.conf.

a) clients.conf

Ce fichier permet de définir la liste des AP qu'il faut autoriser pour accéder au serveur Radius. Le serveur et l'AP partagent un secret (une clé) pour crypter les données.

Par défaut, le localhost (127.0.0.1) est autorisé avec comme secret : *testing123* (pour réaliser des tests en local).

Pour rajouter notre borne Wi-fi avec comme adresse IP 192.168.1.101
AP_client 192.168.1.101 {
secret = secretradius
shortname = AP2100
nastype = other
}

On a une clé partagée entre l'AP et le serveur qui sera secretradius et on lui donne le nom AP2100 via shortname (utile pour le debug).

b) users

Le fichier users doit être configuré pour qu'il puisse utiliser l'annuaire LDAP. Pour ce faire, ajouter les lignes suivantes :

DEFAULT LdapGroup ==wlan, UserProfile := "cn=wlan,ou=profiles,dc=espadom,dc=mg"
FallThrough = yes

c) eap.conf

Dans ce fichier, spécifier que l'on veut utiliser EAP-PEAP et non MD5 à la ligne 22 :

default_eap_type = peap

Ensuite, configurer TLS, il faut enlever les commentaires (les # devant) à partir de la ligne 122.

```
tls {
        […]
}
```

d) radiusd.conf

Voici les lignes d'instructions modifiées dans le contenu de fichier radiusd.conf :

```
server = "localhost"
identity = "cn=admin,dc=espadom,dc=mg"
password = passldap
basedn = " dc=espadom,dc=mg "
filter = "(uid=%{StrippedUserName:-%{UserName}})"
base_filter = "(objectclass=radiusprofile)"

groupname_attribute = cn
groupmembership_filter=
"(|(&(objectClass=GroupOfNames)(member=%{LdapUserDn}))(&(
objectClass=GroupOfUniqueNames)(uniquemember=%{LdapUserDn})))"
groupmembership_attribute = radiusGroupName
```

Annexe3 : INSTALLATION OPENLDAP

A3.1 INSTALLATION

Tout d'abord, il faut chercher les paquets OpenLDAP à l'aide de la commande:

apt-cache search openldap

Puis on installe les paquets OpenLDAP selon ce qui est disponible sur la machine :

apt-get install libiodbc2 libldap-2.2-7 slapd ldaputils

On va répondre les questions pendant l'installation de la manière suivante :

Entrer le nom de domaine DNS	**espadom.mg**
Entrer le nom de l'organisation	polytech
Password de l'admin LDAP	**passldap**
Autoriser le protocole v2	**Oui**

A3.2. CREATION D'UN ANNUAIRE

La création d'un annuaire se fait à partir d'un fichier *LDIF (LDAP Data Interchange Format). LDIF* est un format standardisé d'échange de données, qui permet la représentation des données contenues dans un annuaire LDAP. Un fichier *LDIF* est décrit ci-dessous:

####################CREATION D'UN ANNUAIRE#########################

```
#creation d'une groupe utilisateurs
dn: ou=utilisateurs,dc=espadom,dc=mg
objectClass: organizationalUnit
ou: utilisateurs

#creation d'une organisation profiles
dn: ou=profiles,dc=espadom,dc=mg
objectClass: organizationalUnit
ou: profiles

#creation d'une section dep
dn: ou=dep,ou=utilisateurs,dc=espadom,dc=mg
objectClass: organizationalUnit
ou: dep
#creation d'une section service
dn: ou=service,ou=utilisateurs,dc=espadom,dc=mg
objectClass: organizationalUnit
ou: service
#creation d'un utilisateur  de la section dep nommée deplogin
dn: uid=deplogin,ou=utilisateurs,dc=espadom,dc=mg
objectClass: person
objectClass: inetOrgPerson
objectClass: radiusProfile
sn: deploginsn
userPassword: passdeplogin
```

```
cn: deplogin
radiusGroupName: wlan
uid: deplogin
dialupAccess: ok

#creation d'un utilisateur  de la section dep nommée servicelogin
dn: uid=servicelogin,ou=utilisateurs,dc=espadom,dc=mg
objectClass: person
objectClass: inetOrgPerson
objectClass: radiusProfile
sn: serviceloginsn
userPassword: passservicelogin
cn: servicelogin
radiusGroupName: wlan
uid: servicelogin
dialupAccess: ok

#creation d'un profil: wlan
dn: cn=wlan,ou=profiles,dc=espadom,dc=mg
objectClass: person
objectClass: inetOrgPerson
objectClass: radiusProfile
cn: wlan
uid: wlan
sn: wlan
radiusAuthType: EAP
radiusGroupName: wlan

#creation d'un profil: lan
dn: cn=lan,ou=profiles,dc=espadom,dc=mg
objectClass: person
objectClass: inetOrgPerson
objectClass: radiusProfile
cn: lan
uid: lan
sn: lan
radiusAuthType: EAP
radiusGroupName: lan
```

Une fois le fichier *LDIF* créé, il suffit d'importer ce fichier au sein de l'annuaire.

En mode terminal, et en tant que administrateur (root), frapper la commande :

```
# ldapadd -x -D "cn=admin,dc=espadom,dc=mg" -W -f base_espadom.ldif
```

Vérifier si l'annuaire a été bien rempli :

```
# ldapsearch -x -b 'dc=espadom,dc=mg' '(objectclass=*)'
```

REFERENCES BIBLIOGRAPHIQUES

[1] Site CommentCaMarche.net - "Les réseaux sans-fil" et "Le Wi-Fi"

[2] http://www.fr.wikipedia.org.com

[3] http://www.techniquesingenieur.fr/rubrique/reseaux_locaux_et_reseaux_sans_fil/

[4] Cours E435, « Réseau local», Dept Electronique, ESPA, Année 2007-2008

[5] http://www.blackalchemy.to/project/wifi.pdf

[6] http://www.arubanetworks.com

[7] Cours E558 IA, « Cryptographie », Dept Electronique, ESPA, Année 2008-2009

[8] Cours E510 « Administration système », Dept Electronique, ESPA, Année 2008-2009

[9] http://www.ietf.org/rfc/rfc2868.txt

[10] http://www.untruth.org/~josh/security/radius/radius-auth.html

[11] 802.1x : Solution d'authentification sécurisée du réseau sans fil de l'Université Louis http://2003.jres.org/actes/paper.143.pdf

[12] Protocoles d'authentification réseau - S. Bordères http://raisin.u-bordeaux.fr/

[13] http://www.ietf.org/rfc/rfc3579.txt

[14] http://www.ietf.org/rfc/rfc2251.txt

[15] J.B.Andrianonimpanirimbololona, Mise en place d'un réseau Wi-Fi au Campus Universitaire de Vontovorona, Mémoire de fin d'études, Dept Electronique-ESPA ,2008-2009

Auteur : ANDRIAMANOHISOA Eliot Josélito

Titre : « Sécurisation d'un réseau Wi-Fi au Campus Universitaire de Vontovorona »

Nombre de pages : 49

Nombre de figures : 20

Nombre de tableaux : 04

Ce travail de mémoire montre une approche sécurité réseau, cas des Wi-Fi, au Campus Universitaire de Vontovorona. Il illustre la technologie des réseaux Wi-Fi et après avoir étudié leurs caractéristiques, diverses problématiques seront exposées mais pour y pallier, des mesures de sécurité sont proposées. On peut citer entre autres : le cryptage et firewall, la mise en place d'un serveur d'authentification RADIUS utilisant l'annuaire LDAP.

Mots Clés : Réseau sans fils, Wi-Fi, 802.11, Sécurité réseau, 802.1x, RADIUS, LDAP

Rapporteur : Monsieur RAKOTONDRASOA Justin

Adresse de l'auteur : Lot K4/072 Ter Ivato-Aéroport 105