Abréviations

A

AAA: Authentication, Authorization, Accounting

ACL: Access Control List

AES: Advanced Encryption Standard

AP: Access Point

B

BLR: Boucle Locale Radio.

BSS: Basic Service Set

BSSID: BSS Identifier

C

CA: Certification Authority

CCM: Counter with CBC-MAC

CCMP: Counter with CBC MAC Protocol

CHAP: Challenge Handshake Authentication Protocol

CRC: Control Redundancy Check

D

DECT: Digital Enhanced Cordless Telecommunication

DES: Data Encryptions Standard

DN: Distinguished Name

DoS: Denial of Service

DS: Distribution System

DSSS: Direct Sequence Spred Spectrum

E

EAP: Extensible Authentification Protocol

EAP-AKA: EAP - Authentification and Key Agreement

EAP-MD5: EAP-Message Digest 5

EAP- SIM: EAP - Subsciber Identity Module

EAP- SKE: EAP-Shared Key Exchange

EAP-TLS: EAP-Transport Layer Security

EAP-TTLS: EAP-Tunneled Transport Layer Security

EAPOL: Extensible Authentification Protocol Over Lan

EEPROM: Electrically Erasable Programmable Read-Only Memory

ESS: Extended Service Set

ETSI: European Telecommunications Standards Institute

F

FHSS: Frequency Hopping Spread Spectrum

G

GPS: Global Positioning System

GPRS: General Packet Radio Service

GSM: Global System for Mobile Communications

H

HARQ: Hybrid Automatic Repeat reQuest

HiperLAN: Hiper Local Area Network

hiperLAN2: High Performance Radio LAN 2.0

Home RF: Home Radio Frequency

HR-DSSS: High Rate Direct Sequence Spread Spectrum

I

IBSS: Independent Basic Service Set

ICV: Integrity Check Value

IDEA: International Data Encryptions Algorithm

IEC: International Electrotechnical Commission

IEEE: Institute of Electrical and Electronics Engineer

IETF: Internet Engineering Task Force

IMT 2000: Norme du GSM

IP: Internet Protocol

IPv4: Internet Protocol version 4

IR: Infrarouges

ISO: International Organization for Standardization

IV: Vecteur d'initialisation

L

LAN: Local Area Network

LDAP: Lightweight Directory Access Protocol

LEAP: Lightweight Extensible Authentification Protocol

LLC: Logical Link Control

M

MAC: Medium Access Control

MAN: Metropolitan Area Network

MD5: Message Digest 5

MIC: Message Integrity Code

MIMO: Multiple Input Multiple Output

MS-CHAP 2: Microsoft Challenge Handshake Authentication Protocol version 2

N

NAS: Network Access Server

NTLM: NT Lan Manager

O

OCB: Offset Code Book

OFDM: Orthogonal Frequency Division Multiplexing

OID: Object Identifier

OSI: Open Source Inder

P

PAE: Port Access Entity

PAP: Password Authentication Protocol

PC: Personal Compute / Point of Coordination

PCI: Peripheral Component Interconnect

PCMCIA: Personal Computer Memory Card International Association

PDA: Personal Digital Assistant

PEAP: Protected EAP

PGP: Pretty Good Privacy

PIN: Personal Identification Number

PKA: Public Key Authentication

PPM: Pulse Position Modulation

PPP: Point to Point Protocol

PSK: Pré-Shared Key

R

RADIUS: Remote Authentification Dial In User Service

RC4: Ron's Code #4

RLC: Radio Link Control

RPV: Réseau Privé Virtuel

RSA: Rivest, Shamir, Adelman

S

SCTP: Stream Control Transmission Protocol

SIM: Subscriber Identity Module

SNMP: Simple Network Management Protocol

SRP: Secure Remote Password

SSID: Service Set Identifier

SSL: Secure Socket Layer

T

TACACS+: Terminal Access Controller Access Control System Plus

TCP: Transmission Control Protocol

TKIP: Temporal Key Integrity Protocol

TLS: Transport Layer Security

TSF: Transmission sans fil

TTLS: Tunneled TLS

U

UDP: User Datagram Protocol

UIT: Union internationale des télécommunications

UMTS: Universal Mobile Telecommunications System

USA: United States of America

USB: Universal Serial Bus

V

VPN: Virtual Private Network

WECA: Wireless Ethernet Compatibility Alliance

WEP: Wired Equivalent Privacy

Wi-Fi: Wireless Fidelity

Wi-Max: Worldwide Interoperability for Microwave Access

WMAN: Wireless Metropolitan Area Network

WPA2: Wi-Fi Protected Access version 2

WPAN: Wireless Personal Area Network.

WRAP: Wireless Robust Authenticated Protocol

WRAN: Wireless Regional Area Networks

WWAN: Wireless Wide Area Network.

Table des matières

Chapitre II : Mécanismes de sécurité des réseaux sans fil « Wi-Fi »

Chapitre III : Mise en place d'une sécurité basée sur le 802.1x et d'un serveur d'authentification

Résumé

Le réseau Wi-Fi constitue de plus en plus la technologie qui s'est imposée par excellence ces dernières dix années, permettant aux utilisateurs un accès à l'internet ou au réseau local d'entreprise ou personnel sans les contraintes des câbles. Les débits atteints actuellement avec le réseau wifi rendent possible le transfert de flux multimédia soumis cependant à une forte contrainte sécuritaire due au lien sans fil lui même. Les solutions utilisées dans les réseaux filaires ne sont pas adéquates et efficaces pour les WLAN. D'où l'intérêt certain apporté à trouver et mettre en place des solutions spécifiques au WLAN même si parfois elles sont inspirées de solutions existantes déjà.

Le but de notre projet de fin d'études consiste justement à étudier et analyser ces dites solutions pour en choisir et déployer la plus efficace sur un réseau test.

Dans cette optique, on a donc étudié le réseau Wi-Fi standardisé en détail, avec son fonctionnement ainsi que ses protocoles et ses mécanismes de sécurité. Nous avons ensuite opté pour l'utilisation d'un serveur RADIUS utilisant le protocole 801.1x pour l'authentification des utilisateurs avec des certificats, le protocole AES pour le chiffrement, et enfin le protocole TKIP pour la gestion et l'octroi de clés temporaires de chiffrement, qui devraient être le bon choix comme expliqué dans le chapitre deux.

Introduction générale

Les réseaux sans fil rencontrent aujourd'hui un succès important car ils permettent de déployer des moyens de transmission sans contrainte d'immobilité liée aux câblages et aux prises, la promotion actuelle de ce type de solution est uniquement axée sur les avantages qu'elle procure : facilité et rapidité d'installation, coût inférieur à un système filaire, mobilité, accès partagé à des services de haut débit.

Bien que cette technologie semble aux premiers abords parfaite et sans soucis, la réalité est plus dure, due surtout au problème de la protection de ces réseaux sans fil, même vis-à-vis d'attaque simple. La nature de signal transmis (ondes électro magnétiques) rend difficile, voir impossible la maitrise complète de la propagation. En conséquent, il est assez facile d'écouter les messages et même de s'introduire sur de tels réseau ; il est donc nécessaire de définir pour les réseaux sans fil une politique de sécurité stricte reposant sur des mécanismes, si possible sans failles, tel que l'authentification, le contrôle d'intégrité et le chiffrement.

Toutefois, les réseaux sans fil n'ont pas pour vocation de remplacer les réseaux filaires, ils sont plus souvent considérés comme une extension à un réseau filaire existant et non comme un potentiel remplaçant.

Le travail que nous présentons dans le cadre du projet de fin d'étude consiste à exposer en détail le déploiement d'une solution de sécurité des réseaux sans fil « Wi-Fi ». Notre travail va consister à sécuriser un réseau Wi-Fi en mode infrastructure, par un serveur d'authentification radius. Pour cela le projet a été partagé en trois chapitres :

- Le premier chapitre présente des généralités sur les réseaux sans fil « Wi-Fi », et son fonctionnement.
- Le deuxième chapitre est consacré aux mécanismes de sécurité, les protocoles de sécurité qui existent et les attaques possibles.
- Le troisième chapitre détaille l'implémentation des mécanismes et protocoles qu'on a choisis, et qui est le 802.1x avec un serveur d'authentification radius, dans ce chapitre, on décrit les étapes qu'on a suivi pour la sécurisation d'un réseau expérimental se composant d'un utilisateur, un point d'accès AP et d'un serveur.

Réseaux sans fil

1. Introduction

La grande particularité des réseaux sans fil est d'être un système rapide à déployer, pour un cout raisonnable. En effet, il suffit pour construire un tel réseau d'équiper les postes informatiques d'un adaptateur 802.11 et si nécessaire d'installer un point d'accès. Ce type de réseau utilise donc des ondes radio pour véhiculer des données entre les postes.

L'objectif de ce chapitre est de donner un aperçu technique du standard 802.11 de façon à comprendre les concepts de base. Exposer quelques normes du Wi-Fi puis nous allons passer en revue une présentation globale du fonctionnement.

2. Historique

Les réseaux sans fil sont fondés sur une technologie à spectre étalé, initialement développée pour les communications militaires de l'armée américaine pendant la seconde guerre mondiale. Les techniciens militaires pensaient que les spectres étalés étaient plus intéressants car plus résistants au brouillage. Les autres avancées ont permis d'augmenter les débits. Après 1945, les entreprises commerciales ont commencé à exploiter cette technologie, ayant compris l'intérêt qu'elle représentait pour leurs clients.

La technologie des réseaux sans fil a évolué en 1971 avec un projet de l'université de Hawaii appelé **AlohNet**. Ce projet a permis à sept ordinateurs de communiquer depuis les différentes iles en utilisant un concentrateur central sur Oahu.

La recherche universitaire sur **AlohNet** a posé les bases de la première génération de réseaux sans fil, qui opérait sur la plage de fréquence 901-928 MHz, utilisé principalement par les militaires, cette phase du développement des réseaux sans fil n'a connu que peu d'utilisateurs à cause des problèmes de fréquence et de son faible débit.

A partir de ce moment, la fréquence 2.4 GHz a été définie pour une utilisation sans licence. La technologie a donc commencé à émerger et la spécification 802.11 est née. Celle-ci a évolué pour devenir le standard 802.11b et continue son chemin vers des implémentations plus rapides et plus sures**. [1]**

3. Définition

Un réseau sans fil (en anglais Wireless network) est, comme son nom l'indique, un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire. Grâce aux

réseaux sans fil, un utilisateur à la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu, c'est la raison pour laquelle on entend parfois parler de "mobilité".

Les réseaux sans fil sont basés sur une liaison utilisant des ondes radioélectriques (radio et infrarouges) en lieu et place des câbles habituels. Il existe plusieurs technologies se distinguant d'une part par la fréquence d'émission utilisée ainsi que le débit et la portée des transmissions.

Les réseaux sans fil permettent de relier très facilement des équipements distants d'une dizaine de mètres à quelques kilomètres. De plus, l'installation de tels réseaux ne demande pas de lourds aménagements des infrastructures existantes comme c'est le cas avec les réseaux filaires. En contrepartie se pose le problème de la réglementation relative aux transmissions radioélectriques. De plus, les ondes hertziennes sont difficiles à confiner dans une surface géographique restreinte, il est facile pour un pirate d'écouter le réseau si les informations circulent en clair. Donc il est nécessaire de mettre en place les dispositions nécessaires de telle manière à assurer une confidentialité des données circulant sur les réseaux sans fil. **[2]**

- **L'onde radio**

Les ondes radioélectriques (dites **ondes radio**) sont des ondes électromagnétiques dont la fréquence d'onde est par convention comprise entre 9 KHz et 3000 GHz, ce qui correspond à des longueurs d'onde de 33 km à 0,1 mm. Les ondes hertziennes, utilisées non seulement pour la radio proprement dite (la TSF, comme on l'appelait en 1930) mais aussi pour la télévision, le téléphone portable voire le four à micro-ondes, appartiennent comme la lumière ou les rayons X à la grande famille des ondes électromagnétiques.

Elles sont produites en injectant dans une antenne un courant électrique variable à haute-fréquence. On peut comparer l'antenne à une ampoule électrique nue qui rayonnerait l'énergie que lui communique le courant électrique qui la traverse**. [3]**

4. Technologies sans fil

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

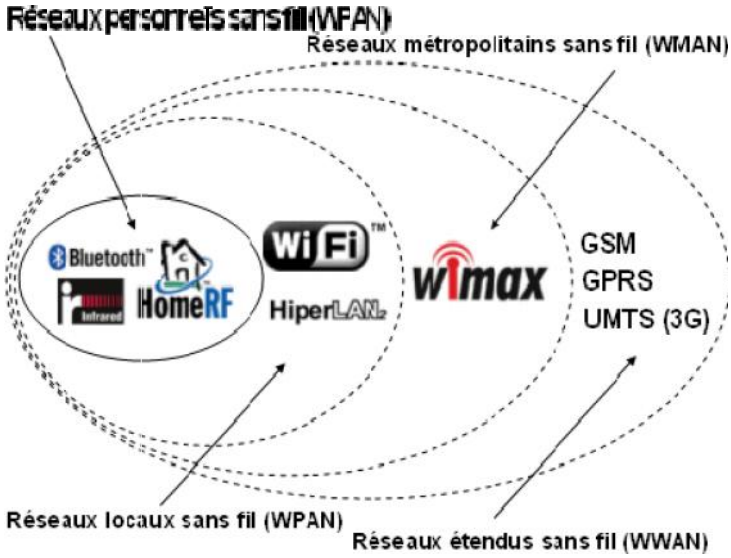

Figure I.1 : Catégories des réseaux sans fil

4.1. Réseaux WPAN

Le réseau personnel sans fil (appelé également réseau individuel sans fil ou réseau domestique sans fil et noté WPAN pour **W**ireless **P**ersonal **A**rea **N**etwork) concerne les réseaux sans fil d'une faible portée : de l'ordre de quelques dizaines mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques, ...) ou un assistant personnel (PDA) à un ordinateur sans liaison filaire ou bien à permettre la liaison sans fil entre deux machines très peu distantes. Il existe plusieurs technologies utilisées pour les WPAN : **Bluetooth, Home RF, La technologie ZigBee.**

4.2. Réseaux WMAN

La BLR (**B**oucle **L**ocale **R**adio) fait partie des réseaux sans fil de type WMAN. La BLR est une technologie sans fil capable de relier les opérateurs à leurs clients grâce aux ondes radio sur des distances de plusieurs kilomètres.

Les réseaux sans fil de type WMAN (**W**ireless **M**étropolitain **A**rea **N**etwork) sont en train de se développer. Ce phénomène risque de s'amplifier dans les années à venir. La norme IEEE 802.16, est plus connue sous son nom commercial Wi-Max. La dernière version de la norme est IEEE 802.16-2004, ratifiée en juin 2004. Comme dans le cas de la dénomination Wi-Fi ; Wi-Max désigne en fait un ensemble de normes regroupées sous une appellation commune. La norme de réseau métropolitain sans fil la plus connue est le Wi-Max.

Techniquement, le Wi-Max permet des débits de l'ordre de 70 Mbit/s avec une portée de l'ordre de 50 km. Actuellement, le Wi-Max peut exploiter les bandes de fréquence 2,4 GHz,

3,5 GHz et 5,8 GHz. Aujourd'hui, en France, la bande de fréquence 2,4 GHz est libre, la bande de fréquence 5,8 GHz est interdite en utilisation extérieure et la bande des 3,5 GHz est licenciée à un unique opérateur. La norme 802.16e ajoutera de la mobilité à la norme actuelle IEEE 802.16**. [4]**

4.3. Réseaux WWAN

Le réseau étendu sans fil (WWAN pour **W**ireless **W**ide **A**rea **N**etwork) est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fil les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil. Les principales technologies sont les suivantes : **GSM, GPRS**, **UMTS.**

4.4. Les réseaux WLAN

Le réseau local sans fil (WLAN pour **W**ireless **L**ocal **A**rea **N**etwork) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres**. [5]**

les WLAN ont été conçus pour offrir un accès large bande radio avec des débits de plusieurs Mbit/s pour relier des équipements de type PC et autres équipements électroniques ou informatiques dans des environnements professionnels, immeubles de bureaux, bâtiments industriels ou grand public et se connecter à un réseau cœur, tel qu'un réseau Ethernet. Ils sont déployés dans des lieux privés mais aussi dans des lieux publics gares, aéroports, campus (hot spots). Ils sont complémentaires des réseaux cellulaires 2G et 3G qui offrent une plus grande mobilité mais des débits plus faibles.

Deux grandes familles se partagent le domaine des WLAN résultant des travaux menés aux Etats-Unis et en Europe. La première famille est celle du Wi-Fi nom donné à la norme IEEE 802.11b qui est actuellement la plus populaire pour offrir des débits jusqu'à 11 Mbit/s pour des distances de 10 à 100 m. La seconde famille est celle de l'HIPERLAN2 et de IEEE 802.11a basée sur l'OFDM (**O**rthogonal **F**requency **D**ivision **M**ultiplexing) plus robuste aux distorsions sélectives en fréquence du canal, offrant des débits jusqu'à 54 Mbit/s mais au prix d'une complexité plus grande**. [6]** Il existe plusieurs technologies concurrentes : **hiperLAN2, DECT, Wi-Fi.**

4.5. Réseaux WRAN

L'organisation de certification, l'Institute of Electrical and Electronics Engineers ou IEEE, vient d'approuver une nouvelle norme la 802.22 WRAN (**W**ireless **R**egional **A**rea **N**etworks ou système de réseau régional sans fil). Celle-ci va permettre de fournir le haut débit sans fils

dans les zones mal desservies, en se servant des fréquences VHF et UHF des canaux de télévision vacants. Cette norme offrira également un débit de l'ordre de 22Mbps par canal, jusqu'à une distance de 100 kilomètres du transmetteur. La 802.22 vise donc à fournir un accès à large bande dans les zones rurales, mais également dans les pays en voie de développement. **[7]**

Wi-Fi : Définition

Le nom **Wi-Fi** (contraction de **W**ireless **F**idelity, parfois notée à tort Wi-Fi) correspond initialement au nom donnée à la certification délivrée par la Wi-Fi Alliance, anciennement WECA, l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11. Par abus de langage (et pour des raisons de marketing), 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. La norme **IEEE 802.11** (ISO/IEC 802-11) est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN).

Grâce au Wi-Fi, il est possible de créer des réseaux locaux sans fil à haut débit pour peu que l'ordinateur à connecter ne soit pas trop distante par rapport au point d'accès. Dans la pratique, le Wi-Fi permet de relier des ordinateurs portables, des ordinateurs de bureau, des assistants personnels (PDA) ou tout type de périphérique à une liaison haut débit (11 Mbps ou supérieur) sur un rayon de plusieurs dizaines de mètres en intérieur (généralement entre une vingtaine et une cinquantaine de mètres) à plusieurs centaines de mètres en environnement ouvert**. [6]**

1. Avantages de Wi-Fi

- **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.

- **Coût**

Si leur installation est parfois un peu plus coûteuse qu'un réseau filaire, les réseaux sans fil ont des coûts de maintenance très réduits ; sur le moyen terme, l'investissement est facilement rentabilisé.

- **Évolutivité**

Les réseaux sans fil peuvent être dimensionnés au plus juste et suivre simplement l'évolution des besoins **[8].**

2. Inconvénients de Wi-Fi

- **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 câblés, mais peut être aussi les quelques ilots Wi-Fi déjà en place), le respect de régulation, le support effectif des standards actuels et à venir, l'administration de ce futur réseau, le monitoring du trafic, etc.

- **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.

- **Sécurité**

La sécurité des réseaux sans fil n'est pas encore tout à fait fiable du fait que cette technologie est novatrice**. [9]** Elle est une préoccupation critique d'un administrateur réseau confronté au Wi-Fi, d'une part parce que les faiblesses des technologies ont été largement traitées sur Internet, d'autre part parce qu'il s'agit d'une approche effectivement nouvelle du sujet, et qui présente une grande diversité.

3. Différentes normes Wi-Fi

Les standards régissant les réseaux sans fil pour les PC sont établis par l'IEEE (**I**nstitue of **E**lecrical and **E**lectronics **E**ngineers). La technologie LAN/MAN a reçu le numéro 802, lui même subdivisé en groupes de travail. Les groupes les plus actifs incluent le 802.15, pour les réseaux personnels (Bluetooth), 802.16 pour les réseaux sans fil à large bande Wi-Max et enfin 802.11 pour les LAN sans fil. Dans le groupe 802.11, des définitions plus précises existent, identifiées par les différentes lettres**. [1]**

La norme IEEE 802.11 est en réalité la norme initial offrant des débits de 1 ou 2 Mbit/s. des révisions ont été apportés à la norme originale afin d'optimiser le débit (c'est le cas des normes 802.11a, 802.11g, appelés normes 802.11 physiques) ou bien préciser des éléments

afin d'assurer une meilleure sécurité ou une meilleure interopérabilité. On trouvera ci-après une brève description des différentes révisions de la norme 802.11 ainsi que leur signification :

- **802.11a**

La norme 802.11a (baptisé **Wi-Fi 5**) permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). Elle spécifie 8 canaux radio dans la bande de fréquence des 5 GHz.

Un des avantages de cette norme consiste à remédier aux problèmes rencontrés avec 802.11b, en utilisant une bande de fréquence moins utilisée pour d'autres applications. Rappelons que les bandes de fréquences 5Ghz et 2Ghz sont libres, c'est-à-dire que leur utilisation ne nécessite aucune licence en Europe. De plus, la vitesse théorique de 54Mbps s'avère être plus confortable pour l'échange de gros fichiers comparé à celle du 802.11b qui vaut 11Mbps.

Le 802.11a possède également des inconvénients comme sa portée réduite (15m) et son incompatibilité avec le 802.11b (le passage à cette norme exige donc l'acquisition d'un tout nouveau matériel)**. [8]**

- **802.11b**

Elle est la première norme à généraliser l'utilisation des transmissions sans fil, tout en ayant connu un vif succès commercial. Elle permet d'obtenir des débits théoriques de 11 Mbit/s (6 Mbit/s réels) sur la bande de fréquence de 2.4 GHz. La portée maximale du signal est de 100 mètres en intérieur, et de 300 mètres en extérieur ; sa portée est bien moindre dans les faits (30 et 100 mètres réels). Elle utilise la modulation radio DSSS (**D**irect **S**equence **S**pred **S**pectrum) et HR-DSSS.

Impatients, car la norme 802.11g a tardé à arriver, des constructeurs ont créé une évolution de cette norme, la 802.11b+ qui permet d'augmenter les débits à 22 et 44 Mbit/s (11 à 20 Mbit/s réels). Ces matériels étaient compatibles avec la 802.11b, mais en bridant leur vitesse à 11 Mbit/s. **[10]**

Le principal inconvénient de 802.11b consiste à présenter des interférences possibles avec les appareils fonctionnant sur les mêmes fréquences tels que les fours à micro ondes, les caméras analogiques sans fil et toutes les formes de surveillance ou d'observation professionnelles ou domestiques à distance comme les transmetteurs de salon, la télé-mesure, la télé-médecine, les radio-amateurs ATV, les claviers et souris sans fil**. [8]**

- **802.11c**

La norme 802.11c est une extension de 802.11b concernant la gestion de la couche MAC. Elle améliore les procédures de connexion en pont entre les points d'accès. Les travaux ont été suspendus et la norme restituée au Groupe de Travail 802.11d**. [8]**

- **802.11d**

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**

La norme 802.11e offre des possibilités de qualité de service (**QoS**) au niveau de la couche liaison de données. Elle définit ainsi les besoins des différents paquets en termes de bande passante et de délai de transmission de telle manière à permettre des flux prioritaires. Nous pouvons alors espérer, par exemple, une transmission de la voix et de la vidéo de meilleure qualité (fluidité et débit important). Actuellement, ces applications font l'objet d'un marché en pleine expansion. Par exemple, les téléphones Wi-Fi (F1000 de **UTStarcom**), télévision Wi-Fi…

- **802.11f**

La norme 802.11f est une recommandation à l'intention des vendeurs d'équipement 802.11 visant une meilleure interopérabilité des produits. 802.11f permet à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, indépendamment des marques des points d'accès. En effet, les fabricants d'équipement 802.11 utilisaient des normes propriétaires parfois incompatibles.

- **802.11g**

La norme 802.11g est la plus répandue, elle offre un haut débit (54 Mbps) sur la bande de fréquence des 2.4 GHz. De plus, les matériels conformes à la norme 802.11g fonctionnent en 802.11b (à 11 Mbps), ce qui garantit une compatibilité avec les points d'accès 802.11b. La modulation de 802.11g est l'OFDM comme pour la norme 802.11a.

Malheureusement, ce standard est aussi sensible aux interférences avec d'autres appareils utilisant les mêmes fréquences dans la bande des 2.4 GHz. Parallèlement à l'émergence de ce standard sur le marché, nous notons la naissance d'un besoin de la part des utilisateurs de qualité de service. La sécurité n'est pas toujours garantie et le cryptage proposé, lorsqu'il est utilisé, s'est avéré faillible (WEP). Il manque un aspect de sécurité de transmission au standard 802.11g. Ce problème est éloigné avec l'utilisation de WPA à la place de WEP. Mais le standard 802.11i consacré à la sécurité des transmissions, propose des solutions complètes, avec l'utilisation de l'algorithme WPA2 (**W**i-Fi **P**rotected **A**ccess version **2**), une version nettement améliorée du WPA. **[11]**

- **802.11h**

La norme 802.11h adapte la couche MAC visant à rendre compatible les équipements 802.11 avec les infrastructures utilisant HiperLAN2. En effet, bien qu'aucune des deux ne soit standardisée, ces normes ne sont jusqu'ici pas compatibles.

802.11h permet la détection automatique de fréquence de l'AP (Access Point) et le contrôle automatique de la puissance d'émission dans le but d'éliminer les interférences entre AP. La conformité est ainsi garantie avec la réglementation européenne en matière de fréquence et d'économie d'énergie (**D**ynamic **F**requency **S**olution & **T**ransmit **P**ower **C**ontrol). Cette norme, pas encore standardisée, est développée par l'IEEE et l'ETSI.

- **802.1x**

Il s'agit d'une sous-section du groupe de travail 802.11i, visant à l'intégration du protocole EAP. 802.1x se charge de la sécurisation de transmission de l'information dans les réseaux filaires et sans fil au moyen d'authentification sûre.

802.1x supporte diverses méthodes d'authentification comme les cartes à jeton, Kerberos, les mots de passe à utilisation unique, les certificats et les clefs publiques. Un exemple d'application est l'emploi d'un serveur d'authentification Radius combiné à une distribution dynamique de clefs, qui garantit un niveau de sécurité élevé.

- **802.11i**

Le but de la norme 802.11i est d'améliorer la sécurité des transmissions (gestion et distribution dynamique des clés, chiffrement des informations et authentification des utilisateurs). **[11]**

802.11b et 802.11g utilisent WEP pour sécuriser la transmission au moyen de clefs de cryptage. Le chiffrement utilisé est RC4, qui s'est avéré faible. 802.11i utilise WPA2. Elle utilise l'authentification EAP définie dans 802.1x et s'appuie sur le chiffrement AES (**A**dvanced **E**ncryption **S**tandard). De plus, elle assure la confidentialité au moyen d'un chiffrement à clés temporaires TKIP, plus performant que l'algorithme utilisé avec 802.11g et 802.11b.

- **802.11j**

Le but de la norme 802.11j est de rendre compatible 802.11a avec la réglementation japonaise.

- **802.11k**

La norme 802.11k permet aux appareils compatibles de faire des mesures de signaux complètes pour améliorer l'efficacité des communications. Les avantages sont multiples tels

que l'administration à distance de la couverture réseau, ou une amélioration du roaming automatique via des « site report ».

- **802.11 IR**

La norme 802.11IR a été élaborée afin d'utiliser des signaux infrarouges. Les applications sont rares et nous pouvons affirmer que cette norme n'est plus d'actualité étant donné les faibles débits proposés (2Mbits/s).

- **802.11n**

Cette norme est très prometteuse car elle doit permettre d'atteindre les débits du filaire, avec un débit de 540 Mbits (100 Mb/s réels) et une portée de 100 mètres réels. Elle intégrera la technologie MIMO et devrait être compatible avec les anciennes normes avec un fonctionnement en mode mixte qui permettra d'avoir des transmissions à débit hétérogène fonctionnant en 802.11a, b ou g avec l'ancien matériel et en 802.11n avec le nouveau. Utilise la modulation radio MIMO-OFDM.

Le 802.11n utilise des fréquences de 2.4 et 5 GHz et ne fonctionne qu'en mode infrastructure avec un point d'accès centrale sur le quel tous les clients se connectent.

4. Equipements Wi-Fi

- **Eléments actifs Wi-Fi**

Les points d'accès ou des cartes clientes possèdent le même type d'éléments actifs Wi-Fi : leur fonction principale est de convertir les données numériques provenant d'un réseau Ethernet en signaux analogiques destinés à l'antenne. C'est à son niveau que les protocoles de modulation/démodulation des signaux interviennent. En réception, il effectue le processus inverse consistant à décoder les signaux transmis par l'antenne en données IP pour le réseau. Les caractéristiques principales d'un élément actif sont sa puissance d'émission et sa sensibilité en réception (puissance minimale admissible pour interpréter les données et assurer la liaison), toutes deux exprimées en mW ou dBm. Sont réglables sur ce matériel Wi-Fi le débit de liaison souhaité, parfois le niveau de puissance de sortie, ainsi que plusieurs protocoles liés à la sécurité et à l'identification des autres AP connectées.

- **Points d'accès (AP)**

Le rôle des points d'accès est similaire à celui que tiennent les hubs dans les réseaux traditionnels. Il permet aux stations équipées de cartes Wi-Fi d'obtenir une connexion au réseau. On parle alors d'association entre l'AP et chaque station connectée. Les trames d'information envoyées par un client sont ré émises par l'AP, ce qui permet à la station de

joindre un autre client qu'elle ne peut pas forcément voir directement (éloignement, obstacle). Le support physique étant les ondes radio, on ne peut pas empêcher les stations non destinataires de recevoir les trames émises, d'où l'analogie avec le hub. Les APs sont nécessaires lorsque le réseau sans fil fonctionne en mode infrastructure. Ce sont en fait des boîtes qui contiennent une carte Wi-Fi comme on en trouve sur les stations, une ou plusieurs antennes et du logiciel embarqué dans une puce pour gérer tout cela. Le logiciel présent permet de fournir des services supplémentaires liés à la sécurité et l'identification des autres AP connectés. Il est possible de transformer un ordinateur équipé d'une carte Wi-Fi en point d'accès, par simple adjonction de programmes.

Figure I.2 : Exemple de point d'accès

- **Routeurs**

Centre névralgique de votre installation, connectés à votre modem haut débit, le routeur « transforme » votre connexion Internet filaire en connexion sans fil.

La plupart des routeurs font office de borne sans fil offrant l'accès Internet à tous vos ordinateurs. Ils disposent également de ports Ethernet (en générale quatre) pour raccorder physiquement les postes les plus proches et certains offrent une sécurité pour le réseau en étant dotés de firewall et de limitations d'accès.

- **Les modems/routeurs**

Les modems/routeurs offrent une solution deux-en-un en regroupant dans un même appareil un modem (pour accédera la ligne Internet) et un routeur pour repartir cette connexion sur vos différents ordinateurs.

- **Cartes Wi-Fi**

Ce terme désigne les périphériques actifs Wi-Fi/Antenne directement branchés à un ordinateur client. Ils jouent exactement le même rôle que les cartes réseaux traditionnelles à la différence

près qu'on ne branche pas de câble dessus, puisque la liaison est assurée par radio. Elles existent en trois formats.

- **PCMCIA**

Il s'agit du format le plus répandu puisque ce format est spécifique aux portables dont les propriétaires étaient les premiers intéressés par la technologie sans fil.

Figure I.3 : Carte PCMCIA

- **PCI**

C'est le format standard pour les ordinateurs de bureau mais les cartes restent au format PCMCIA. Il y a donc un adaptateur PCMCIA-PCI sur lequel est logée une carte PCMCIA ; le prix d'achat est donc légèrement supérieur aux modèles précédents.

Figure I.4 : Carte PCI

- **USB**

Ce format s'est rapidement popularisé pour sa simplicité d'utilisation et les constructeurs n'ont pas tardé à proposer également des cartes Wi-Fi à ce format.

Figure I.5 : Carte USB

- **Antennes**

L'antenne intégrée à l'AP ou à la carte Wi-Fi peut être remplacée par une antenne externe plus puissante reliée par un câble d'antenne, la plupart du temps avec un parafoudre pour protéger l'appareil. Le choix d'une antenne est important et doit être déterminé par le rôle qu'elle devra assurer, c'est à dire les interactions souhaitées avec les autres éléments Wi-Fi distants. En fonction des caractéristiques du terrain et des zones à couvrir, il pourra par exemple être décidé de réaliser des liaisons point à point via deux antennes directionnelles ou utiliser un élément omnidirectionnel en cas de clients plus dispersés et rapprochés. Il y a 3 grandes familles d'antennes :

- Les omnidirectionnelles
- Les directionnelles
- Les patchs ou antennes sectorielles

Figure I.6 : Schéma général du réseau Wi-Fi

5. Architecture Wi-Fi (802.11)

La norme IEEE 802.11 définit les deux premières couches (basses) du modèle OSI, à savoir la couche physique et la couche liaison de données. Cette dernière est elle-même subdivisée en deux sous-couches, la sous-couche LLC et la couche MAC.

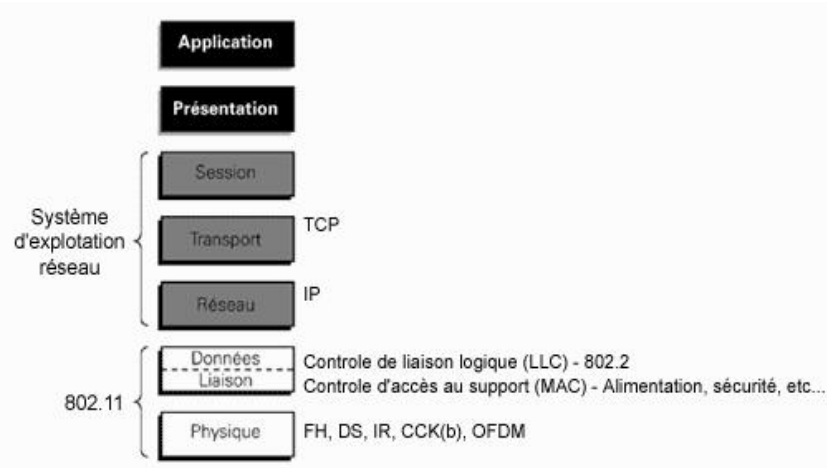

Figure I.7 : Couches du modèle OSI

5.1. Couche physique

(Notée parfois couche PHY) elle définit la modulation des ondes radio-électriques et les caractéristiques de la signalisation pour la transmission de données, tandis que la couche liaison de données définit l'interface entre le bus de la machine et la couche physique, notamment une méthode d'accès proche de celle utilisée dans le standard Ethernet et les règles de communication entre les différentes stations. La norme 802.11 propose en réalité trois couches physiques, définissant des modes de transmission alternatifs: DSSS, FHSS, Infrarouges.

a. FHSS (Frequency Hopping Spread Spectrum)

La technique de FHSS consiste à découper la large bande de fréquence en un minimum de 75 canaux (hops ou sauts d'une largeur de 1MHz), puis de transmettre en utilisant une combinaison de canaux connue de toutes les stations de la cellule. Dans la norme 802.11, la bande de fréquence 2.4 - 2.4835 GHz permet de créer 79 canaux de 1 MHz. La transmission est ainsi réalisée en émettant successivement sur un canal puis sur un autre pendant une courte période de temps (d'environ 400 ms), ce qui permet à un instant donné de transmettre un signal plus facilement reconnaissable sur une fréquence donnée. L'émetteur et le récepteur s'accordent sur un schéma de saut, et les données sont envoyées sur une séquence de sous-canaux. Chaque conversation sur le réseau 802.11 s'effectue suivant un schéma de saut différent, et ces schémas sont définis de manière à minimiser le risque que deux expéditeurs utilisent simultanément le même sous-canal. La séquence de fréquences utilisée est publique. FHSS est utilisé dans le standard 802.11 de telle manière à réduire les interférences entre les transmissions des diverses stations d'une cellule.

Les techniques FHSS simplifient relativement la conception des liaisons radio, mais elles sont limitées à un débit de 2 Mbps, cette limitation résultant essentiellement des réglementations de l'ETSI qui restreignent la bande passante des sous-canaux à 1 MHz. Ces contraintes forcent les systèmes FHSS à s'étaler sur l'ensemble de la bande des 2,4 GHz, ce qui signifie que les sauts doivent être fréquents et représentent en fin de compte une charge importante.

b. DSSS (Direct-Sequence Spread Spectrum)

En revanche, la technique divise la bande de 2,4 GHz en 14 canaux de 22 MHz. Les canaux adjacents se recouvrent partiellement, seuls trois canaux sur les 14 étant presque entièrement isolés. DSSS augmente la fréquence du signal numérique en le combinant avec un autre signal d'une fréquence plus élevée. Les données sont transmises intégralement sur l'un de ces canaux

de 22 MHz, sans saut. La technique du « chipping » aide à compenser le bruit généré par un canal donné, c'est-à-dire moduler chaque bit avec la séquence Barker. **[12]**

Dans ce but, le standard 802.11 DSSS original spécifie un chipping sur 11 bits (baptisé séquence Barker) pour le codage des données. La longueur du « chipping code » détermine combien de données seront transmises au-dessus d'une unité de temps (c'est-à-dire la bande passante). Ainsi chaque bit valant 1 est remplacé par une séquence de bits et chaque bit valant 0 par son complément.

c. Infrarouges (IR)

Le standard IEEE 802.11 prévoit également une alternative à l'utilisation des ondes radio : la lumière infrarouge. Cette technologie a pour caractéristique principale d'utiliser une onde lumineuse pour la transmission de données. Ainsi les transmissions se font de façon unidirectionnelle, soit en vue direct soit par réflexion. Le caractère non dissipatif des ondes lumineuses offre un niveau de sécurité plus élevé. Il est possible grâce a la technologie infrarouge d'obtenir des débits allant de 1 à 2 Mbit/s en utilisant une modulation appelés PPM (**P**ulse **P**osition **M**odulation).

La modulation PPM consiste à transmettre des impulsions à amplitude constante, et à coder l'information suivant la position de l'impulsion. Le débit de 1 Mbps est obtenu avec une modulation de 16-PPM, tandis que le débit de 2Mbps est obtenu avec une modulation 4-PPM permettant de coder deux bits de données avec 4 positions possibles.

5.2. Couche liaison de données

Constitué de deux sous-couches : le contrôle de la liaison logique (**L**ogic **L**ink **C**ontrol, ou LLC) et le contrôle d'accès au support (**M**edia **A**ccess **C**ontrol, ou MAC).

- Couche LLC : utilise les mêmes propriétés que la couche LLC 802.2.
- Couche MAC : son rôle est similaire à celui de la couche MAC 802.3 du réseau Ethernet terrestre, puisque les terminaux écoutent la porteuse avant d'émettre. Si la porteuse est libre, le terminal émet, sinon il se met en attente. Cependant la couche MAC 802.11 intègre un grand nombre de fonctionnalités que l'on ne trouve pas dans la version terrestre.

Les fonctionnalités nécessaires pour réaliser un accès sur une interface radio sont les suivantes :

- Procédure d'allocation du support
- Adressage des paquets
- Formatage des trames
- Contrôle d'erreur CRC

- Fragmentation et réassemblage

a. Couche MAC

Le but principale de la couche MAC est de fournir un couplage efficace entre les services de la couche RLC 2 et la couche physique. De cette perspective, la couche MAC supporte quatre fonctions principales :

- Le mappage entre les canaux logiques et de transport. En effet, quand le standard offre différents options pour le transport de données pour un canal logique donné, la couche MAC s'occupe de choisir le canal de transport selon la configuration choisi par l'opérateur.
- La sélection du format de transport qui fait référence par exemple, au choix la taille du' Transport Block' et le schéma de modulation.
- Gestion de propriété entre les connais logique d'une terminale ou entre plusieurs terminaux.
- Correction d'erreur à travers le mécanisme HARQ.

b. Couche LLC

Couche dépourvue du codage analogique: on récupère les bits. Réalisé à la limite du hardware et du software (firmware EEPROM). Les services rendus par la couche LLC aux couches supérieures sont spécifié par 3 classes :

- **LLC1 :** service sans connexion et sans acquittement. Le travail est fait dans les couches supérieures ou on accepte de perdre des données (ex : Visio confi et temps réel) les couches supérieures assurent la reprise en cas d'erreur).
- **LLC2 :** service avec connexion ex : porteuse (pour les transmissions longues de fichiers,).
- **LLC3 :** service sans connexion et avec acquittement. Cela évite de maintenir une table active : datagramme. En fait, on écoute en permanence car il y a des diffusions d'écoute (on arrose tout le monde).

5.3. Modes de fonctionnement

De manière générale, la machine cliente demande des informations via le réseau et la machine serveur offre des services. Deux types d'architectures sont généralement distinguées pour les réseaux sans fil à savoir le mode Ad hoc et le mode Infrastructure.

5.3.1. Mode infrastructure

C'est un mode de fonctionnement qui permet de connecter les ordinateurs équipés d'une carte réseau Wifi entre eux via un ou plusieurs points d'accès qui agissent comme des concentrateurs.

L'ensemble formé par le point d'accès et les stations situés dans sa zone de couverture est appelé Cellule de base BSS (**B**asic **S**ervice **S**et). Chaque BSS est identifié par un BSSID (un identifiant de 6 octets). Dans le mode infrastructure, le BSSID correspond à l'adresse MAC du point d'accès.

Lorsque le réseau est relié à plusieurs BSS, chacun d'eux est relié à un système de distribution DS (**D**istribution **S**ystem) par l'intermédiaire de leur point d'accès. Le système de distribution (DS) peut être aussi bien un réseau filaire (Ethernet), qu'un câble entre deux points d'accès ou bien même un réseau sans fil.

Un groupe de BSS interconnectés par un système de distribution forme un ensemble de services étendu ESS (**E**xtended **S**ervice **S**et). **[13]**

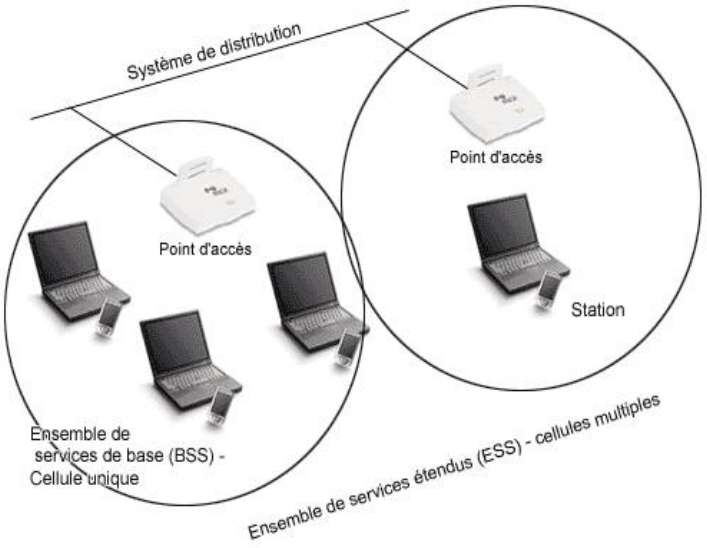

Figure I.8 : Mode infrastructure

Lorsqu'une station entre dans un BSS ou ESS, elle doit s'associer à un point d'accès. L'association comporte les différentes étapes suivantes :

- **La station écoute le canal afin de découvrir le point d'accès disponible**

Cette écoute peut se faire de deux manières différentes :

- Ecoute passive : la station écoute sur tous les canaux de transmissions et attend de recevoir une trame balise du point d'accès.
- Ecoute active : sur chaque canal de transmission, la station envoi une trame de requête (**P**robe **R**equest **F**rame) et attend la réponse. Une fois l'écoute est terminée, la station choisi le point d'accès le plus approprié.

- **Authentification**

Une fois que le point d'accès est choisi, la station doit s'authentifier auprès lui. Il y a deux méthodes d'authentification:

- Open System Authentification : Authentification par défaut, le terminal peut s'associer à n'importe quel point d'accès et écoute toutes les données qui transitent au sein du BSS.
- Shared Key Authentification : Meilleur que la précédente utilisé dans le cas d'une sécurité WEP.

- **Association**

Dés qu'une station est authentifiée, elle peut s'associer avec le point d'accès, elle envoie pour cela une trame de requête d'association et attend que le point d'accès lui réponde. **[13]**

5.3.2. Mode Ad-Hoc

Un groupe de terminaux forme un ensemble de services de base indépendants IBSS (**I**ndependent **B**asic **S**ervice **S**et). Chaque station peut établir une communication avec n'importe quelle station dans l'IBSS, sans être obligée de passer par un point d'accès. **[13]**

Ce mode permet de déployer, rapidement et n'importe où, un réseau sans fil. Le fait de ne pas avoir besoin d'infrastructure, autre que les stations et leurs interfaces, permet d'avoir des nœuds mobiles. D'un point de vue militaire, c'est très intéressant. Sur le champ de batailles, même si une partie des équipements est détruite, il est toujours possible de communiquer. On imagine aussi, l'intérêt lors de catastrophes naturelles, tel que les tremblements de terre. Les réseaux ad-hoc permettent d'établir très rapidement un système de communication efficace. **[14]**

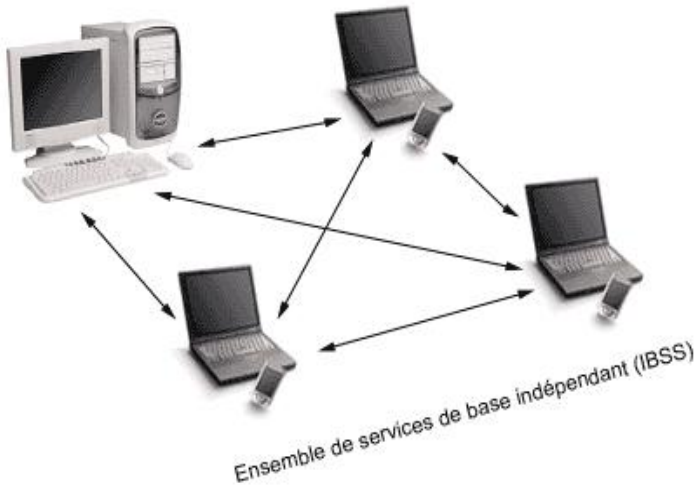

Figure I.9 : Mode Ad-Hoc

Conclusion

Dans ce chapitre on a bien vu que lors du déploiement d'un réseau sans fil, le Wi-Fi (802.11) semble être la solution répondant au mieux aux besoins des réseaux locaux sans fil grâce à l'avantage qu'elle procure, qui est son interopérabilité avec les réseaux de type Ethernet. Cette technologie, est fréquemment utilisée dans les entreprises désirant accueillir des utilisateurs mobiles ou souhaitant une alternative au réseau filaire tout en conservant des performances quasi identiques. Contrairement le Wi-Fi a beaucoup de problèmes de sécurité, dans le chapitre qui suit, on va détailler les mécanismes utilisé pour mettre au point une stratégie de sécurité.

Introduction

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 mais l'écoute passive nécessite une intrusion physique. Car toute personne possédant quelques notions d'informatique et un peu de matériel peut facilement trouver les informations et les programmes pour écouter et percer des réseaux Wi-Fi. En plus de ces faiblesses intrinsèques aux ondes radio, un réseau Wi-Fi doit se protéger des attaques classiques. Ces failles de sécurité ont porté un préjudice certain à son développement en entreprise, car elles deviennent les points d'accès au réseau interne sur lequel il est connecté. Il existe des moyens de sécurité implantés de base sur le matériel Wi-Fi (carte et point d'accès) permettant un premier niveau de protection, mais ces moyens de sécurisation sont facilement contournable. Dans ce chapitre, on va présenter d'une part une analyse des différentes attaques susceptibles d'atteindre un réseau Wi-Fi, d'autre part une série de notions utilisé qui répondent aux trois principes élémentaires de sécurité qui sont: Codage, Authentification et Intégrité, permettant à leurs administrateurs et usagers de mieux contrôler et si possible réduire les risques.

1. Risques et attaques

1.1. Les risques

Les risques dépendent des paramètres que l'on peut maitriser. Contrairement au réseau câblé, le contrôle des accès physiques au réseau sans fil est difficile, voir impossible.
Il existe deux types de risques :

- **Risque structurel :** dépend de l'organisation de l'entreprise.
- **Risque accidentel :** indépendant de tous les facteurs de l'entreprise.

On peut classifier les risques en quatre niveaux :

a. **Acceptables :** pas des conséquences graves pour les utilisateurs du réseau.

   Exemple : panne éclectique, perte de liaison, engorgement…

b. **Courants :** pas de préjudices graves au réseau, on peut réparer facilement.

Exemple : gestion du réseau, mauvaise configuration, erreur utilisateur…

c. Majeurs : dus à des facteurs graves et qui causent de gros dégâts mais récupérables.

Exemple : foudre qui tombe sur un routeur…

d. Inacceptables : fatals pour l'entreprise, ils peuvent entrainer son dépôt de bilan.

Exemple : perte ou corruption des informations importantes…

1.2. Les attaques

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

1.2.1. Attaques passives

Dans un réseau sans fil 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. L'attaque passive la plus répandue est la recherche de point d'accès. Cette attaque (appelée Wardriving) est devenu le " jeu " favori de nombreux pirates informatique, les points d'accès sont facilement détectables grâce à un scanner (portable équipé d'une carte Wi-Fi et d'un logiciel spécifique de recherche de PA). Ces cartes Wi-Fi sont équipées d'antennes directives (type Yagi) permettant d'écouter le trafic radio à distance hors de la zone de couverture du point d'accès. Il existe deux types de scanners, les passifs (Kismet, Wifiscanner, Prismstumbler…) ne laissant pas de traces (signatures), quasiment indétectables et les actifs (Netstumbler, dstumbler) détectables en cas d'écoute, ils envoient des " probe request ". Seul Netstumbler fonctionne sous Windows, les autres fonctionnent sous Linux. **[15]**

Les sites détectés sont ensuite indiqués par un marquage extérieur (à la craie) suivant un code (warchalking) :

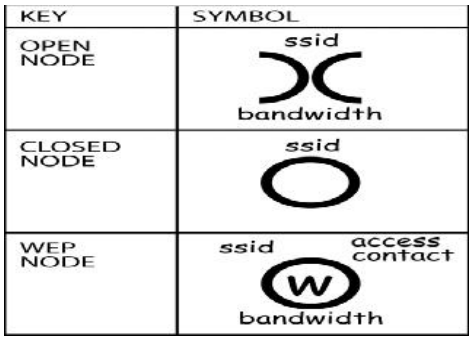

Figure II.1 : Code warchalking

Une première analyse du trafic permet de trouver le SSID (nom du réseau), l'adresse MAC du point d'accès, le débit, l'utilisation du cryptage WEP et la qualité du signal. Associé à un GPS, ces logiciels permettent de localiser (latitude longitude) ces points d'accès.
A un niveau supérieur des logiciels (type Aisnort ou Wepcrack) permettent, en quelques heures (suivant le trafic), de déchiffrer les clés WEP et ainsi avec des outils d'analyse de réseaux conventionnels la recherche d'informations peut aller plus loin. Le pirate peut passer à une attaque dite active.

1.2.2. Attaques actives

Nous allons revoir, assez succinctement, les différentes attaques connues dans les réseaux filaires et qui touchent bien évidemment, le monde du Wi-Fi.

- **DoS (Denial of Service)**

Le déni de service réseau est souvent l'alternative à d'autres formes d'attaques car dans beaucoup de cas il est plus simple à mettre en œuvre, nécessite moins de connaissances et est moins facilement traçable qu'une attaque directe visant à entrer dans un système pour en prendre le contrôle. Cette attaque a pour but d'empêcher des utilisateurs légitimes d'accéder à des services en saturant de fausses requêtes ces services. Elle se base généralement sur des " bugs " logiciel. Dans le milieu Wi-Fi, cela consiste notamment à bloquer des points d'accès soit en l'inondant de requête de désassociassions ou de dés authentification (programme de type Airjack), ou plus simplement en brouillant les signaux hertzien. **[15]**

- **Spoofing (usurpation d'identité)**

Le spoofing IP 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. Le spoofing IP n'est pas pour autant un changement d'adresse IP. Plus exactement il s'agit d'une mascarade (il s'agit du terme technique) de l'adresse IP au niveau des paquets émis, c'est-à-dire que les paquets envoyés sont modifiés afin qu'ils semblent parvenir d'une machine. **[15]**

- **Man in the middle (home au milieu) en milieu Wi-Fi**

Cette attaque consiste, pour un réseau Wi-Fi, à disposer un point d'accès étranger dans à proximité des autres PA légitimes. Les stations désirant se connecter au réseau livreront au PA " félon " leurs informations nécessaires à la connexion. Ces informations pourront être utilisées par une station pirate. Il suffit tout simplement à une station pirate écoutant le trafic, de récupérer l'adresse MAC d'une station légitime et de son PA, et de s'intercaler au milieu. **[15]**

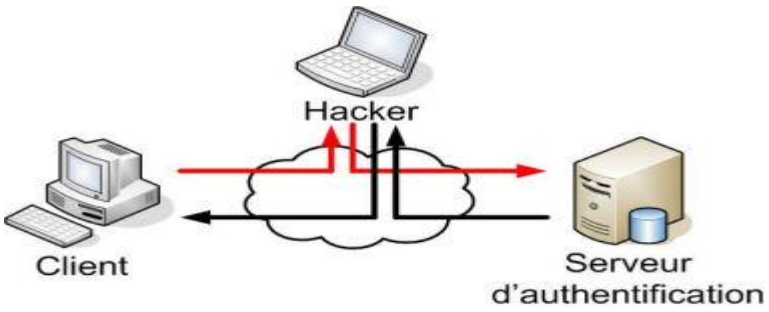

Figure II.2 : Attaque MITM

1.2.3. Autres attaques

- **Craquage de mots de passe**

Cette méthode est souvent le dernier de recours. Il consiste à faire beaucoup d'essais pour déterminer un mot de passe. On distinguera deux grandes méthodes :

- L'utilisation de dictionnaires : la plupart des mots de passes ne sont pas des chaines aléatoires mais des mots ou des phrases faciles à retenir. Cela permet d'écarter une très grande quantité de possibilités.
- La force brute consiste à essayer toutes les combinaisons possibles. Elle est rapidement efficace sur les petites chaînes (moins de 8 caractères) mais devient rapidement trop longue à exécuter quand la longueur du mot de passe augmente (plus de 16 caractères). **[14]**

- **Backdoors**

Quand un pirate arrive à accéder à un système et qu'il veut pouvoir y accéder plus facilement par la suite, il crée une ``Backdoors'' ou porte de derrière. Cela pourra se traduire par : **[14]**

- Le rajout d'un nouveau compte au serveur avec le mot de passe choisi par le pirate.
- La modification du firewall pour qu'il accepte une IP définie (une que le pirate pourra spoofer facilement) ou qu'il ouvre certains ports.
- La création d'un compte FTP.
- L'ouverture de Telnet.
- L'utilisation d'un troyen.

- **Virus, vers et chevaux de Troie**

Un virus est un programme capable de se cacher dans un autre et qui peut se reproduire en infectant d'autres programmes ou d'autres ordinateurs. Les dégâts pourront aller d'un simple affichage à l'écran à une mise hors service d'un système. On recense plusieurs catégories : **[14]**

- Les vers capables de se propager dans le réseau.
- Les chevaux de Troie ou troyens créant des failles dans un système.
- Les bombes logiques se lançant suite à un événement du système (appel d'une primitive ou date spéciale).
- Les hoax qui sont des canulars envoyés par mail.

- **Le sniffing**

Ce type d'attaque est basé sur l'interception de données émises sans précaution à toutes les parties comme lors des diffusions. Il suffit d'être présent sur le réseau pour intercepter tout le trafic et récupérer n'importe quelles données transitant sur le réseau si celles-ci ne sont pas cryptées. **[14]**

2. Services de sécurité

Les services de sécurité représentent les logiciels et matériels mettant on œuvre les mécanismes dans le but de mettre à la disposition des utilisateurs des fonctions de sécurité dont ils ont besoin.

Il existe cinq notions fondamentales de la sécurité :

2.1. Confidentialité

Le service de confidentialité garantie aux deux entités communicantes à être les seules à pouvoir comprendre les données échangées. Ceci implique la mise en œuvre des algorithmes de chiffrement en mode flux, c'est-à-dire octet par octet, ou en mode bloc.

Un message écrit en clair est transformé en un message chiffré, appelé « cryptogramme » grâce aux algorithmes de chiffrement. Cette transformation est fondée sur une ou plusieurs clés. **[16]**

2.1.1. Chiffrement (la cryptographie)

Le chiffrement consiste à rendre un texte incompréhensible en le codant. On code (crypte ou chiffre) le texte en effectuant une opération sur le texte en clair à partir d'une règle appelée clé de chiffrement. Le texte codé (cryptogramme) peut alors être envoyé à son destinataire. La cryptanalyse consiste à déchiffrer un texte codé en effectuant sur ce texte avec une clé. Il existe trois méthodes de chiffrement : à clé symétrique, à clé asymétrique (ou clé publique), à clé mixte (utilisation des deux précédentes).

2.1.1.1. Clé symétrique

La clé de chiffrement est identique à la clé de déchiffrement. Ainsi c'est la même clé qui va nous permettre à la fois de chiffrer le message et de permettre aux destinataires de le déchiffrer. Cela ne va pas sans poser un problème majeur: l'échange préalable de la clé entre les protagonistes. Or, ceci est particulièrement difficile à réaliser, puisque, tant que la clé n'est pas transmise, il n'existe pas de moyen sûr d'échange d'information, en dehors d'une rencontre physique qui n'est pas forcément possible.

Le deuxième problème est le nombre de clés nécessaire pour sécuriser un ensemble de relations. En effet, si l'on désire que chaque utilisateur d'un réseau puisse communiquer avec un autre utilisateur de manière sécurisée, une clé différente est alors utilisée pour chaque paire d'utilisateurs du réseau. Le nombre total de clés croît alors suivant un polynôme quadratique. Ainsi, un groupe de 10 utilisateurs met en jeu 45 clés différentes et 100 utilisateurs, 4950 clés. **[17]**

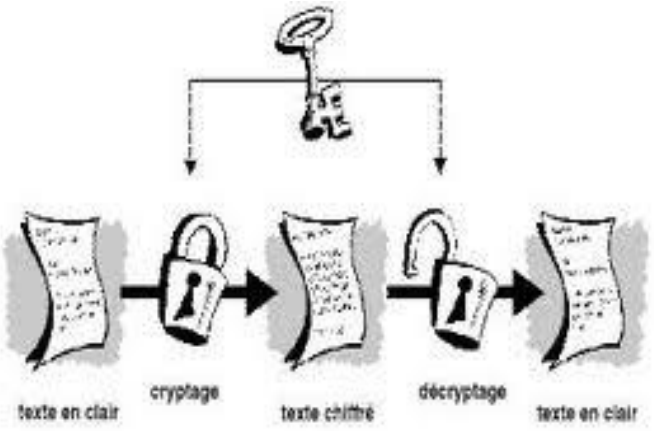

Figure II.3 : Chiffrement symétrique

Les principes algorithmes de chiffrement symétriques sont :

- **DES (Data Encryptions Standard) :** a été le plus utilisé, mais n'est plus utilisé depuis 1998 considéré peu sûr. Clé de 40 à 56 bits.
- **IDEA (International Data Encryptions Algorithm) :** est utilisé par PGP (**P**retty **G**ood **P**rivacy), le logiciel de cryptographie le plus utilisé au monde. Clé de 128 bits.
- **Série RC (Ron's Code) RC2 à RC6 :** algorithme développé par Ron Rivest, la version RC4 est utilisé dans le protocole WEP d'IEEE 802.11.
- **AES (Advanced Encryption Standard) :** remplaçant du DES dans l'administration américaine et du RC4 dans la norme 802.11 avec 802.11i. Fondé sur l'algorithme de Rijndael, est considéré comme étant incassable.

2.1.1.2. Clé Asymétrique

Dans ce cas, les clés de chiffrement et de déchiffrement sont distinctes, et généralement symétriques entres elles: la clé de chiffrement permet de déchiffrer ce qui a été chiffré avec la clé de déchiffrement, et vice versa. Le possesseur d'une telle paire de clés, en rend une (au choix) publique, c'est-à-dire qu'il la donne à tout le monde, dans une sorte d'annuaire. Tout correspondant qui veut envoyer un message, chiffre son message à l'aide de la clé publique du destinataire. Seul le possesseur de la clé secrète correspondant à cette clé publique pourra déchiffrer le message. **[17]**

Les algorithmes de chiffrement à clé publique permettent aussi à l'envoyeur de signer son message. En effet, il lui suffit de chiffrer le message (ou une partie de ce message) avec sa propre clé secrète. Le destinataire déchiffrera cette fonction avec la clé publique de l'envoyeur et sera ainsi certain de l'identité de l'expéditeur, puisqu'il est le seul à posséder la clé secrète qui permet de faire un tel chiffrement. Ainsi cette méthode permet de réaliser une communication confidentielle sans échanger auparavant de code secret.

Le principal inconvénient de ce type d'algorithme est la lenteur à laquelle s'effectuent les opérations de chiffrement et de déchiffrement. **[17]**

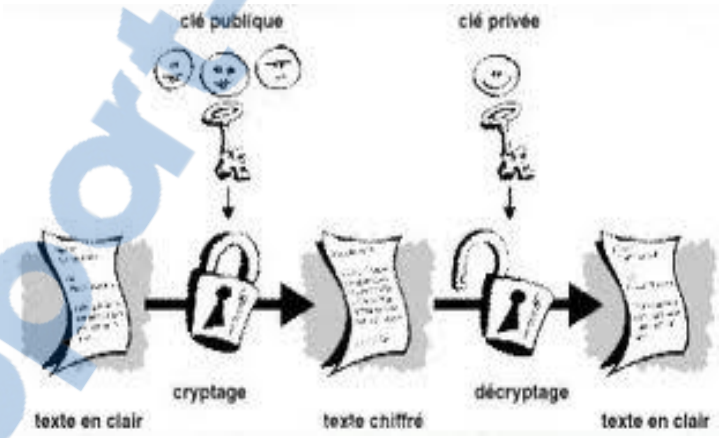

Figure II.4 : Chiffrement asymétrique

- **RSA (Rivest, Shamir, Adelman) :** comme le plus connu de ces algorithmes. La sécurité du RSA réside dans l'impossibilité pratique de factoriser un grand nombre de quelques centaines de chiffres en un temps raisonnable. Qui plus est pour assurer sa pérennité il est toujours possible d'augmenter la longueur de la clé qui varie entre 1024 et 2048 bits.

En résumé, une synthèse de ces deux méthodes de cryptographie est décrite dans le tableau ci-après.

Type de crypto système	Avantages	Inconvénients
Clé Symétrique	- Rapide - Peut être facilement réalisé sur une puce	- Difficultés de distribuer les clés - Ne permet pas de signature électronique
Clé Asymétrique	- Utilise deux clés différents - Fournit des garanties d'intégrité et non répudiation par signature électronique	- Lent et demandant beaucoup de calculs

Tableau II.1 : Comparaison entre les types de chiffrement

Finalement comme nous avons pu le voir précédemment, les deux systèmes de base de la cryptographie (symétrique et asymétrique) souffrent de problèmes complémentaires. Ainsi l'intérêt pour augmenter la sécurité des systèmes de cryptage passe certainement par l'utilisation combinée de ces deux techniques, ce que l'on nomme la cryptographie mixte. **[17]**

2.1.1.3. Clé mixte

Ce principe fait appel aux deux techniques précédentes, à clé symétrique et à clé publique, combinant les avantages des deux touts en évitant leurs inconvénients. Le principe général consiste à effectuer le chiffrement des données avec des clés symétriques, mais en ayant effectué au départ l'envoi de la clé symétrique par un algorithme à clé publique.
L'un de ces algorithmes est PGP**.**

- **PGP (Pretty Good Privacy)**

PGP est un système de cryptographie hybride, utilisant une combinaison des fonctionnalités de la cryptographie à clé publique et de la cryptographie symétrique.
Lorsqu'un utilisateur chiffre un texte avec PGP, les données sont d'abord compressées. Cette compression des données permet de réduire le temps de transmission par tout moyen de communication, d'économiser l'espace disque et, surtout, de renforcer la sécurité cryptographique.
La plupart des cryptanalyses exploitent les modèles trouvés dans le texte en clair pour casser le chiffrement. La compression réduit ces modèles dans le texte en clair, améliorant par conséquent considérablement la résistance à la cryptanalyse.
Ensuite, l'opération de chiffrement se fait principalement en deux étapes :

- PGP crée une clé secrète IDEA de manière aléatoire, et chiffre les données avec cette clé

- PGP crypte la clé secrète IDEA et la transmet au moyen de la clé RSA publique du destinataire.

L'opération de décryptage se fait également en deux étapes :

- PGP déchiffre la clé secrète IDEA au moyen de la clé RSA privée.
- PGP déchiffre les données avec la clé secrète IDEA précédemment obtenue.

Cette méthode de chiffrement associe la facilité d'utilisation du cryptage de clef publique à la vitesse du cryptage conventionnel. Le chiffrement conventionnel est environ 1000 fois plus rapide que les algorithmes de chiffrement à clé publique. Le chiffrement à clé publique résout le problème de la distribution des clés. Utilisées conjointement, ces deux méthodes améliorent la performance et la gestion des clefs, sans pour autant compromettre la sécurité.

2.1.2.Certificats

Un certificat permet d'associer une clé publique à une entité (une personne, une machine, ...) afin d'en assurer la validité. Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé autorité de certification (souvent notée CA pour **C**ertification **A**uthority). L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité (équivalent à la date limite de péremption des produits alimentaires), ainsi que de révoquer éventuellement des certificats avant cette date en cas de compromission de la clé (ou du propriétaire).

- **Structure d'un certificat**

Les certificats sont des petits fichiers divisés en deux parties :

- La partie contenant les informations
- La partie contenant la signature de l'autorité de certification

La structure des certificats est normalisée par le standard X.509 de l'UIT (plus exactement X.509v3), qui définit les informations contenues dans le certificat :

- La version de X.509 à laquelle le certificat correspond ;
- Le numéro de série du certificat ;
- L'algorithme de chiffrement utilisé pour signer le certificat ;
- Le nom (DN, pour **D**istinguished **N**ame) de l'autorité de certification émettrice ;
- La date de début de validité du certificat ;
- La date de fin de validité du certificat ;
- L'objet de l'utilisation de la clé publique ;
- La clé publique du propriétaire du certificat ;

- La signature de l'émetteur du certificat.

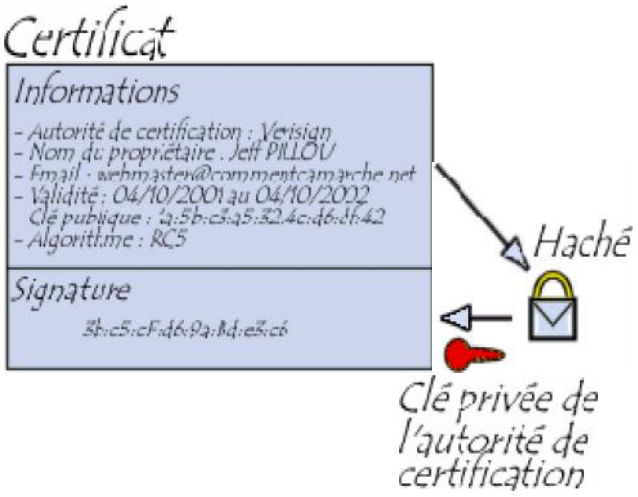

Figure II.5 : Certificat

L'ensemble de ces informations (informations + clé publique du demandeur) est signé par l'autorité de certification, cela signifie qu'une fonction de hachage crée une empreinte de ces informations, puis ce condensé est chiffré à l'aide de la clé privée de l'autorité de certification; la clé publique ayant été préalablement largement diffusée afin de permettre aux utilisateurs de vérifier la signature avec la clé publique de l'autorité de certification.
Lorsqu'un utilisateur désire communiquer avec une autre personne, il lui suffit de se procurer le certificat du destinataire. Ce certificat contient le nom du destinataire, ainsi que sa clé publique est signé par l'autorité de certification. Il est donc possible de vérifier la validité du message en appliquant d'une part la fonction de hachage aux informations contenues dans le certificat, en déchiffrant d'autre part la signature de l'autorité de certification avec la clé publique de cette dernière, et en comparant ces deux résultats. **[18]**

2.2. Service d'authentification

L'authentification a pour but de garantir l'identité des correspondantes. Parmi les solutions simples qui existent, l'utilisation d'un identificateur et d'un mot de passe, une méthode de défi basé sur une fonction cryptographique et un secret, l'authentification peut s'effectuer par un numéro d'identification personnel, comme le numéro inscrit dans une carte à puce, ou code PIN.

L'authentification peut être simple ou mutuelle. Elle consiste surtout à comparer les données provenant de l'utilisateur qui se connecte à des informations, stockées dans un site protégé et susceptibles de piratage. Les sites mémorisant les mots de passe. **[16]**

- **Les protocoles**

Un protocole d'authentification est un moyen de contrôle d'accès caractérisé par les 3 A (AAA) qui signifient **A**uthentication, **A**uthorization, **A**ccounting, soit authentication, autorisation et compte en français. La signification de ces termes est la suivante :

- Authentication : consiste à vérifier qu'une personne/équipement est bien celle qu'elle prétend être.
- Autorisation : consiste à permettre l'accès à certains services ou ressources.
- Accounting : le serveur AAA a la possibilité de collecter des informations sur l'utilisation des ressources.

➢ **DIAMETER**

Diameter est un protocole d'Authentication conçu pour servir de support à l'architecture AAA, successeur du protocole Radius. Ce protocole est défini par la RFC 3588. Il a repris les principales fonctions de Radius (Diameter est compatible avec Radius) et en a rajouté de nouvelles pour s'adapter aux nouvelles technologies (IPv4 Mobile, NASREQ ...) et plus particulièrement offrir des services aux applications mobiles. Ce protocole se situe au niveau de la couche transport. Il utilise le port 3868 via le protocole TCP ou bien SCTP. **[19]**

➢ **TACACS+**

TACACS+ (**T**erminal **A**ccess **C**ontroller **A**ccess **C**ontrol **S**ystem **P**lus) est un protocole de sécurité inventé à la fin des années 90 par CISCO Systems. Même s'il a fini par remplacer les protocoles TACACS et XTACACS, TACACS+ n'est pas basé sur ces derniers. Ce protocole se situe au niveau de la couche transport. Il utilise le port 46 via le protocole TCP.

TACACS+ permet de vérifier l'identité des utilisateurs distants mais aussi, grâce au modèle AAA, d'autoriser et de contrôler leurs actions. **[19]**

➢ **PAP**

Le protocole PAP (**P**assword **A**uthentication **P**rotocol) utilise des mots de passe en texte brut et constitue le protocole d'authentification le moins sécurisé. Il est généralement négocié lorsque le client d'accès distant et le serveur d'accès distant ne disposent d'aucun moyen de validation plus sûr.

➢ **CHAP**

Le protocole CHAP (**C**hallenge **H**andshake **A**uthentication **P**rotocol) est un protocole

d'authentification par stimulation-réponse, qui utilise le modèle de hachage MD5 (**M**essage **D**igest 5) standard pour crypter la réponse. CHAP est utilisé par de nombreux fournisseurs de clients et de serveurs d'accès réseau. Un serveur exécutant routage et accès distant prend en charge CHAP pour que les clients d'accès distant exigeant CHAP soient authentifiés. Dans la mesure où CHAP exige l'utilisation d'un mot de passe crypté à l'envers, vous devez envisager un autre protocole d'authentification comme MSCHAP version 2.

- **Kerberos**

Kerberos est un protocole de sécurité originaire de monde Unix, il a pris un nouveau départ lorsqu'il a été choisi par Microsoft pour remplacer NTLM (**NT L**an **M**anager) dans Windows 2000. Kerberos a pour objectif :

- D'authentifier les utilisateurs ;
- De leur allouer des droits d'accès à des applications (sur un serveur) sur le réseau sous forme de ticket ou jetons d'accès périssables dans le temps ;
- D'assurer la transmission sécurisée de ces tickets ou jetons d'accès vers les applications et ressources demandées ;
- De protéger les échanges entre les utilisateurs et les applications. **[19]**

2.3. L'intégrité des données

Dans certaines cas, il peut être nécessaire d'assurer simplement que les données sont intégrés, c'est-à-dire qu'elles n'ont pas été au passage falsifiées par un intrus. Ces données restent claires, au sens ou elles ne sont pas secrètes.

2.4. Non répudiation

Elle fournit au récepteur/émetteur une preuve qui empêche l'émetteur/récepteur de l'envoi de message.

2.5. Contrôle d'accès

De nos jours, toutes les entreprises possédant un réseau local et aussi un accès à internet, afin d'accéder à la manne d'information disponible sur le réseau, et pouvoir communiquer avec l'extérieur. Cette ouverture vers l'extérieur est indispensable…et dangereuse en même temps.

Ouvrir l'entreprise vers le monde signifie aussi laisser place ouverte aux étrangers pour essayer de pénétrer le réseau local de l'entreprise, et y accomplir des actions douteuse, pour cela une architecture sécurisée est nécessaire.

Le cœur d'une telle architecture est basé sur un firewall (un pare-feu).

Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les

tentatives d'intrusion. Cela représente une sécurité supplémentaires rendant le réseau ouvert sur internet beaucoup plus sur. De plus, il peut permettre de restreindre l'accès interne de l'extérieur et l'accès vers l'extérieur de l'intérieur.

En effet, des employés peuvent s'adonner à des activités (exemple : les jeux en ligne) que l'entreprise ne cautionne pas. En plaçant un firewall, on peut limiter ou interdire l'accès à ces services, l'entreprise peut donc avoir un contrôle sur les activités se déroulant dans son enceinte.

Le firewall propose donc un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser, de sécurisé et de gérer le trafic réseau, et ainsi d'utiliser le réseau de la façon pour laquelle il a été prévu et sans l'encombrer avec des activités inutiles, et d'empêcher une personne sans autorisation d'accéder à ce réseau de données. Mais il ne fournit pas les services de sécurité tels que (authentification, intégrité, confidentialité, etc.).**[20]**

Sécurisation du Wi-Fi

Installer un réseau sans fil sans le sécuriser peut permettre à des personnes non autorisées d'écouter, de modifier et d'accéder à ce réseau. Il est donc indispensable de sécuriser les réseaux sans fil dès leur installation. Il est possible de sécuriser son réseau de façon plus ou moins forte selon les objectifs de sécurité et les ressources que l'on y accorde. La sécurité d'un réseau sans fil peut être réalisée à différents niveaux : configuration des équipements et choix des protocoles. **[4]**

1. Sécurité des points d'accès

La première chose à faire lors de la mise en place d'un réseau sans fil consiste à positionner intelligemment les points d'accès selon la zone que l'on souhaite couvrir. Eviter les murs extérieurs mais choisir plutôt un emplacement central. En se promenant autour de l'immeuble, on peut établir le périmètre à l'intérieur duquel la borne est accessible. Il n'est toutefois pas rare que la zone effectivement couverte soit largement plus grande que souhaitée, auquel cas il est possible de réduire la puissance de la borne d'accès afin d'adapter sa portée à la zone à couvrir. **[2]**

1.1. Eviter les valeurs par défaut

Lors de la première installation d'un point d'accès, celui-ci est configuré avec des valeurs par défaut, y compris en ce qui concerne le mot de passe de l'administrateur. Un grand nombre d'administrateurs en herbe considèrent qu'à partir du moment où le réseau fonctionne

il est inutile de modifier la configuration du point d'accès. Toutefois les paramètres par défaut sont tels que la sécurité est minimale. Il est donc impératif de se connecter à l'interface d'administration notamment pour définir un mot de passe d'administration.

D'autre part, afin de se connecter à un point d'accès il est indispensable de connaître l'identifiant du réseau (SSID). Ainsi il est vivement conseillé de modifier le nom du réseau par défaut et de désactiver la diffusion (broadcast) de ce dernier sur le réseau. Le changement de l'identifiant réseau par défaut est d'autant plus important qu'il peut donner aux pirates des éléments d'information sur la marque ou le modèle du point d'accès utilisé. L'idéal est même de modifiez régulièrement le nom SSID, Il faudrait même éviter de choisir des mots reprenant l'identité de l'entreprise ou sa localisation, qui sont susceptibles d'être plus facilement devinés. **[2]**

1.2. Filtrage des adresses MAC

Chaque adaptateur réseau possède une adresse physique qui lui est propre. Les points d'accès permettent généralement dans leur interface de configuration de gérer une liste de droits d'accès (appelée ACL) basée sur les adresses MAC des équipements autorisés à se connecter au réseau sans fil. Cette précaution un peu contraignante permet de limiter l'accès au réseau à un certain nombre de machines. En contrepartie cela ne résout pas le problème de la confidentialité des échanges. **[2]**

Remarque : certains adaptateurs permettent de modifier leurs adresses et donc de se faire passer pour d'autres adaptateurs se trouvant sur d'autres postes.

2. Sécurité des protocoles liés aux Wi-Fi

De nombreuses évolutions protocolaires ont rythmé la sécurité des réseaux Wi-Fi. Les objectifs sont les suivants :

- Garantir la confidentialité des données ;
- Permettre l'authentification des clients ;
- Garantir l'intégrité des données ;

Les différents protocoles sont :

2.1. WEP (Wired Equivalent Privacy)

Le WEP est un protocole pour sécuriser les réseaux sans fil de type Wi-Fi. Les réseaux sans fil diffusant les messages échangés par ondes radioélectriques, sont particulièrement

sensibles aux écoutes clandestines. Le WEP tient son nom du fait qu'il devait fournir aux réseaux sans fil une confidentialité comparable à celle d'un réseau local filaire classique.

2.1.1. Clé WEP

La clé de session partagée par toutes les stations est statique, c'est-à-dire que pour déployer un grand nombre de stations Wi-Fi, il est nécessaire de les configurer en utilisant la même clé de session. Ainsi la connaissance de la clé est suffisante pour déchiffrer les communications. De plus, 24 bits de la clé servent uniquement pour l'initialisation, ce qui signifie que seuls 40 bits de la clé de 64 bits servent réellement à chiffrer et 104 bits pour la clé de 128 bits.

2.1.2. Principe du WEP

Le principe du WEP consiste à définir dans un premier temps la clé secrète. Cette clé doit être déclarée au niveau du point d'accès et des clients. Elle sert à créer un nombre pseudo-aléatoire d'une longueur égale à la longueur de la trame. Chaque transmission de donnée est ainsi chiffrée en utilisant le nombre pseudo-aléatoire comme masque grâce à un OU Exclusif entre ce nombre et la trame.

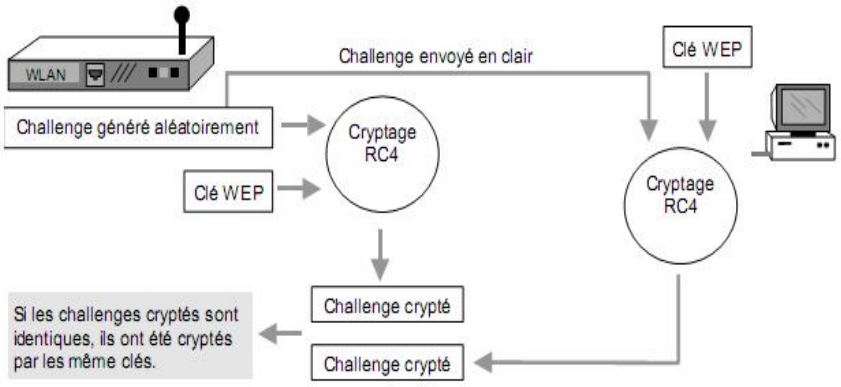

Figure II.6 : Principe du WEP

2.1.3. Failles du WEP

La faiblesse de WEP se situe dans son vecteur d'initialisation IV. Le IV est un nombre 24 bits qui est combiné avec la clef que l'administrateur réseau entre dans la configuration de son point d'accès. Un nouveau IV est utilisé pour chaque paquet transmis, il n'y a pas de problème ici. Par contre, le nombre IV n'est pas réellement un numéro aléatoire et peut être prédit par un panel. Ce qui est plus grave, le nombre IV se recycle lui même au bout d'un certain temps mais avec le même IV et la même clef avec un payload (contenu du message) différent. Si un

intrus collecte suffisamment de paquets (100 Mo à 1 Go), il sera capable de compromettre votre réseau.

Le WEP n'est donc pas suffisant pour garantir une réelle confidentialité des données. Pour autant, il est vivement conseillé de mettre au moins en œuvre une protection WEP 128 bits afin d'assurer un niveau de confidentialité minimum et d'éviter de cette façon 90% des risques d'intrusion.

2.2. WPA (Wi-Fi Protected Access)

Le WPA, développé par l'IEEE, est un autre protocole de sécurisation des réseaux sans fil offrant une meilleure sécurité que le WEP car il est destiné à en combler les faiblesses. En effet, le WPA permet un meilleur cryptage de données qu'avec le WEP car il utilise des clés TKIP (**T**emporal **K**ey Integrity **P**rotocol) - dites dynamiques - et permet l'authentification des utilisateurs. Ainsi, le WPA permet d'utiliser une clé par station connectée à un réseau sans fil, alors que le WEP lui utilisait la même clé pour tout le réseau sans fil. Les clés WPA sont en effet générées et distribuées de façon automatique par le point d'accès sans fil qui doit être compatible avec le WPA.

De plus, un vérificateur de données permet de vérifier l'intégrité des informations reçues pour être sûr que personne ne les a modifiées. **[9]**

2.2.1. Fonctionnement du WPA

WPA, lui est plus évolué avec un nombre IV de 48 bits: ce qui veut dire qu'il prendra beaucoup plus de temps avant que le nombre IV ne soit recyclé. Il faut également noter que dans la manière, WPA est supérieur dans sa méthode de connexion lorsque des utilisateurs sont connectés, ils sont authentifiés par des clefs pré-partagées, ou bien par des configurations plus sophistiquées, par une authentification (LDAP, RADIUS).

Une fois qu'un utilisateur est membre d'un réseau, une clef WPA est crée. Périodiquement, WPA va générer une nouvelle clef par utilisateur. Combiné à la longueur du nombre IV, ceci rend très difficile le piratage. Sur la transmission de chaque paquet, WPA ajoute un code de vérification d'intégrité de 4 bit (ICV) afin de les vérifier (injection de paquets, forge etc.). On peut donc conclure que l'utilisation de WPA est renforcée par rapport à la vérification WEP. Néanmoins un problème ici reste évident : Un attaquant peut intercepter la transmission, modifier le payload, recalculer le code d'intégrité, et le retransmettre sans que personne ne s'en aperçoive. WPA résout ce problème avec un message d'intégrité 8 bit : un payload crypté

et des facteurs dans le calcul de l'ICV réduise fortement les possibilités de forge de paquets (l'usurpation d'adresses IP sources).

2.2.2.TKIP (Temporal Key Integrity Protocol)

Protocole permettant le cryptage et le contrôle d'intégrité des données. Ce protocole utilise toujours le RC4 (d'où sa comptabilité avec le WEP) comme algorithme de cryptage avec une clé de 128 bits, par contre l'IV passe à 48 bits. De plus il y a une clé par station (et non une pour tout le réseau avec WEP), cette clé est générée et changer automatiquement de façon périodique. Le contrôle d'intégrité des données s'effectue par un code de hachage de 8 octets appelé MIC (**M**essage **I**ntegrity **C**ode) ou Michael. Ce code porte aussi les adresses MAC, ce qui évite de modifier ou forger des trames. De plus, il utilise un numéro de séquence sur les paquets, permettant un contrôle de bon séquencément.

2.3. WPA 2/ 802.11i

La dernière évolution en juin 2004, est la ratification de la norme IEEE 802.11i, aussi appelé WPA2 dans la documentation grand public. Ce standard reprend la grande majorité des principes et protocoles apportés par WPA, avec une différence notoire dans le cas du chiffrement : l'intégration de l'algorithme AES. Les protocoles de chiffrement WEP et TKIP sont toujours présents. Deux autres méthodes de chiffrement sont aussi inclus dans IEEE 802.11i en plus des chiffrements WEP et TKIP :

WRAP (**W**ireless **R**obust **A**uthenticated **P**rotocol) s'appuyant sur le mode opératoire OCB (**O**ffset **C**ode **B**ook) de AES ; CCMP (**C**ounter with **C**BC **M**AC **P**rotocol) : s'appuyant sur le mode opératoire CCM (**C**ounter with **C**BC-**M**AC) de AES ; Le chiffrement CCMP est le chiffrement recommandé dans le cadre de la norme IEEE 802.11i. Ce chiffrement, s'appuyant sur AES, utilise des clefs de 128 bits avec un vecteur d'initialisation de 48 bits. Ces mécanismes cryptographiques sont assez récents et peu de produits disponibles sont certifiés WPA2. Le recul est donc faible quant aux vulnérabilités potentielles de cette norme. Même si ce recul existe pour l'algorithme AES, le niveau de sécurité dépend fortement de l'utilisation et de la mise en œuvre d'AES.

La norme IEEE 802.11i définit deux modes de fonctionnement :

- **WPA Personal :** le mode « WPA personnel » permet de mettre en œuvre une infrastructure sécurisée basée sur le WPA sans mettre en œuvre de serveur d'authentification. Le WPA personnel repose sur l'utilisation d'une clé partagée, appelées PSK pour **P**ré-**S**hared **K**ey, renseignée dans le point d'accès ainsi que dans les postes clients. Contrairement au

WEP, il n'est pas nécessaire de saisir une clé de longueur prédéfinie. En effet, le WPA permet de saisir une phrase secrète, traduite en PSK par un algorithme de hachage. **[9]**

- **WPA Enterprise :** le mode entreprise impose l'utilisation d'une infrastructure d'authentification 802.1x basée sur l'utilisation d'un serveur d'authentification, généralement un serveur RADIUS, et d'un contrôleur réseau (le point d'accès). Cette solution est actuellement ce qu'il y a de plus sûr en termes de sécurité d'authentification forte. Mais attention, toutefois, rien n'est acquis et il y a fort à parier que cette solution ne restera pas à l'abri des hackers très longtemps. **[9]**

2.4. VPN (réseau privé virtuel)

Pour toutes les communications nécessitant un haut niveau de sécurisation, il est préférable de recourir à un chiffrement fort des données en mettant en place un réseau privé virtuel.

2.4.1. Concept de VPN

Une solution consiste à utiliser le réseau Wi-Fi comme support de transmission en utilisant un protocole d'encapsulation (en anglais tunneling, d'où l'utilisation impropre parfois du terme "tunnelisation"), c'est-à-dire encapsulant les données à transmettre de façon chiffrée. On parle alors de réseau privé virtuel (noté RPV ou VPN, acronyme de **V**irtual **P**rivate **N**etwork) pour désigner le réseau ainsi artificiellement créé. Le système de VPN permet donc d'obtenir une liaison sécurisée à moindre coût, si ce n'est la mise en œuvre des équipements terminaux.

2.4.2. Fonctionnement

Un réseau privé virtuel repose sur un protocole, appelé protocole de tunnelisation (tunneling), c'est-à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie. Le terme de "tunnel" est utilisé pour symboliser le fait qu'entre l'entrée et la sortie du VPN les données sont chiffrées (cryptées) et donc incompréhensible pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. Dans le cas d'un VPN établi entre deux machines, on appelle client VPN l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client) et serveur VPN, l'élément chiffrant et déchiffrant les données du côté de l'organisation.

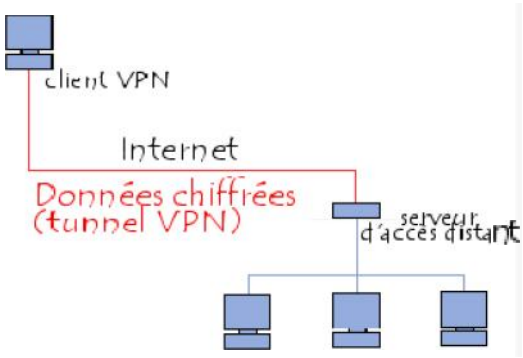

Figure II.7 : Principe de VPN

2.5. 802.1x

Le protocole 802.1x est une solution de sécurisation d'un réseau mis au point par l'organisme de standardisation IEEE en 2001. Il a pour but de contrôler l'accès à un réseau filaire ou sans fil grâce à un serveur d'authentification. Le standard permet de mettre en relation le serveur d'authentification et le système à authentifier par des séquences par des échanges EAP. Le protocole 802.1x va donc unifier les différents méthodes d'authentification sous la même bannière : le protocole EAP.

La principale innovation amenée par le standard 802.1x consiste à scinder le port logique, qui est connectés en parallèle sur le port physique. Le premier port logique est dit "contrôle", et peut prendre deux états "ouvert" ou "fermé". Le deuxième port logique est lui toujours accessible mais il ne gère que les trames spécifique à 802.1x. Cela permet de gérer le dialogue nécessaire à l'authentification au préalable à une connexion réseau. La connexion initiale est donc limitée à un usage de sécurité qui ouvre ultérieurement le canal des données en cas d'authentification réussie. **[19]**

802.1x est aussi appelé Port-based Network Access Control, c'est-à-dire qu'il introduit une notion de port contrôlé par l'authentification. Une station ne pourra accéder aux ressources d'un LAN que si elle a été auparavant authentifiée.

Le protocole fonctionne à partir de trois éléments :

- **Le client (supplicant) :** c'est le système à authentifier c'est-à-dire l'élément qui désire se connecter sur le réseau ;
- **Le contrôleur (point d'accès) :** ou système authentificateur c'est-à-dire l'élément qui va demander l'authentification;
- **Le serveur d'authentification :** Ce serveur d'authentification est en général un serveur Radius. Selon la requête du supplicant, ce serveur détermine les services auxquels le demandeur a accès (serveur placé sur le LAN).

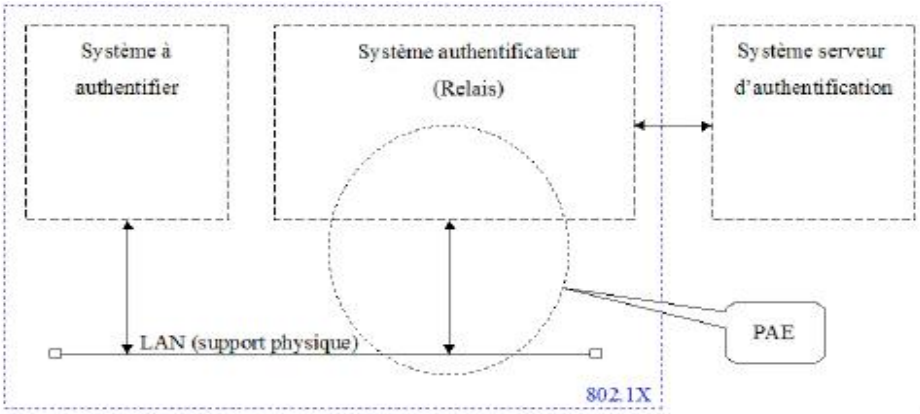

Figure II.8 : Les trois entités qui interagissent dans le 802.1x

La communication entre ces éléments fait intervenir différents protocoles suivant un principe de fonctionnement spécifique.

2.5.1.Mécanisme générale

Le supplicant souhaite accéder aux ressources du réseau, mais pour cela il va devoir s'authentifier. Le système authentificateur gère cet accès via le PAE (**P**ort **A**ccess **E**ntity) ; ce PAE est divisé en deux ports, un port contrôlé (connexion ouverte ou fermée) donnant accès à la ressource en cas de succès de l'authentification, et un port non contrôlé (connexion toujours ouverte) servant à l'authentification où tout autre trafic est rejeté.

Le port contrôlé peut être ouvert ou fermé suivant le contrôle qui a été défini au moyen d'une variable (Auth Controlled Port Control). Cette variable peut prendre trois états :

- **ForceUnauthorized :** l'accès au port contrôlé est interdit (connexion toujours ouverte).
- **ForceAuthorized :** l'accès au port contrôlé est autorisé (connexion toujours fermée).
- **Auto (par défaut) :** l'accès dépend du résultat de l'authentification.

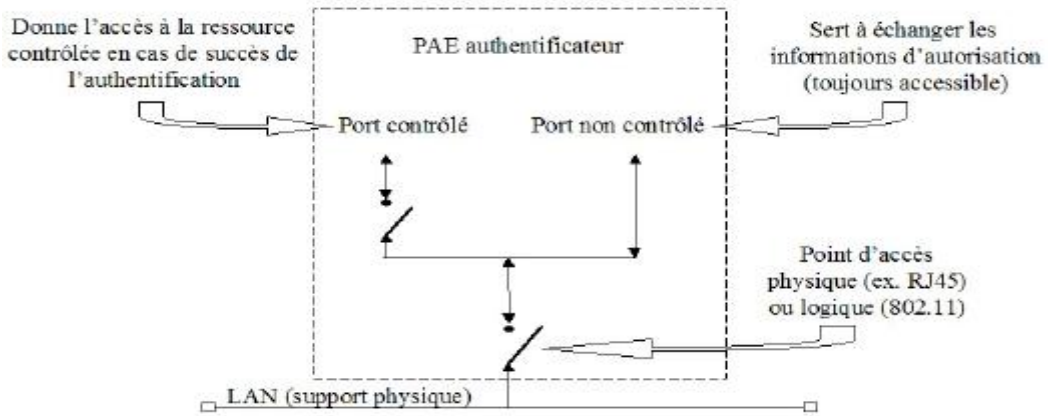

Figure II.9 : PAE

L'utilisation du 802.1x en Wi-Fi permettra l'authentification du demandeur, le contrôle d'accès aux bornes et la distribution des clés WEP. Mais attention, il faut que le 802.1x soit bien implémenté sur les différentes machines. Si les implémentations sur les bornes et serveurs sont disponibles, il n'en est pas de même chez les postes clients. Le 802.1x est maintenant de plus en plus intégré avec le système d'exploitation. **[21]**

2.5.2.EAP (Extensible Authentification Protocol)

EAP est une extension de PPP définie par la RFC 2284. Il permet l'authentification des utilisateurs du lien selon de nombreuses méthodes possibles. En somme, on peut dire que l'EAP est une sorte de protocole "parapluie" pour l'authentification : il détermine un schéma d'authentification (Kerberos, mot de passe jetable, PKA, etc.). **[14]**

Une extension d'EAP s'appelle EAPOL pour "**EAP O**ver **L**an". Celle-ci permet de faire transiter des requêtes EAP à travers un réseau LAN en direction d'un serveur compétent qui se chargera de passer la requête EAPOL en EAP.

2.5.2.1. Composition du paquet EAP

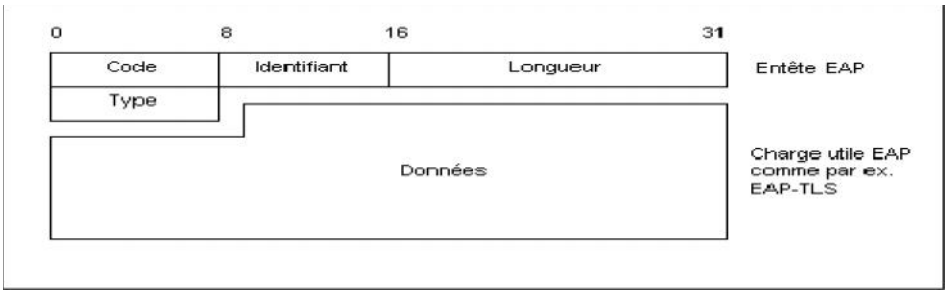

Figure II.10 : Paquet EAP

- **Champ code**

Dans l 'en-tête du paquet EAP, le champ code correspond au premier octet.

Il en existe 4 types : **[22]**

- Request : le système authentificateur émet une requête d'information auprès du supplicant.
- Response : le supplicant répond à la requête du système authentificateur.
- Success : le système authentificateur informe le supplicant du succès de la demande d'authentification.
- Failure : le système authentificateur informe le supplicant de l'échec de la demande d'authentification.

- **Champ identifiant**

Codé sur un octet également, il sert à identifier une session d'authentification. Ce champ change pour chaque nouvelle requête ou réponse. Si une duplication d'une requête doit être faite, l'identifiant ne change pas. **[22]**

- **Champ longueur**

Codé sur 2 octets, il indique la longueur de l'ensemble du paquet EAP, il prend donc en compte la longueur des données mais aussi des longueurs des autres champs de l'entête comme le type, le code...

Ainsi on connaîtra la taille des données utiles même en cas de bourrage par la couche liaison. **[22]**

- **Champ type**

Ce champ est codé sur un octet et définit le type de données que contient le paquet EAP. Logiquement, requête et réponse possèdent des trames de même type.

Nous allons particulièrement nous intéresser au champ type lors des communications requête / réponse. **[22]**

2.5.2.2. Méthodes d'authentification associés a EAP

Le standard 802.1x ne propose pas une seule méthode d'authentification mais un canevas sur lequel sont basés plusieurs types d'authentification. Ainsi, une méthode d'authentification EAP utilise différents éléments pour identifier un client :

- Login / mot de passe ;
- Certificats ;
- Carte à puce ou calculette ;

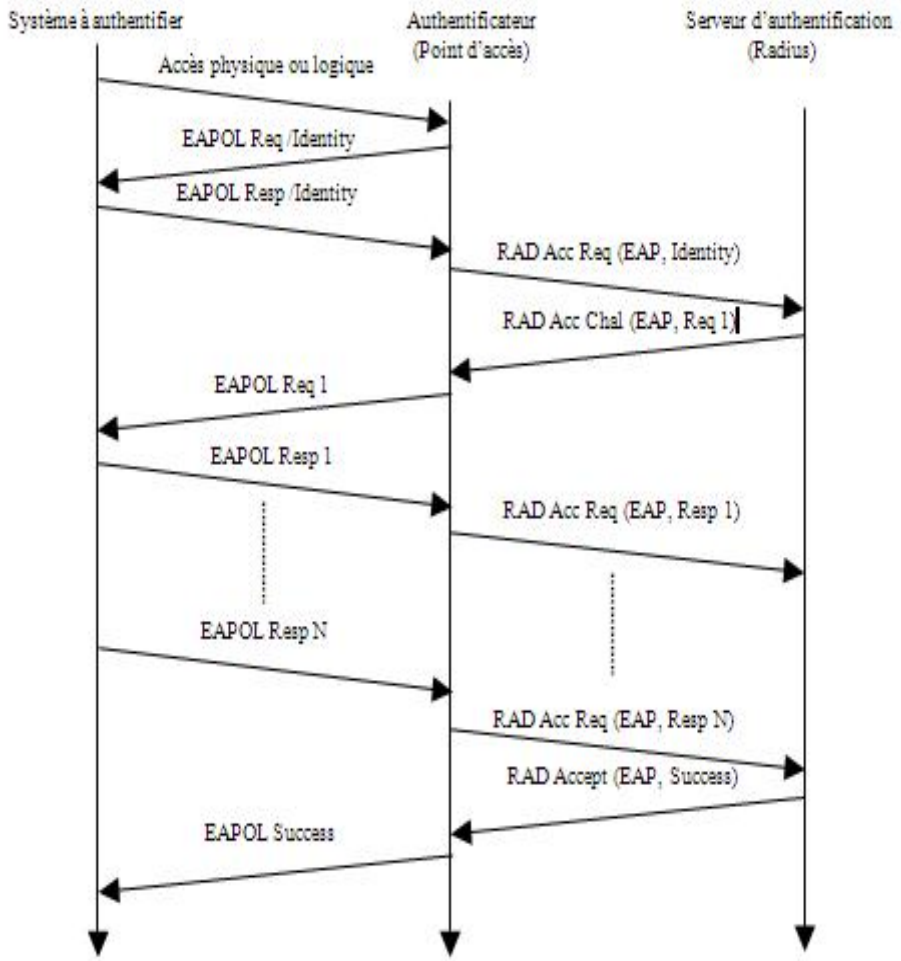

Figure II.11 : Séquence d'authentification 802.1x

a. Méthodes basées sur les mots de passes [22]

- **LEAP:** (**L**ightweight **E**xtensible **A**uthentification **P**rotocol) c'est la méthode la plus utilisée pour les points d'accès. Il gère la distribution dynamique de clés WEP. C'est aussi à la base une solution propriétaire de Cisco (CISCO-EAP) mais qui a aussi été implémentée par la suite par d'autres constructeurs.
- **EAP-MD5:** (**EAP-M**essage **D**igest **5**) il est souvent utilisé pour les informations d'authentification des clients, par un système basé sur le nom d'utilisateur et le mot de passe. Il n'existe pas d'authentification du serveur. Une machine qui se fait passer pour un serveur peut ainsi facilement récupérer les authentifiants (login, mot de passe) de la machine qui cherche à s'authentifier.
- **EAP-SKE:** (**EAP-S**hared **K**ey **E**xchange) il permet une authentification mutuelle ainsi qu'une itinérance entre les réseaux de plusieurs fournisseurs d'accès Internet.
- **EAP-SRP:** Il s'agit de l'adaptation du protocole SRP (RFC2945) à l'EAP.

b. Méthodes basées sur les certificats

- **EAP-TLS:** utilise le mécanisme d'authentification à clé publique de TLS. Client et serveur doivent posséder un certificat. Permet l'authentification mutuelle, l'échange des clés (WEP dynamique ou TKIP), la fragmentation et le réassemblage, la reconnexion rapide.
- **EAP-TTLS:** méthode du tunnel TLS. Fournit une séquence d'attributs inclus dans le message. En incluant un attribut de type RADIUS, EAP peut fournit les mêmes fonctionnalités que PEAP. Cependant, si un mot de passe RADIUS ou CHAP est encapsulé, il est chiffré par TLS. Cette méthode est moins utilisée que PEAP qui rend les mêmes services.
- **PEAP:** (**P**rotected **EAP)** authentification sans certificat. Ajoute une couche TLS sur EAP (comme EAP-TTLS), permet d'authentifier le serveur au client mais pas l'inverse, c'est la méthode protégée par PEAP qui doit authentifier le client. Offre les services d'authentification (impossible de falsifier ou insérer des messages EAP), de chiffrement, d'échange de clé (WEP dynamique ou TKIP), fragmentation et réassemblage, reconnexion rapide.
- **PEAP Microsoft:** supporte l'authentification du client via MS-CHAP v2 uniquement réduisant ainsi le champ d'utilisation au domaine NT et ADS.

c. Méthodes basées sur les cartes à puces

- **EAP-SIM:** (**EAP** - **S**ubsciber **I**dentity **M**odule) utilisé pour les points d'accès public (hot spot), utilise la carte à puce SIM du GSM, permet la mise en place de facturation.
- **EAP-AKA:** (**EAP** - **A**uthentification and **K**ey **A**greement) utilise le système d'authentification de la carte SIM de l'UMTS, il est compatible avec le GSM.

2.5.3.Faiblesses 802.1x

La principale faiblesse de 802.1x vient de ce qu'il a été conçu au départ dans un contexte de connexion physique (type accès PPP sur RTC). Rien n'empêche en effet un utilisateur d'insérer un hub (transparent à 802.1x) et de faire bénéficier d'autres utilisateurs de l'ouverture du port Ethernet d'un commutateur. La plupart des implémentations d'équipementiers permettent de surmonter cette difficulté en permettant de configurer un blocage du port Ethernet si l'adresse MAC du système authentifié change. Les attaques par écoute et rejeu sont aussi possibles, ainsi que le vol de session des faiblesses de 802.1x. Les attaques sur 802.1x sont, de plus, facilitées dans le cas de l'Ethernet sans fil.

2.6. Protocole Radius

2.6.1. Présentation

RADIUS (**R**emote **A**uthentification **D**ial **I**n **U**ser **S**ervice) est un protocole d'authentification client/serveur habituellement utilisé pour l'accès à distance, défini par la RFC 2865. Ce protocole permet de sécuriser les réseaux contre des accès à distance non autorisés. Ce protocole est indépendant du type de support utilisé. **[14]**

Le protocole Radius repose principalement sur un serveur (serveur Radius), relié a une base d'identification (fichier local, base de données, annuaire LDAP, etc.) et un client Radius, appelé NAS (**N**etwork **A**ccess **S**erver), faisant office d'intermédiaire entre l'utilisateur final et le serveur. Le mot de passe servant à authentifier les transactions entre le client Radius et le serveur Radius est chiffré et authentifier grâce a un secret partagé.

Il est à noter que le serveur Radius peut faire office de proxy, c'est-à-dire transmettre les requêtes du client a d'autres serveurs Radius.

2.6.2. Principe de fonctionnement

Le fonctionnement de Radius est basé sur un scénario proche de celui-ci :

1. Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance ;
2. Le NAS achemine la demande au serveur Radius ;
3. Le serveur Radius consulte la base de données d'identification afin de connaître le type de scénario d'identification demandé pour l'utilisateur. Soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur. Le serveur Radius retourne ainsi une des quatre réponses suivantes :

- **ACCEPT :** l'identification a réussi ;
- **REJECT :** l'identification a échoué ;
- **CHALLENGE :** le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un « défi » (en anglais « *challenge* ») ;
- **CHANGE PASSWORD :** le serveur Radius demande à l'utilisateur un nouveau mot de passe.

Suite à cette phase d'authentification débute une phase d'autorisation ou le serveur retourne les autorisations aux utilisateurs.

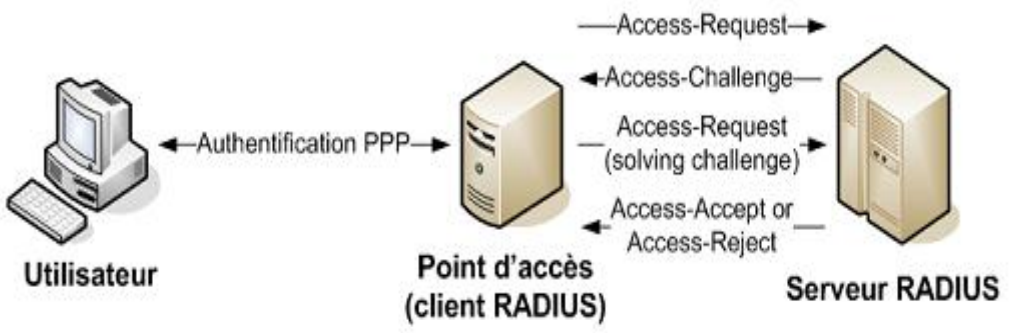

Figure II.12 : Principe de fonctionnement de Radius

- **Paquets Radius**

Un paquet Radius est inclus dans un et un seul paquet UDP. Le schéma suivant représente un paquet Radius standard, les unités étant exprimées en octets :

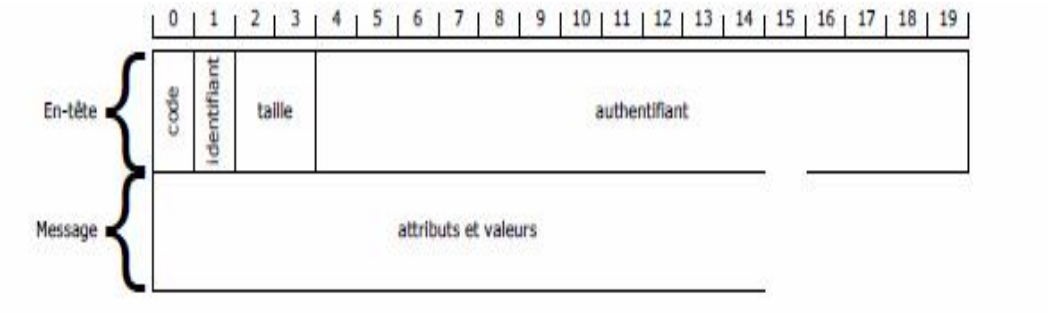

Figure II.13 : Paquets Radius

- **Code :** identifie le type de message

Code	Description
Access - Request	Demande accès à un service
Access -Accept	Réponse favorable à la demande du client
Access - Reject	Réponse négative au client
Accounting - Request	Demande les informations d'authentification
Accounting - Response	Informations d'authentification
Access - challenge	Sollicite des informations supplémentaires pour l'autorisation du client

Tableau II.2 : Description du champ code

- **Identifiant :** permet de reconnaitre les messages (requêtes et réponses) d'une même session d'authentification.
- **Longueur (taille) :** définie la longueur de la trame.
- **Authentificateur :** permet au client d'authentifier la réponse de serveur Radius et de protégé les mots de passe (évite le phénomène « man in the middle » par exemple). Il contient également la méthode d'authentification à utiliser avec le client.
- **Attributs :** ce champ est utilisé pour véhiculer toutes les informations nécessaires, il a pour format :

Type	Longueur	Valeur

Figure II.14 : Format des attributs Radius

Conclusion

En prenant connaissance des faiblesses de sécurité des réseaux de type Wi-Fi et au vu de l'essor important de ce type de matériel, il est probable que le marché des serveurs d'authentification va prendre de l'importance. Ainsi, depuis les tests, certains produits ont déjà beaucoup évolué pour prendre en charge davantage de méthodes d'authentification et de plateformes. Cependant, sur le segment de la sécurité des réseaux Wi-Fi, d'autres solutions restent envisageables notamment celles basées sur les VPN.

Le niveau de sécurité proposé par 802.1x est correct mais il ne permet pas de résoudre les problèmes liés aux faiblesses de WEP. Ainsi, pour proposer une architecture vraiment sûre il faudra utiliser d'autres techniques de chiffrement comme WPA et attendre les avancées proposées par 802.11i. La relative jeunesse de tous ces protocoles, et des réseaux Wi-Fi en général, ne permettent pas encore de garantir une pérennité de la solution retenue. Malgré tout, il est nécessaire de prendre le risque d'opter pour une solution plutôt que d'attendre et de laisser son réseau sans fil sans protection.

Chapitre III Mise en place d'une sécurité basée sur le 802.1x et un serveur d'authentification

Introduction

Pour la réalisation de ce projet, il a fallu mettre en place un réseau test, ceci a nécessité la mise en place d'un serveur d'authentification radius, et d'un mécanisme de génération de certificats. Nous avons opté pour l'installation de ces outils dans un environnement LINUX, d'une part parce qu'ils sont en Open Source, et d'autre part, ils sont moins vulnérables aux attaques.

- **Systèmes d'exploitation utilisés**

- Linux mandriva 2010.2 pour le serveur
- Windows XP pour les postes clients

Dans ce chapitre, on va détailler les étapes de l'installation des programmes nécessaires à notre expérimentation.

1. Installation et configuration d'OpenSSL

1.1. Installation

On a utilisé la version openssl-0.9.7g téléchargé sur le site www.openssl.org

On commence par la décompression du fichier pour l'installer en utilisant la commande suivante :

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

Openssl se compile, cela dure plus ou moins longtemps suivant la machine utilisée. Une fois la compilation terminée, un message comme ci-dessous s'affichera.

Figure III.1 : Compilation d'Openssl

1.2. Configuration

Il faut maintenant éditer le fichier de configuration d'openssl. Ce fichier contient différentes informations comme : le nom de l'entreprise, le pays, l'adresse e-mail, le nom du propriétaire du certificat…

L'Edition via l'éditeur de texte (nous utiliserons **gedit**) du fichier de configuration openssl.cnf

gedit /usr/local/openssl-certgen/ssl/openssl.cnf

Vers le milieu du fichier se trouve les paramètres à modifier : toutes les lignes qui sont de la forme XXX_default (Comme encadré ci-dessous) :

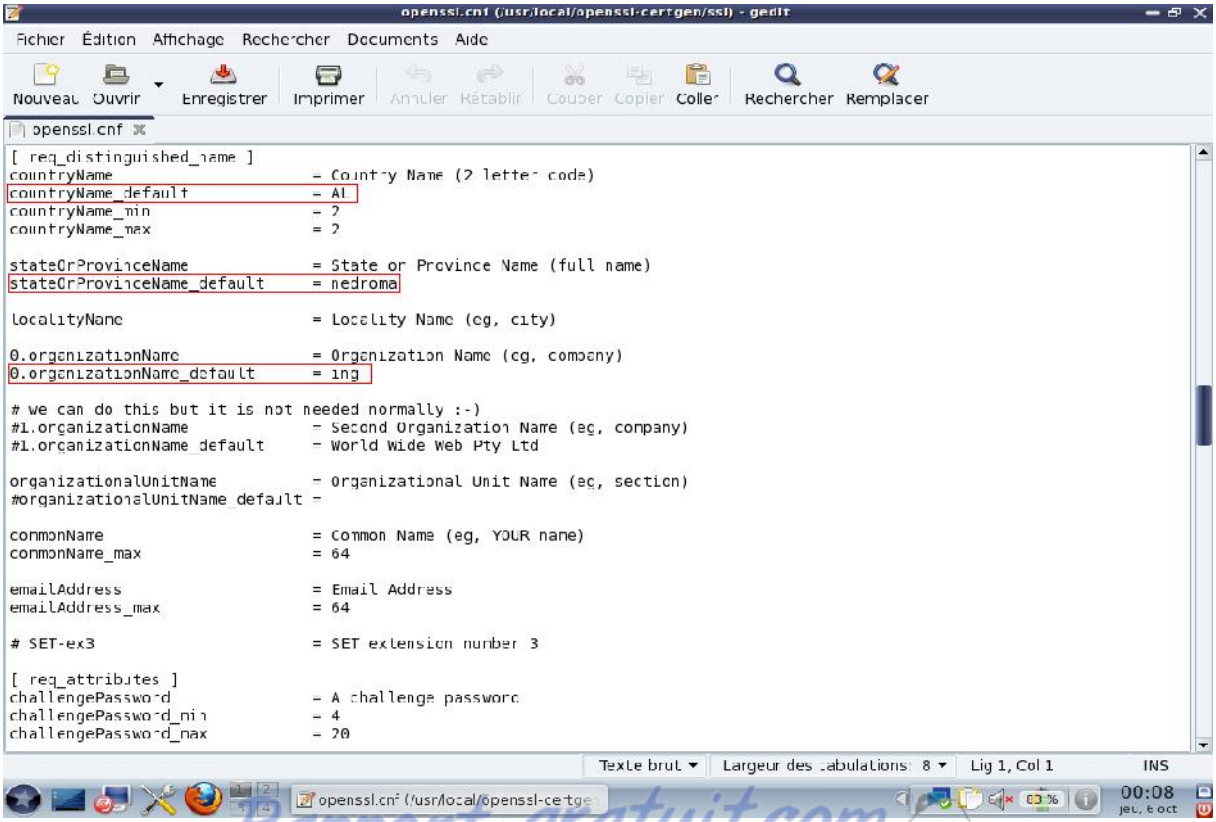

Figure III.2 : Les informations à remplir sur SSL

L'installation d'openssl est terminée.

2. Générations des certificats

Sur le site ***http://www.nantes-wireless.org/actu/article.php3?id_article=8***, nous pouvons trouver les scripts suivants : **xpextensions**, **CA.root**, **CA.svr**, **CA.clt**

Ceux-ci nécessaires à la génération des certificats.

Possédant déjà les scripts, il nous reste seulement à les copier dans le chemin approprié :

/usr/local/openssl-certgen/ssl

Attention à ne pas oublier de copier le fichier **xpextensions** contenant les OID pour la génération des certificats.

2.1. Génération du certificat root

Le certificat root lui même autorité de certification sera générer par le fichier CA.root, permettant aussi la signature des autres certificats (client, serveur,…).

Le lancement du certificat root se fera par la commande suivante :

```
[/usr/local/openssl-certgen/ssl] # chmod 700 CA.root
[/usr/local/openssl-certgen/ssl] # ./CA.root
```

A chaque question appuyée sur la touche entrer. Une fois cette série terminée (questions), la création des fichiers **root.pem**, **root.der**, **root.p12** et dossier demoCA se fera d'elle-même (dans le chemin: **/usr/local/openssl-certgen/ssl**). Le fichier root.pem est utilisé par freeradius, et il faudra installer le root.der sur chaque station client.

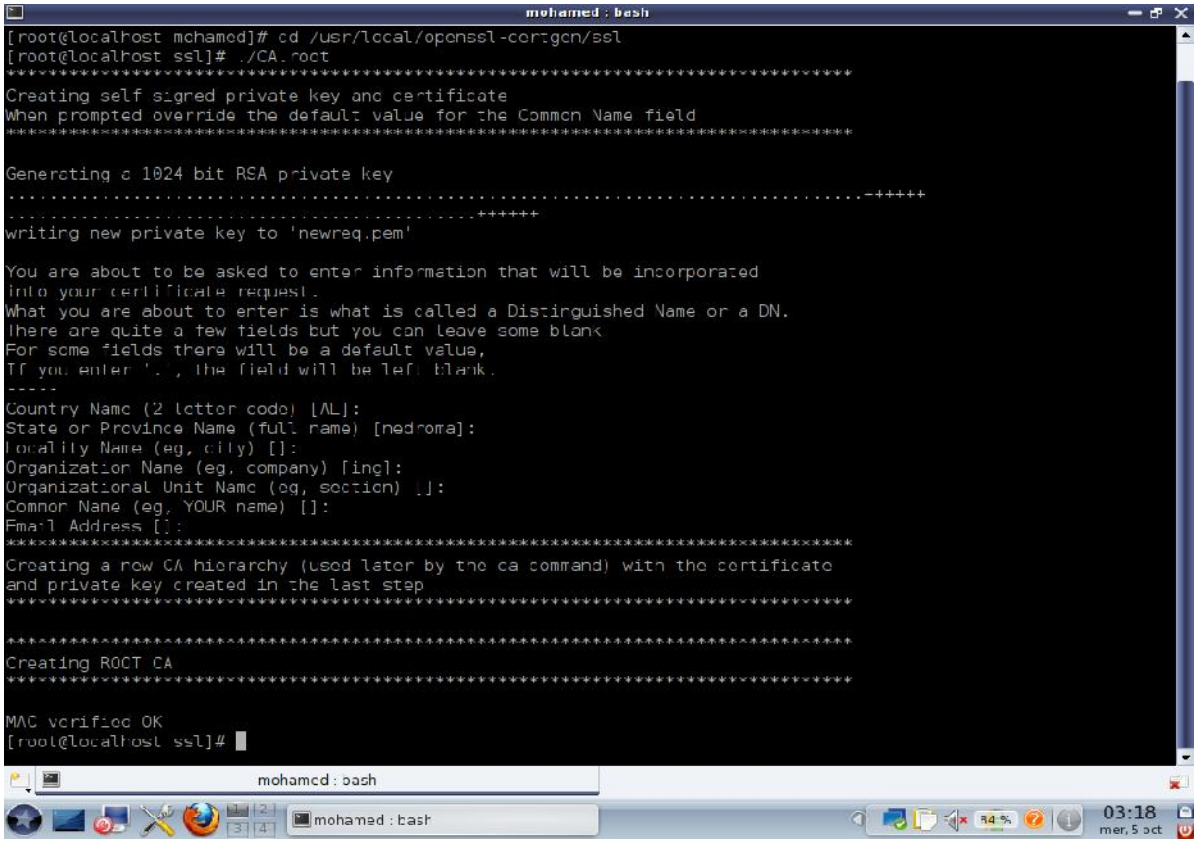

Figure III.3 : Génération du certificat root

2.2. Génération du certificat serveur

Avant d'exécuter ce script, il faut s'assurer que le fichier serial est présent dans le répertoire demoCA (crée à l'étape précédente). Dans le cas où celui-ci (serial) n'existe pas, il faudra donc le crée, puis placer une valeur hexadécimale dans ce même fichier.

A la différence du certificat root, nous devrons ajouter dans un premier temps un paramètre supplémentaire qui sera le nom du fichier que nous désirons obtenir (nom du serveur). Celui-ci devra être inscrit à la suite de l'exécution du script CA.svr comme suivant :

[/usr/local/openssl-certgen/ssl] # chmod 700 CA.svr

[/usr/local/openssl-certgen/ssl] # ./CA.svr **serveur**

Dans un second temps, il faudra répondre aux questions comme précédemment (touche entrer), ceci étant dit à la question ***Common Name (eg, YOUR name) [] :*** nous devrons répondre en utilisant le paramètre ajouté (comme ci-dessus : serveur).

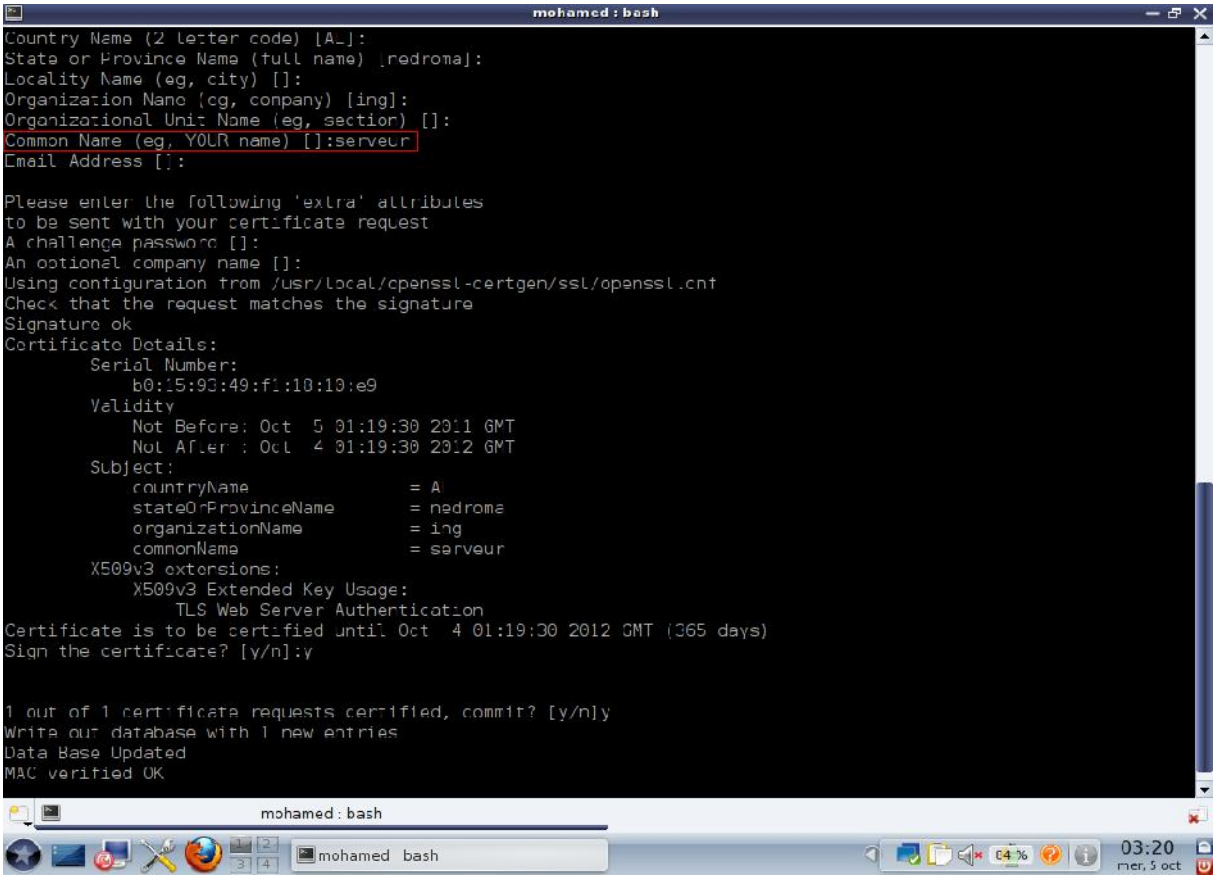

Figure III.4 : Génération du certificat serveur

On se retrouve donc avec les fichiers **serveur.pem**, **serveur.der**, **serveur.p12**, dont le dernier devra être installé sur chaque ordinateur client.

2.3. Génération du certificat client

Nous devrons réitérer la même manipulation (certificat serveur) afin d'obtenir le certificat client. Sauf qu'à la question ***Common Name (eg, YOUR name) [] :*** il faudra simplement inscrire le nom de l'utilisateur (ici se sera **wissame**) comme ci-dessous :

```
[/usr/local/openssl-certgen/ssl] # chmod 700 CA.clt
[/usr/local/openssl-certgen/ssl] # ./CA.clt wissame
```

On aura donc les 3 fichiers suivants : **wissame.pem, wissame.der, wissame.p12** dont le dernier devra être installé sur chaque ordinateur client.

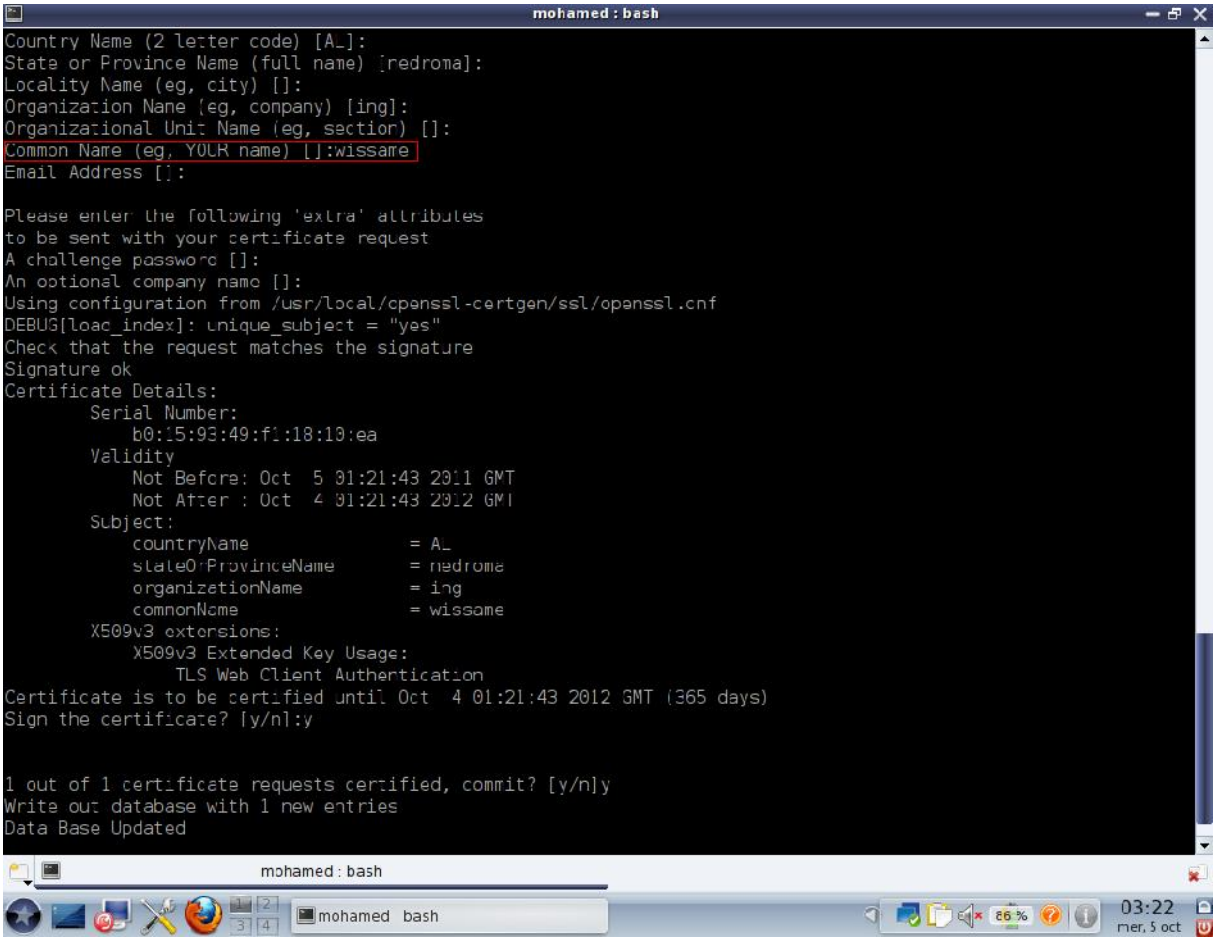

Figure III.5 : Génération du certificat client

Cependant il est impossible d'avoir 2 certificats avec le même nom d'utilisateur.

Une fois la génération des certificats est terminée, nous sommes passés à l'installation de freeradius.

3. Installation et configuration de freeradius

3.1. Installation

Version utilisé : freeradius-1.0.4 téléchargé sur le site www.freeradius.org

```
tar zxvf freeradius-1.0.4.tar.gz
cd freeradius-1.0.4
```

3.2. Configuration

Pour la configuration et la compilation de freeradius, on utilise le paramètre **--sysconfdir=/etc** qui placera tous les fichiers de configuration dans **/etc/raddb.**

```
./configure –sysconfdir=/etc
```

Important : Il faut vérifier pendant la configuration qu'il n'y a pas d'erreur au niveau d'EAP-TLS.

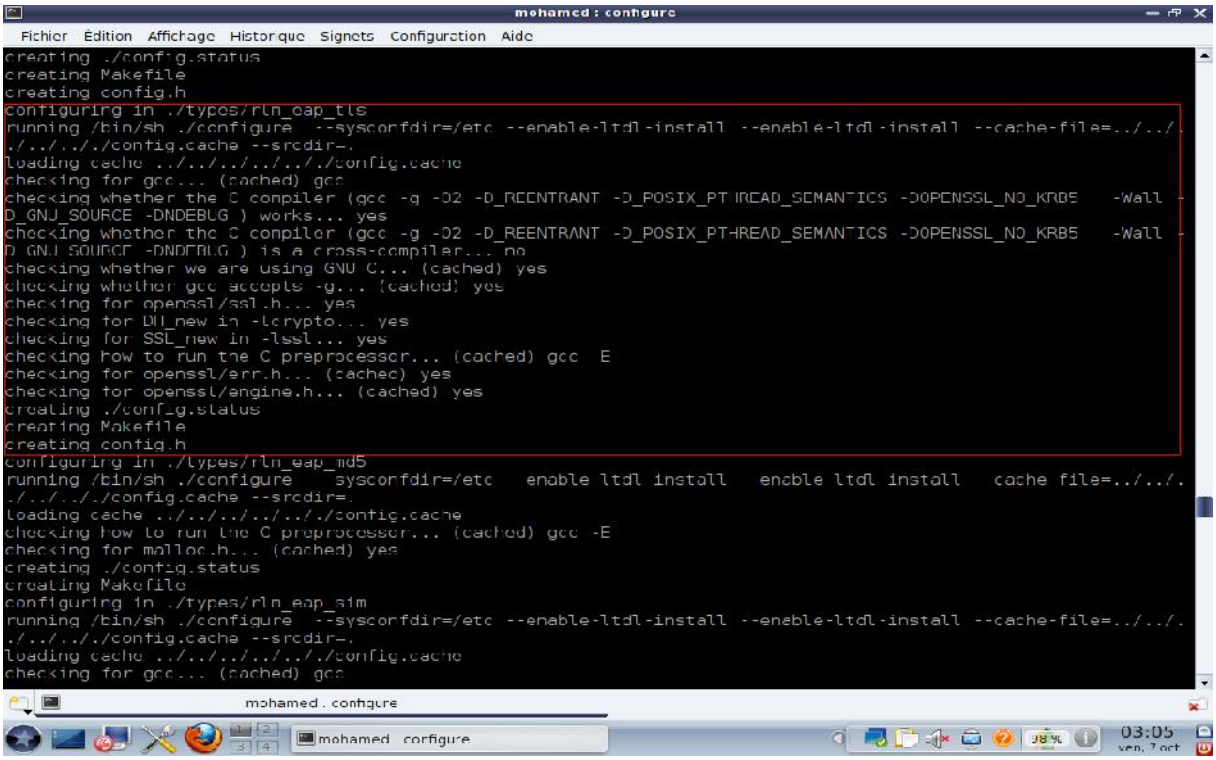

Figure III.6 : Configuration sans erreurs au niveau d'EAP-TLS

On peut passer à la compilation et l'installation de freeradius :

```
make
make install
```

Une fois l'installation terminée, un message comme ci-dessous s'affichera.

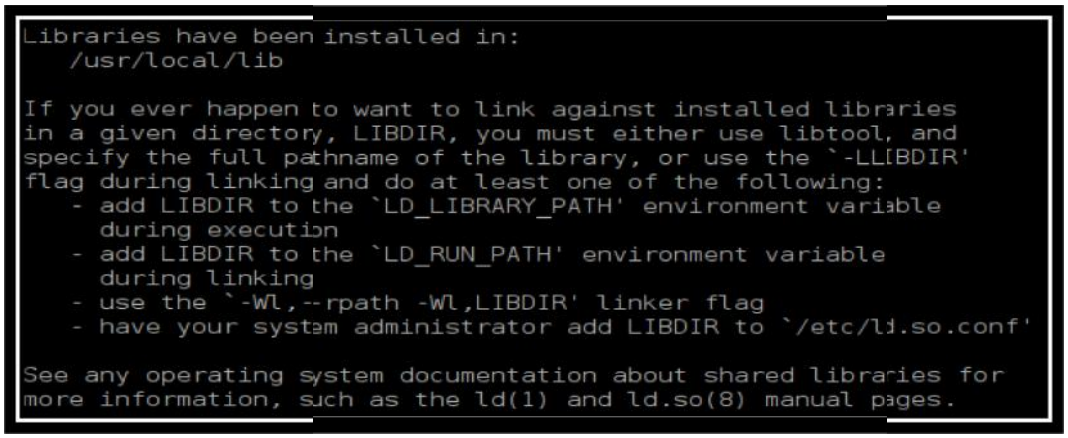

Figure III.7 : Fin d'installation de freeradius

Maintenant que freeradius est bien installé, il nous faut copier fans un première temps les certificats serveur.pem, root.pem dans le répertoire **/etc/raddb/certs** en utilisant la commande **cp**.

```
cd /etc/raddb/certs
rm –rf *
cp /usr/local/openssl-certgen/ssl/root.pem /etc/raddb/certs
cp /usr/local/openssl-certgen/ssl/serveur.pem /etc/raddb/certs
```

Dans un second temps, nous allons générer deux fichiers aléatoires : **dh** et **random**, qui vont nous permettre de mieux sécuriser notre serveur radius.

```
[/etc/raddb/cers]# openssl dhparam –check –text -5 512 –out dh
```

Enfin créez et compiler ce court programme en C pour générer un fichier comportant des caractères aléatoires.

```
[/etc/raddb/certs]# touch random.c
[/etc/raddb/certs]# gedit random.c
```

Copiez ces quelques lignes de C dans le fichier random.c :

```
#include <stdio.h>
#include <openssl/rand.h>
// you will need to compile it with openssl lib
// $ gcc –lcrypto
main void {
unsigned char buf[100] ;
if ( !RAND_bytes[buf, 100]) {
// the usual md5(time+pid)
}
Printf("Random : %s\n", buf) ;
}
```

Puis exécutez la commande suivante :

```
[/etc/raddb/certs]# gcc random.c –o random -lcrypto
```

A noter que cette commande diffère selon la version de linux.

Tester avec la commande :

```
[/etc/raddb/certs]# ./random
```

Le test donne quelque chose qui ressemble à ça :

3.3. Fichiers de configuration de freeradius

Les fichiers de configuration se trouvent dans **/etc/raddb** (comme nous l'avons précisé plus tôt via le --sysconfdir), ces fichiers sont très bien commentés et constituent la documentation de freeradius. La section suivante présente les fichiers de configuration principaux a modifié:

- **eap.conf :** pour la configuration des méthodes EAP d'authentification. Le contenu de ce fichier était au départ inclus dans la partie module du fichier « radiusd.conf » mais les développeurs ont préféré le séparer pour des raisons de lisibilité car il devenait de plus en plus volumineux du fait du nombre de méthodes d'authentification EAP différentes. En fonction des méthodes EAP que le serveur devra supporter dans son environnement de production il y aura éventuellement certains paramètres à configurer. Par exemple dans le cas d'une authentification via EAP-TLS, il faudra indiquer le répertoire contenant le certificat du serveur (qu'il enverra au supplicant) et la clé privée avec le mot de passe associé, celui contenant le certificat de l'autorité (qui permettra de vérifier le certificat fourni par le supplicant), indiquer si le serveur doit vérifier un fichier contenant les certificats révoqués ou encore s'il faut vérifier que le nom de l'utilisateur correspond au nom du propriétaire du certificat fourni.

- **clients.conf :** pour définir et paramétrer le dialogue avec les authentificateurs. Ici sont recensés les authentificateurs via un nom, une adresse IP et un secret partagé. D'autres informations optionnelles peuvent être ajoutées pour éviter les connexions simultanées d'un même utilisateur.

- **users :** est le fichier des utilisateurs. Un utilisateur est défini par son nom et sa méthode d'authentification (en fonction des méthodes, ce fichier peut contenir des mots de passe).

- **radiusd.conf :** pour la configuration globale du serveur. Ce fichier est découpé en deux grandes parties, d'abord les paramètres propres au démon (interfaces d'écoute, port, etc.), puis une partie définition des modules (définition et configuration des modules d'authentification disponibles hormis ceux du type EAP qui sont traités séparément, des modules de journalisation, de relayage des requêtes, etc.).

➢ Fichier eap.conf

```
gedit /etc/raddb/eap.conf
```

On spécifie que l'on veut utiliser EAP-TLS et non MD5
Ligne 22

```
default_eap_type = tls
```

Après on configure EAP-TLS, il faut que l'on enlève les commentaires (les # devant) a partir de la ligne 122 et on modifie les chemins des certificats :

```
tls {
        private_key_password = whatever
        private_key_file = ${raddbdir}/certs/serveur.pem
        certificate_file = ${raddbdir}/certs/serveur.pem
        CA_file = ${raddbdir}/certs/root.pem
        dh_file = ${raddbdir}/certs/dh
        random_file = ${raddbdir}/certs/random
        fragment_size = 1024
        include_length = yes
#       check_crl = yes
        check_cert_cn = %{User-Name}
}
```

private_key_password : est le mot de passe du certificat serveur (par default est whatever on peut le modifier en éditant le fichier CA.svr).
private_key_file et certificate_file : est le chemin vers le certificat serveur.
CA_file : est le chemin pour le certificat racine.
dh_file et random_file : sont les chemins vers les fichiers aléatoires qu'on a générer précédemment
check_cert_cn : permet de vérifier que le nom d'utilisateur fournit par le client est le même que celui dans le certificat (utile car certain driver propose de choisir le nom d'utilisateur et le certificat).

check_crl : est le seul paramètre qu'on laisse commenter, il permet de vérifier si le certificat n'a pas été révoqué.

- **Fichier clients.conf**

```
gedit /etc/raddb/eap.conf
```

Ce fichier permet de définir la liste des AP que l'on autorise à accéder au serveur radius. Le serveur et l'AP partagent un secret (une clé) pour crypter les données.
Par default on autorise le localhost (127.0.0.1) avec comme secret : testing123 (pour réaliser des tests en local).

```
client 127.0.0.1 {
        secret = testing123
        shortname = localhost
        nastype = other
        }
```

Pour rajoutez notre borne wifi avec comme adresse IP **192.168.1.1**

```
client 192.168.1.1 {
        secret = demoh
        shortname = D-Link
        nastype = other
          }
```

- **Fichier users**

```
gedit /etc/raddb/users
```

Éditez-le et ajoutez la ligne suivante en haut du texte, avant toute autre chose :

```
farid Auth-Type := local, User-Password == "virus"
```

Cela nous permet de vérifier les tests en local.
Dans ce fichier, on défini la liste des utilisateurs qu'on autorise. On a précédemment géré le certificat pour l'utilisateur wissame, on ajoute donc a la fin du fichier :

```
"wissame" Auth-Type := EAP
```

On spécifie que l'utilisateur « wissame » peut s'authentifier avec la méthode EAP (EAP-TLS, EAP-TTLS, EAP-PEAP,…). Pour forcer un type, il faut utiliser l'attribut EAP-Type, par exemple si on veut que l'utilisateur ne fasse que de l'EAP-TLS, il faut mettre alors :

```
"wissame"   Auth-Type := EAP, EAP-Type := EAP-TLS
```

- **Fichier radiusd.conf**

```
gedit /etc/raddb/radiusd.conf
```

Ceci étant dit la configuration de radiusd.conf ne doit pas être complètement modifiée.
Il faudra seulement s'assurer que les paramètres évoqués auparavant soient bien inscrit sur le fichier tout en respectant le modèle suivant :

```
prefix = /usr/local
exec_prefix = ${prefix}
sysconfdir = /etc
localstatedir = ${prefix}/var
sbindir = ${exec_prefix}/sbin
logdir = ${localstatedir}/log/radius
raddbdir = ${sysconfdir}/raddb
radacctdir = ${logdir}/radacct
confdir = ${raddbdir}
run_dir = ${localstatedir}/run/radiusd
log_file = ${logdir}/radius.log
libdir = ${exec_prefix}/lib
pidfile = ${run_dir}/radiusd.pid
...
user = nobody
group = nogroup
...
max_request_time = 30
...
max_requests = 1024
...
bind_address = *
...
port = 0
...
hostname_lookups = yes
log_stripped_names = yes
…
log_auth = yes
…
log_auth_badpass = yes
log_auth_goodpass = yes
...
modules {
$include ${confdir}/eap.conf
}
…
authorize {         # on définit l'autorisation eap
preprocess
eap
files               # on lit le fichier users
}
authenticate {
eap                  # authentification eap
}
```

Ainsi la configuration est terminée.

- **Lancement de test du serveur**

Si tout ce passe bien, vous n'avez qu'à utiliser le daemon avec la commande :

radiusd –X –A &

On obtient à la fin :

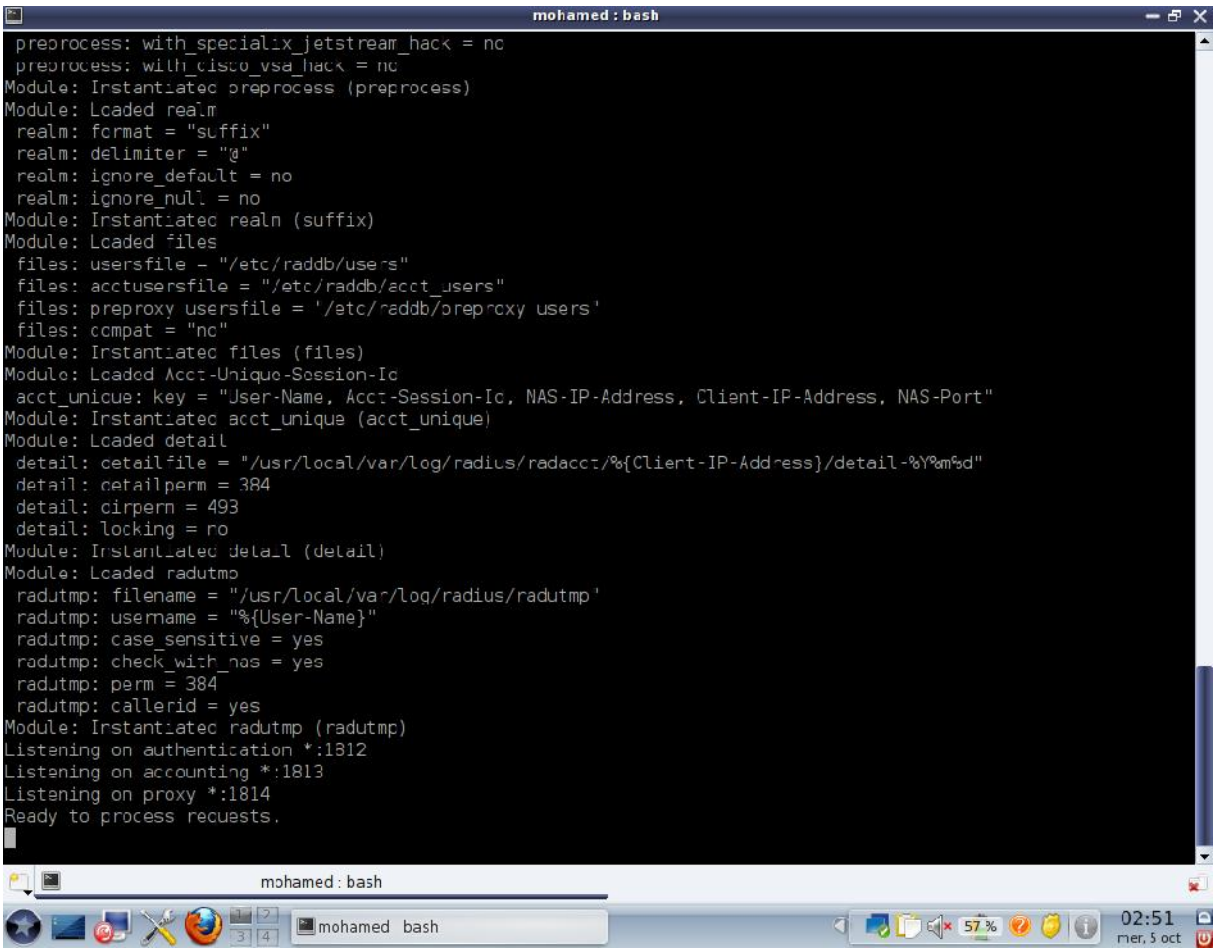

Figure III.8 : Lancement du serveur radius

Cette étape démontre que le serveur a été installé et configuré correctement.

Pour arrêter le radius, il suffit de taper :

```
killall radiusd
```

Maintenant il faut tester en local avec la commande suivante :

```
radtest farid virus localhost 0 testing123
```

On a vérifié le bon fonctionnement du serveur, par la réponse « **Access-Accept** » comme suit :

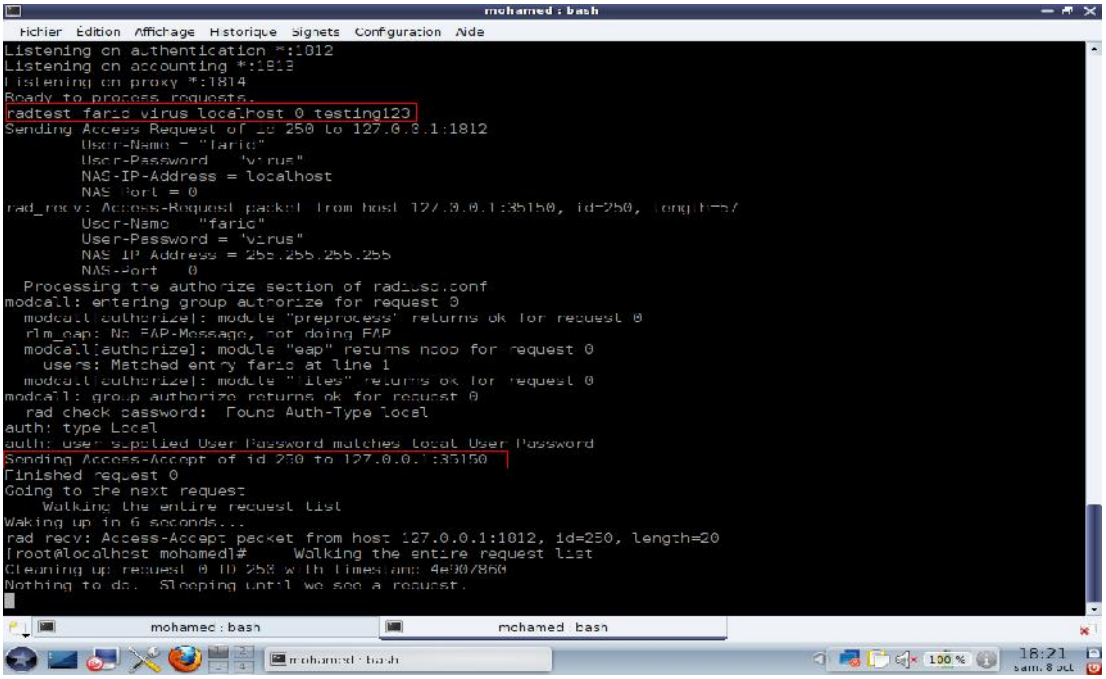

Figure III.9 : Réussite du test en local

4. Configuration du point d'accès

Le point d'accès est un **« D-Link DSL-2640U Wireless G ADSL2 + Router ».**

Voici sa configuration :

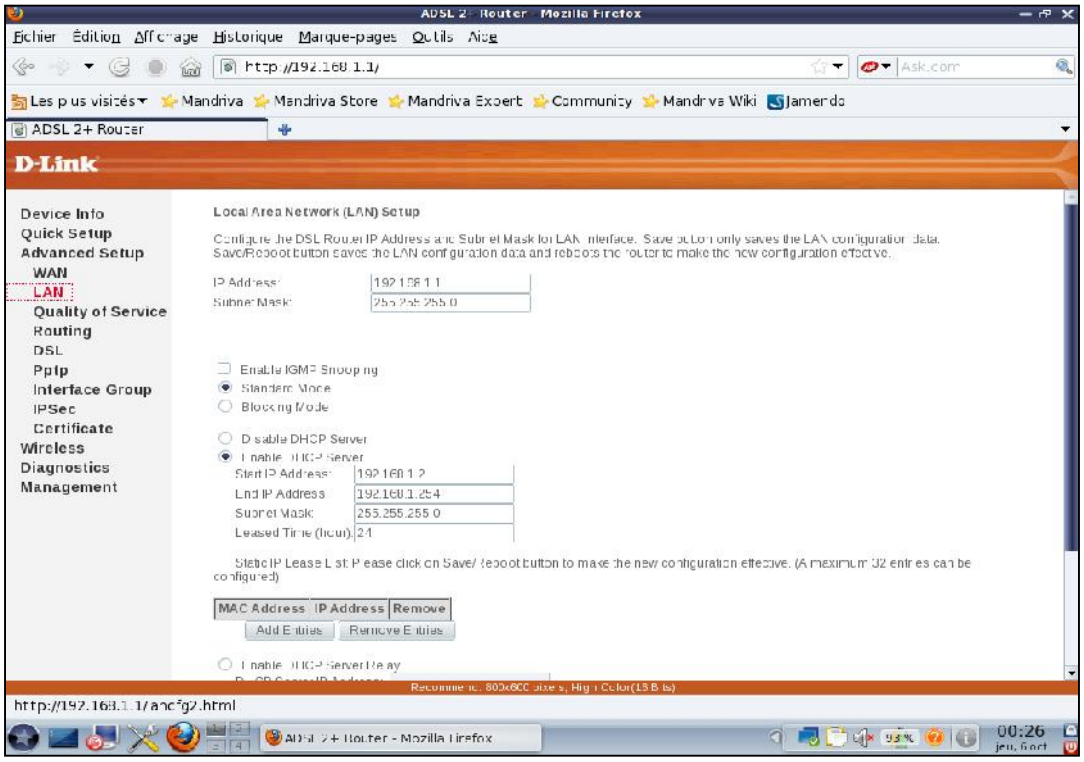

Figure III.10 : Attribution de l'adresse IP statique de l'AP

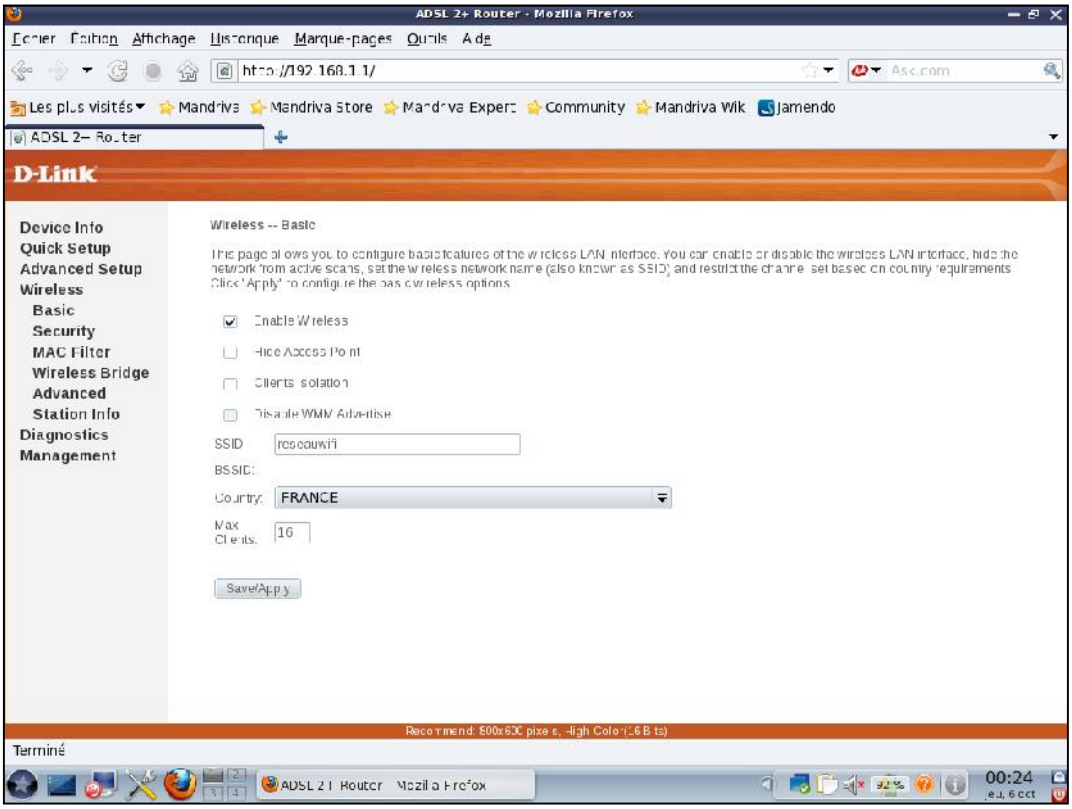

Figure III.11 : Attribution du SSID au point d'accès

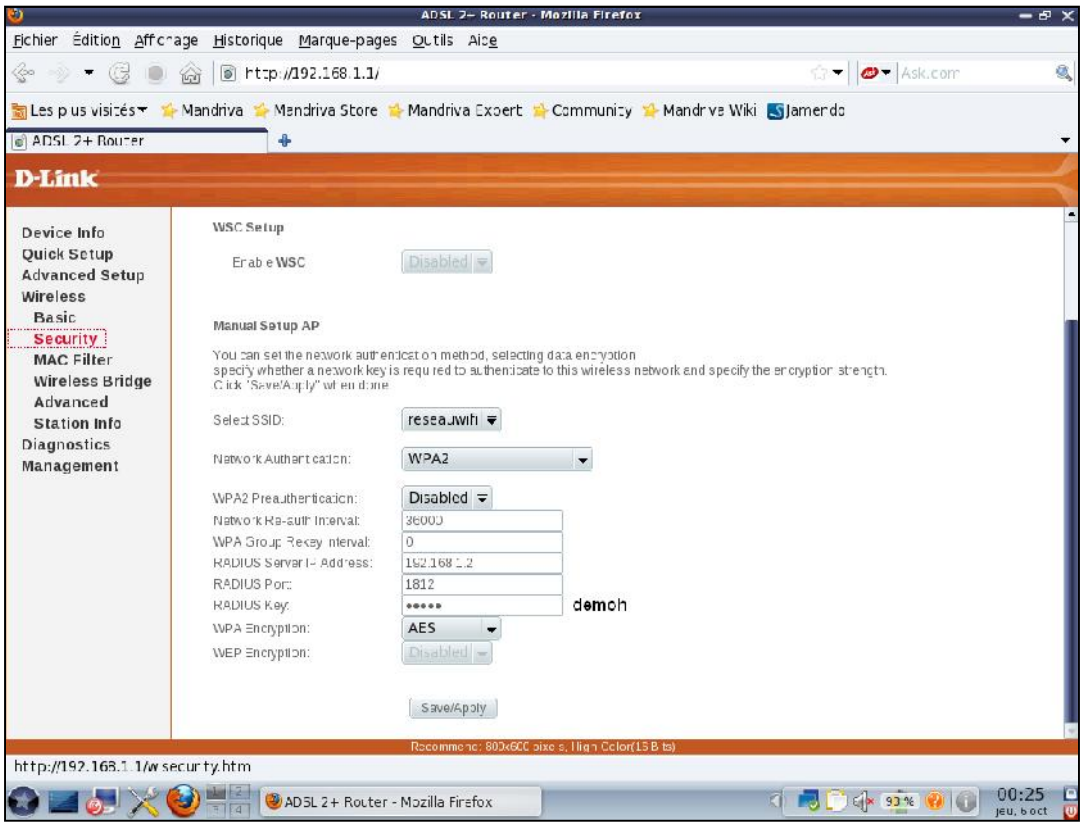

Figure III.12 : Attribution de l'adresse IP du radius à l'AP

Ainsi la configuration est terminée.

5. Configuration du poste client sous Windows XP

La configuration de Windows XP ne doit pas trop poser de problèmes vu qu'il y a tout plein d'assistantes partout.

On dispose déjà des certificats suivants :

5.1. Installation du certificat d'autorité

I l faut simplement double cliquer sur root.der

Etape 1 : cliquer ensuite sur « installer le certificat »

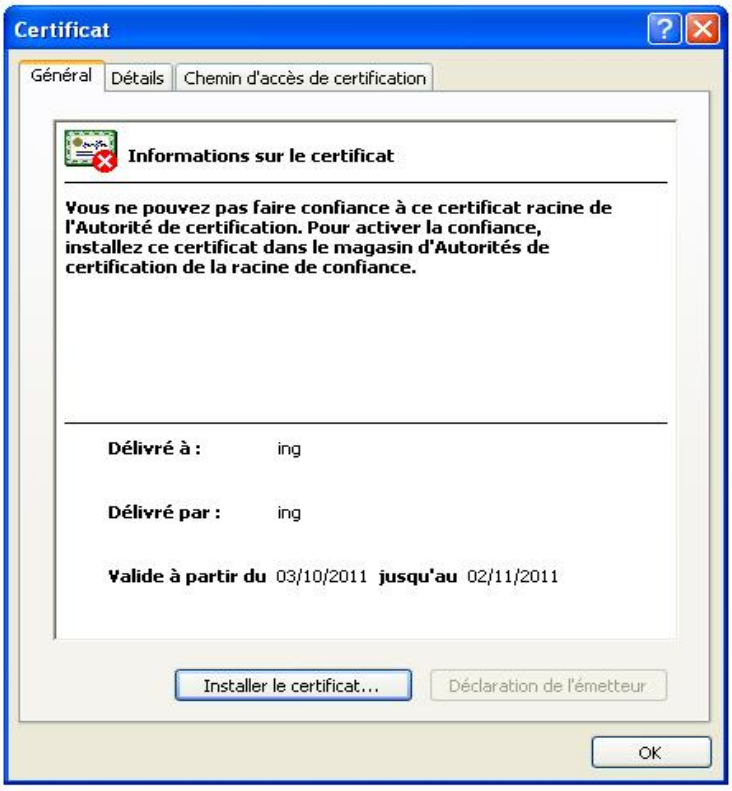

Figure III.13 : Début de l'installation du certificat root

Etape 2 : cliquez sur « suivant »

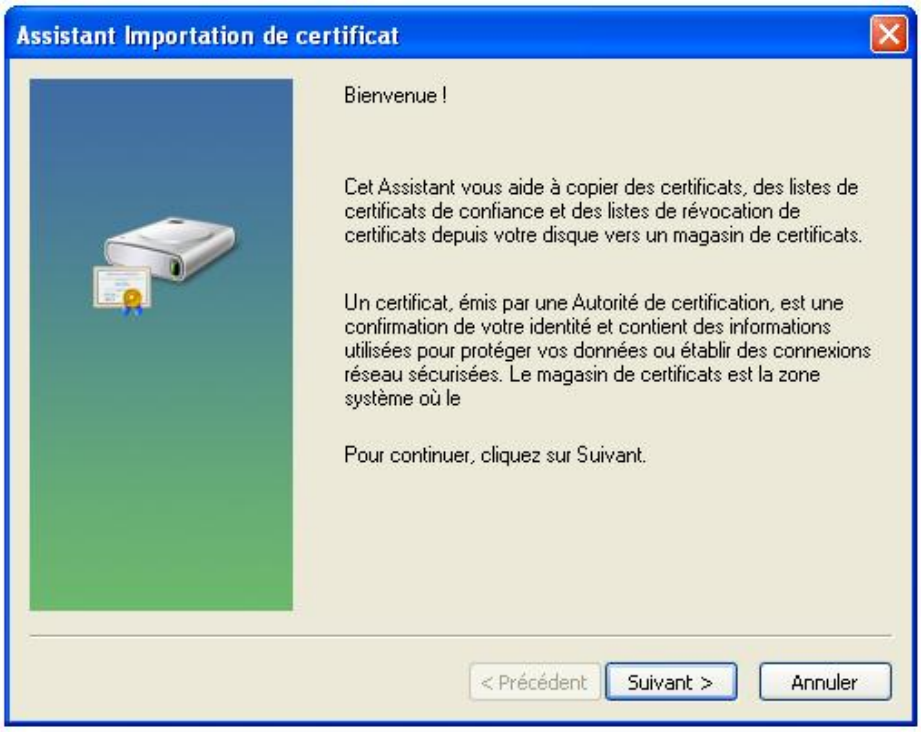

Figure III.14 : Confirmation de l'installation

Etape 3 : cliquez sur « parcourir »

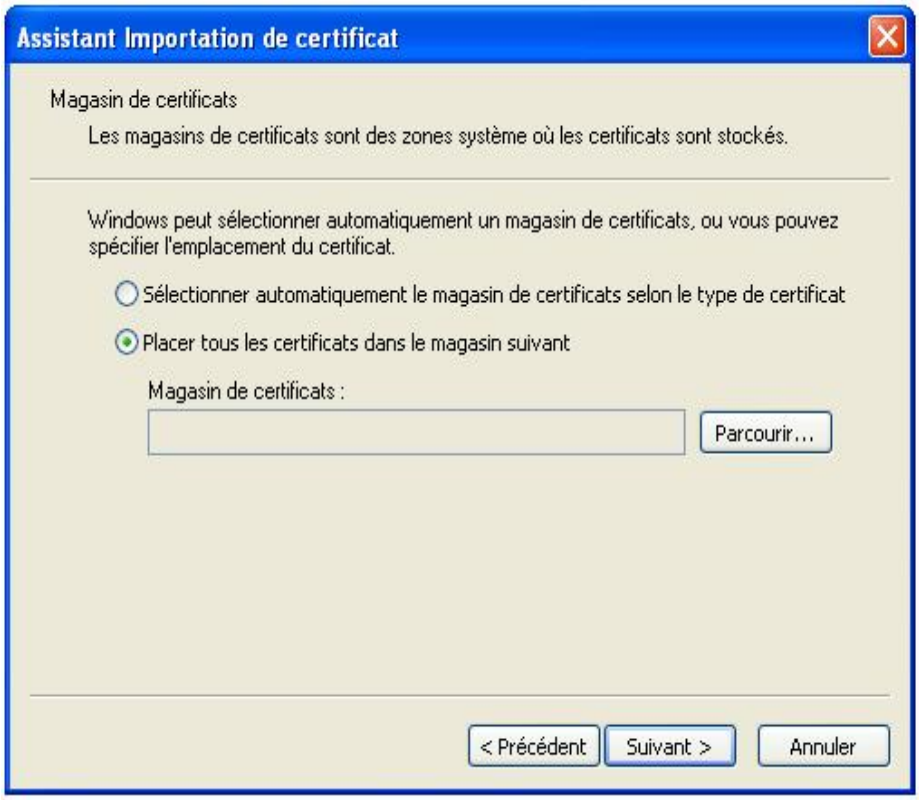

Figure III.15 : Choix de magasin du certificat

Etape 4 : La sélection du magasin de certificat que l'on souhaite utiliser puis « OK »

Figure III.16 : Sélection d'autorités de certification racines de confiance

Etape 5 : « terminer »

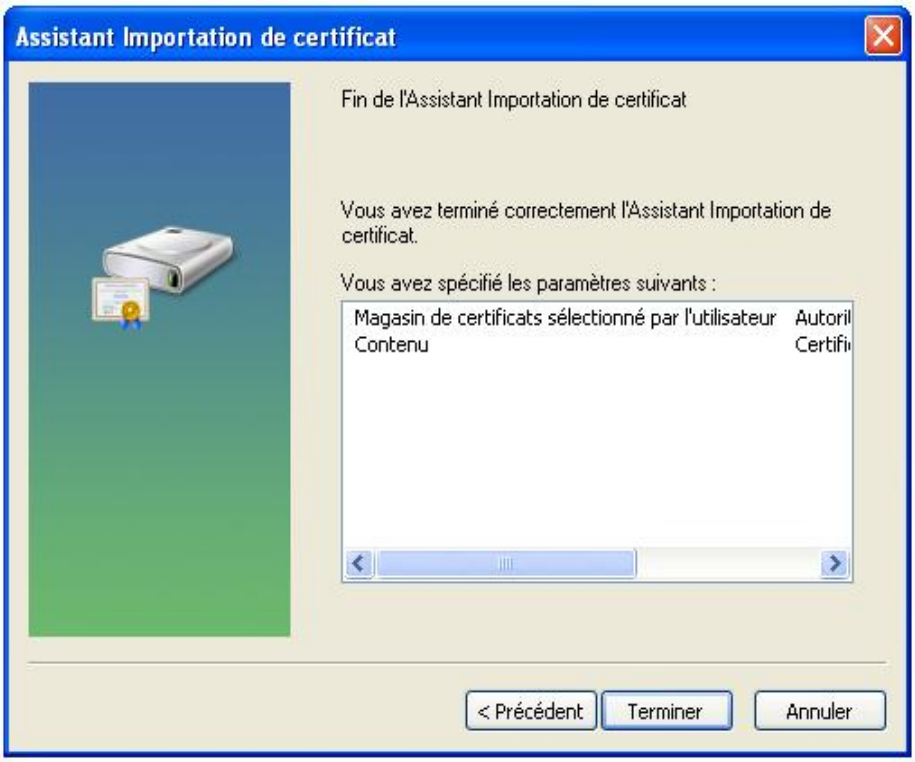

Figure III.17 : Fin de l'importation du certificat

Etape 6 : « oui »

Figure III.18 : Confirmation de la validité du certificat root

Figure III.19 : Fin de l'importation du certificat

L'importation du certificat racine est terminée.

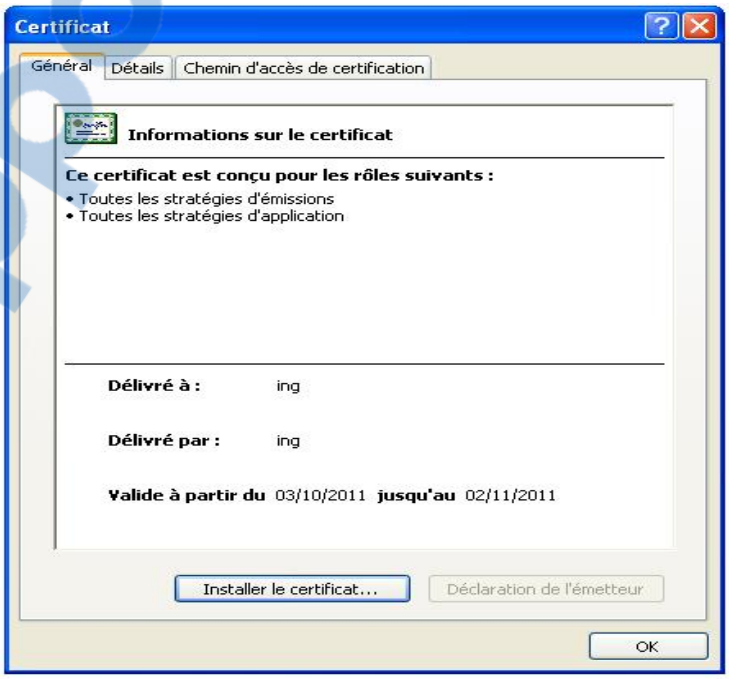

Figure III.20 : Certificat d'autorités root

5.2. Installation du certificat client

Etape 1 : « suivant »

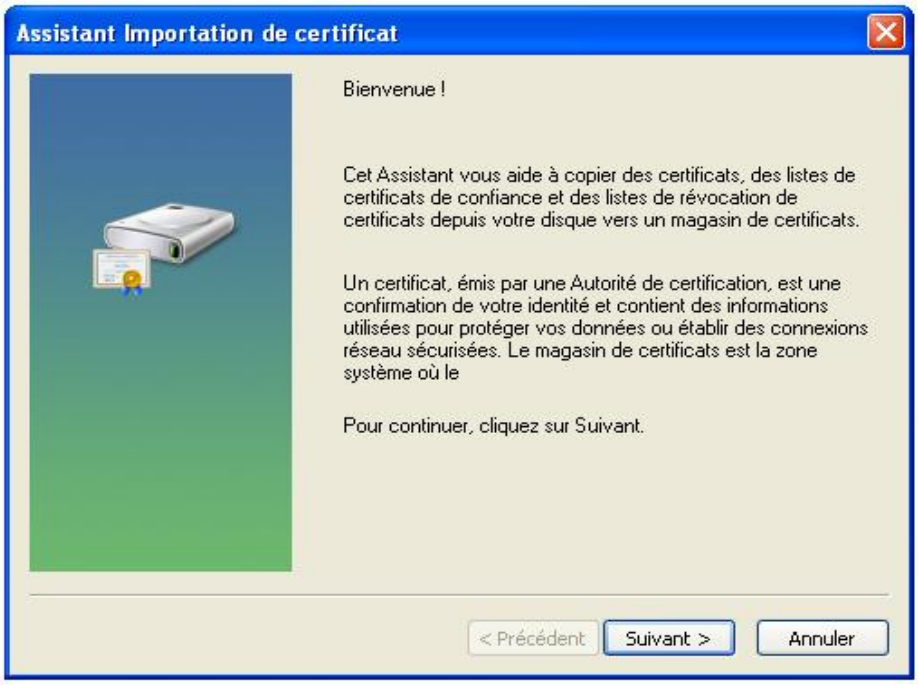

Figure III.21 : Confirmation de l'installation

Etape 2 : « suivant »

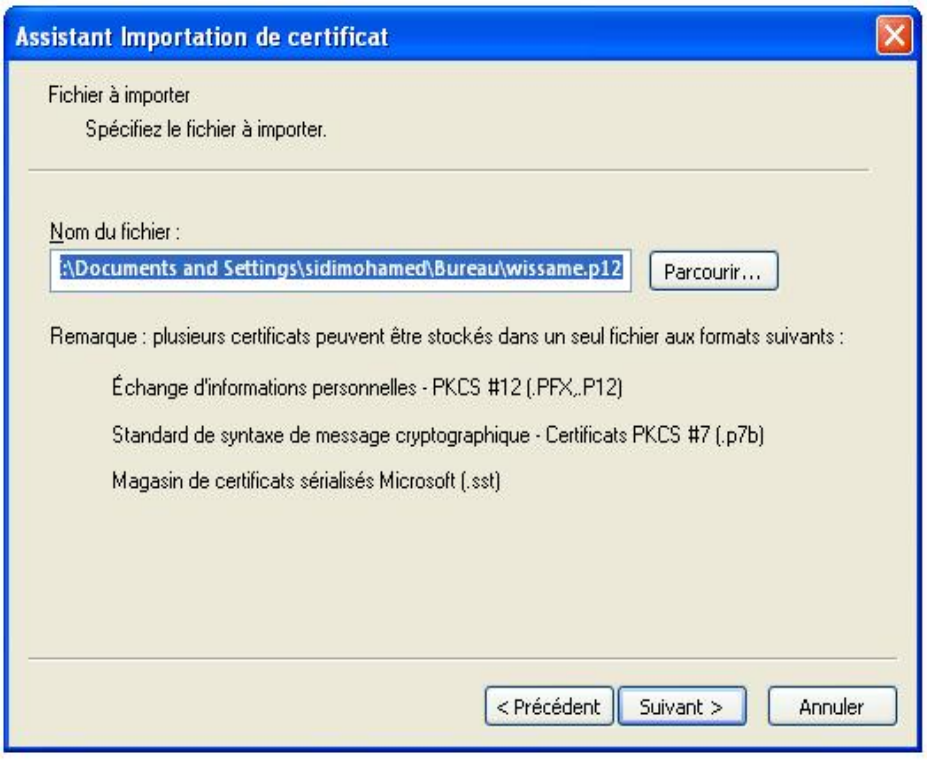

Figure III.22 : Installation du certificat wissame.p12

Etape 3 : On a entré le mot de passe utilisé dans le certificat client (notre mot passe est : whatever)

Figure III.23 : Mot de passe

Etape 4 : sélection du magasin de certificat que l'on veut utilisez puis « OK »

Figure III.24 : Choix de l'emplacement du certificat wissame.p12

Etape 5 : « terminer »

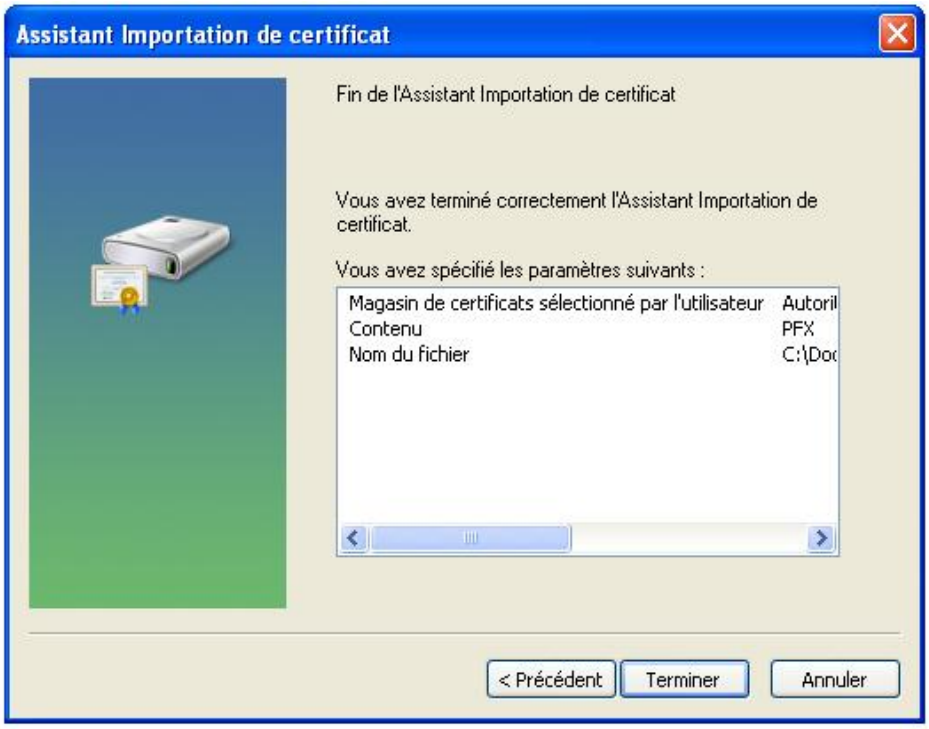

Figure III.25 : Fin de l'importation du certificat

Etape 6 : « OK » pour terminer l'importation

Figure III.26 : Confirmation de la réussite

5.3. Installation du certificat serveur

Identique à celui de certificat client, la seule différence c'est le choix de magasin du certificat qui sera « autorité de certification racine de confiance » et non « personnel ».

6. Configuration de la connexion sans fil

La configuration de la connexion sans fil est très simple.

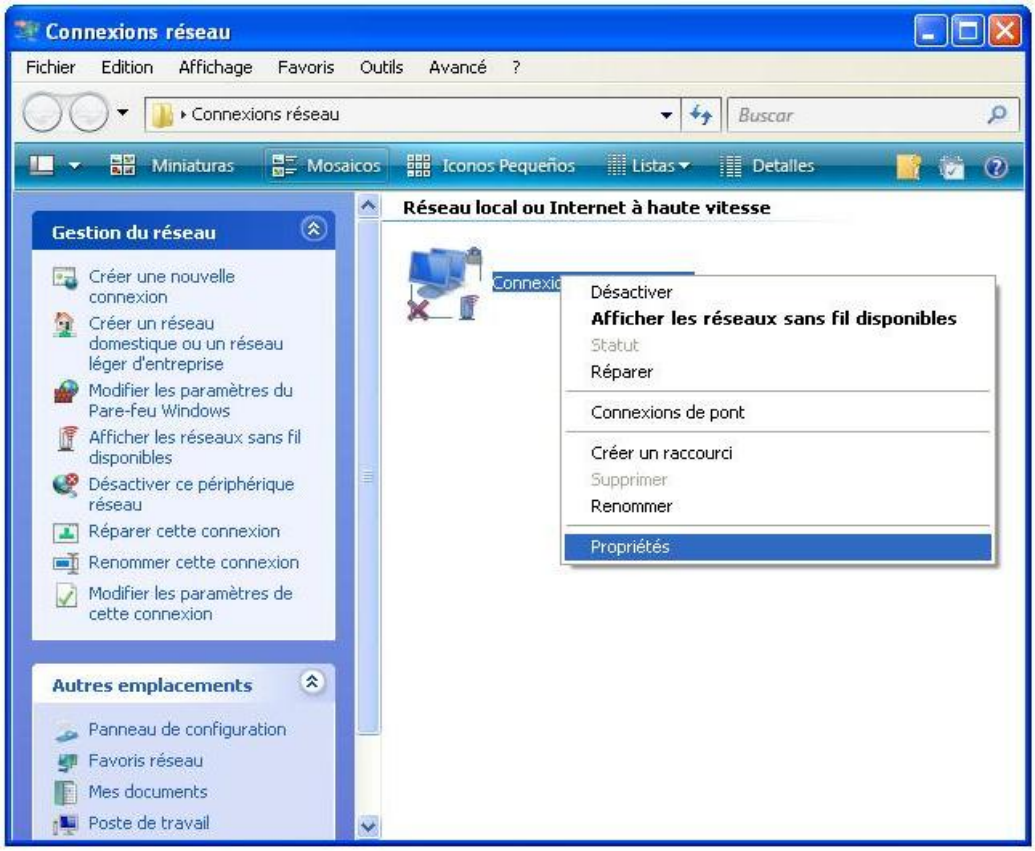

Figure III.27 : Choix de la propriété de la connexion sans fil

Etape 1 : cliquez sur le protocole internet (TCP/IP) puis sur propriétés

Figure III.28 : Choix du Protocole Internet (TCP/IP)

Etape 2 : cliquez sur la configuration réseaux sans fil

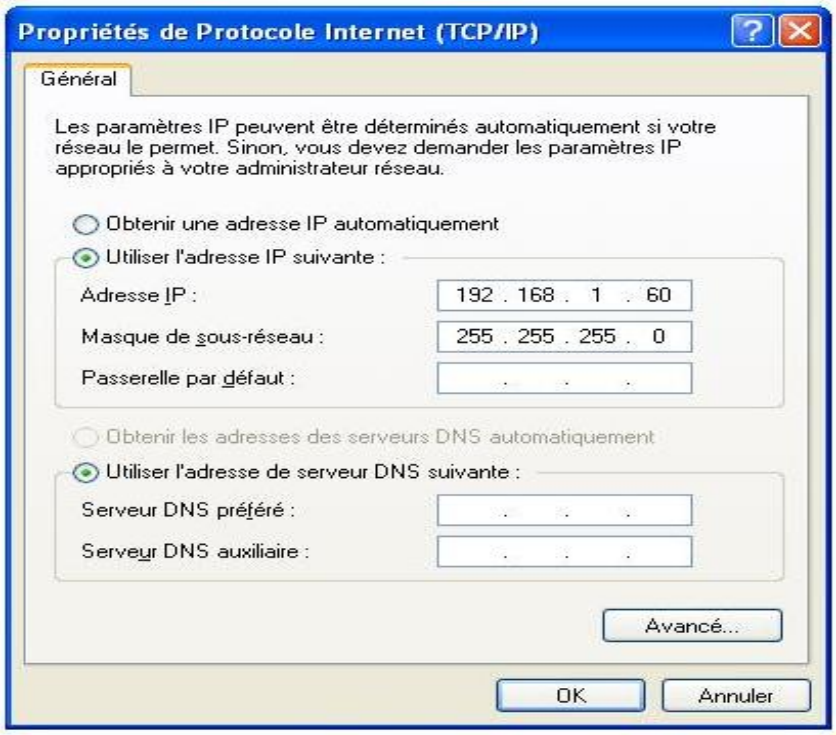

Figure III.29 : Début de la configuration

Etape 3 : sélectionner votre réseau puis cliquez sur propriétés ; s'il n'existe pas dans la liste ajouter-le, ensuite continuer la configuration en cliquant sur propriétés.

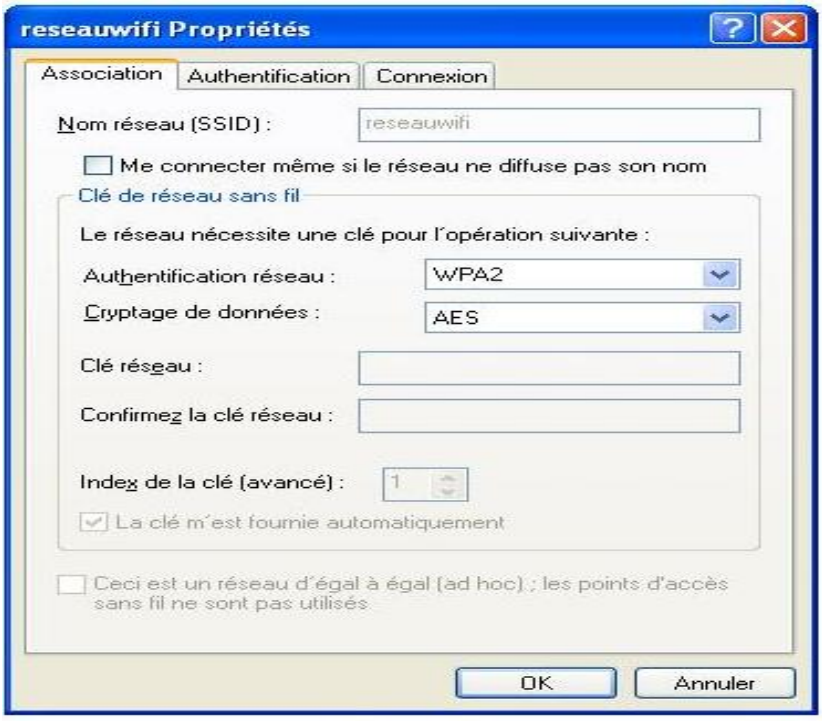

Figure III.30 : Choix de type d'authentification réseau et de type de cryptage des données

Etape 4 : sélectionner le type d'authentification

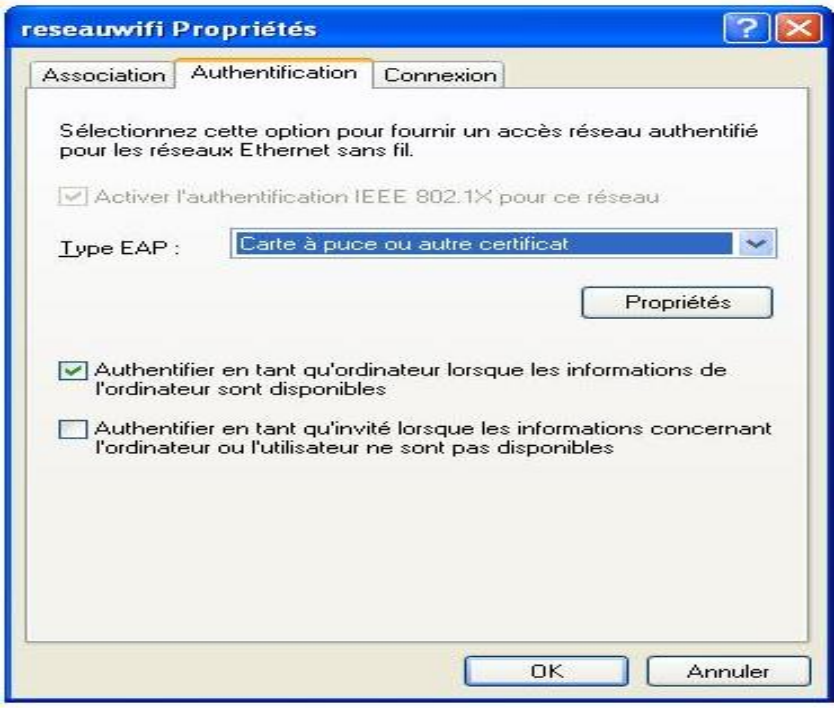

Figure III.31 : Choix du type EAP

Etape 5 : cliquez sur propriété pour choisir les certificats qu'on a installés sur l'ordinateur du client wissame.

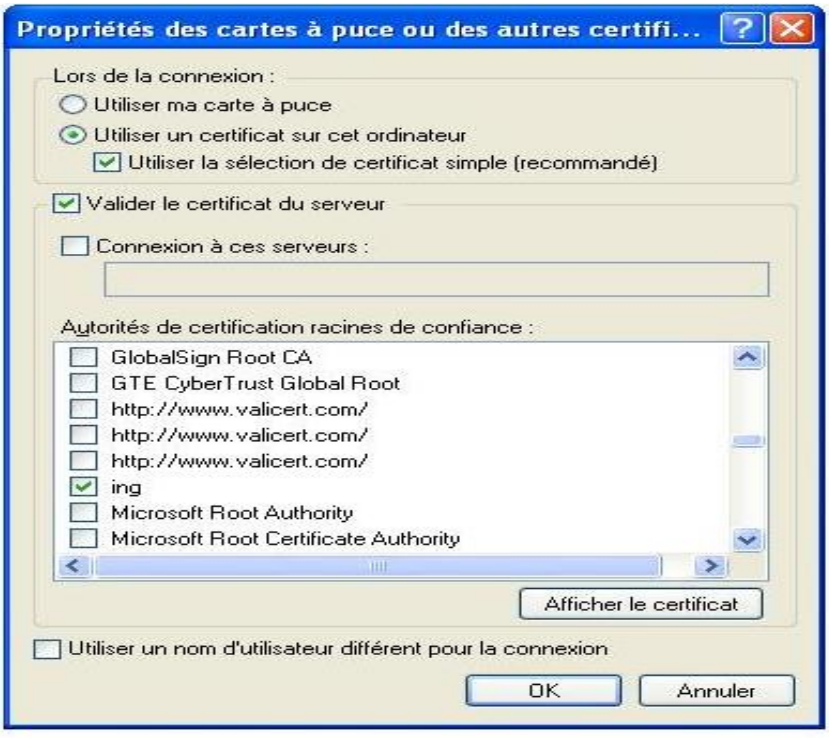

Figure III.32 : Choix du certificat d'autorité root nommé « ing »

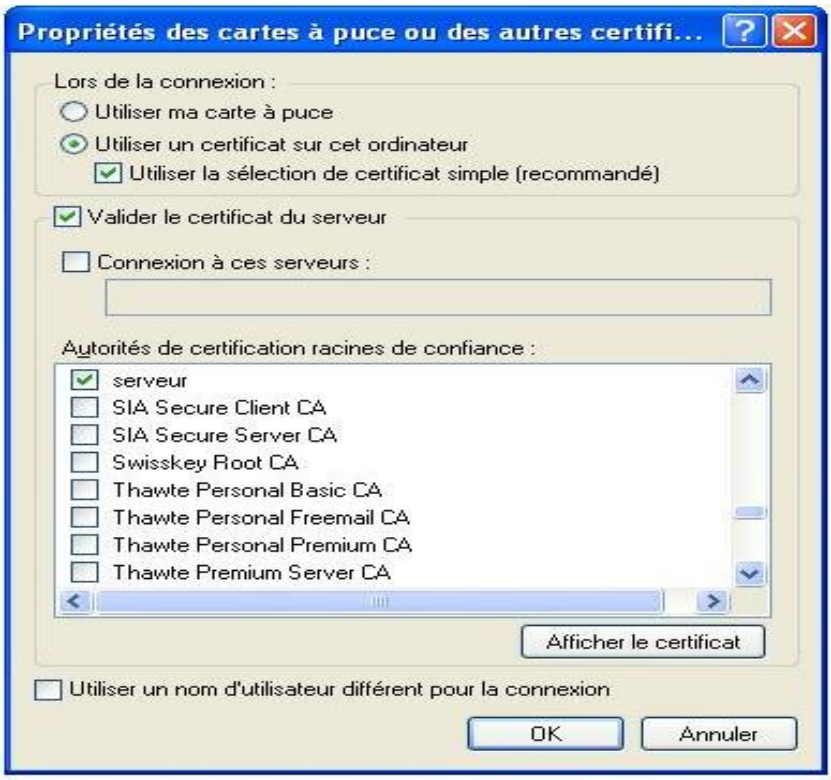

Figure III.33 : Choix du certificat serveur

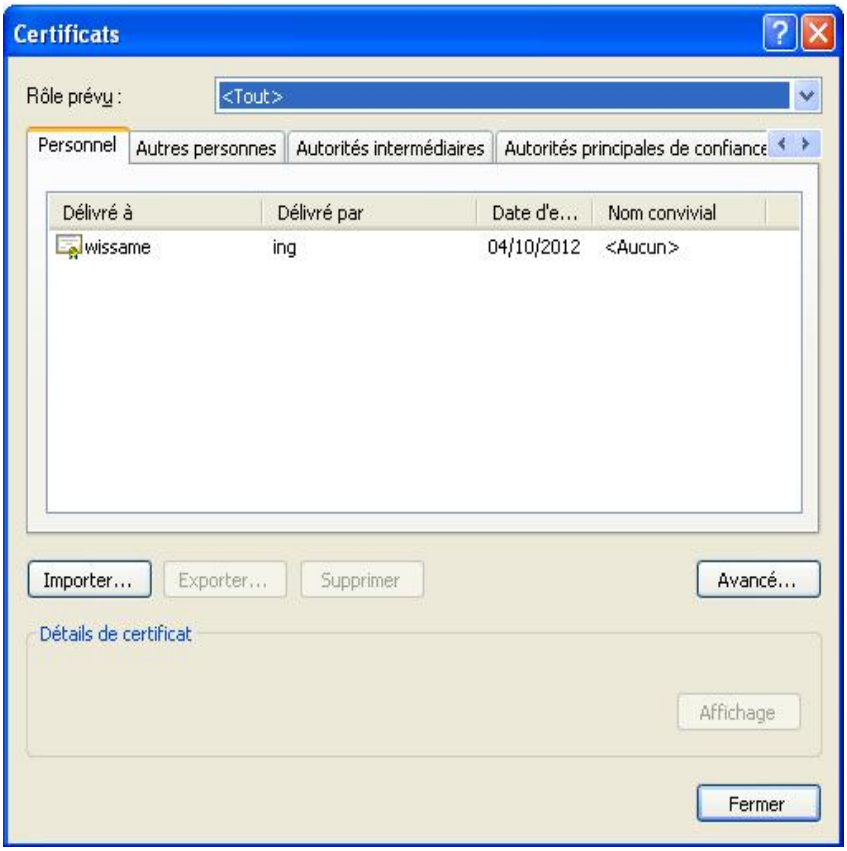

Figure III.34 : Certificat client wissame

Etape 6 : cliquez sur connexion et cochez « Me connecter à ce réseau lorsqu'il est a porté » puis cliquez sur « OK »

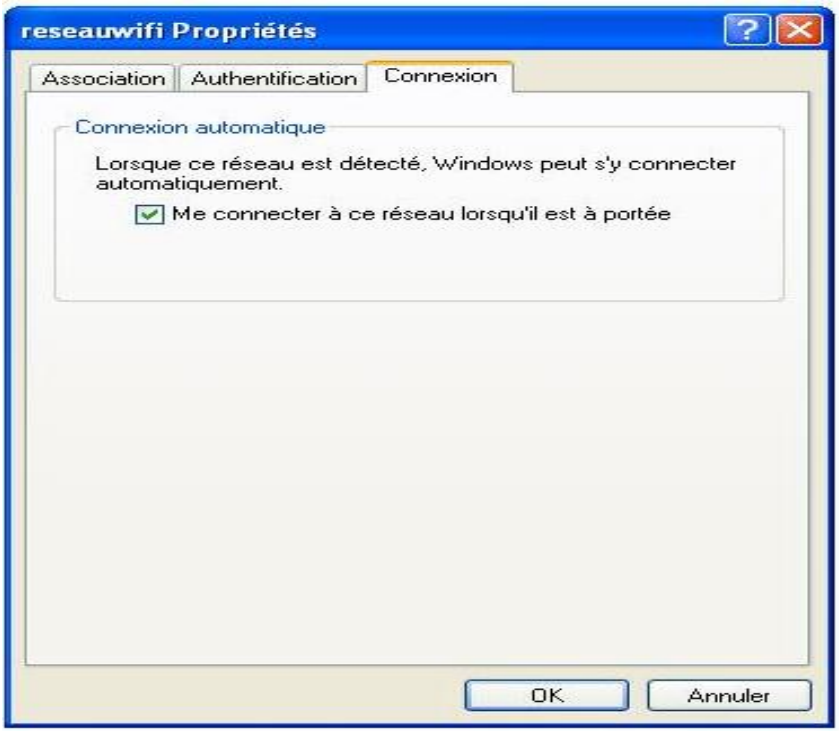

Figure III.35 : Choix de la connexion

Etape 7: cocher « réseaux avec point d'accès seulement (infrastructure) », puis sur fermer

Figure III.36 : Choix du réseau avec point d'accès seulement

Ainsi on a fini la configuration de notre connexion sans fil « reseauwifi ».

Nous allons maintenant essayer de nous connecter au réseau « reseauwifi », mais d'abord on lance le serveur radius.

La carte a détecté un seul réseau sans fil : notre réseau « reseauwifi ».

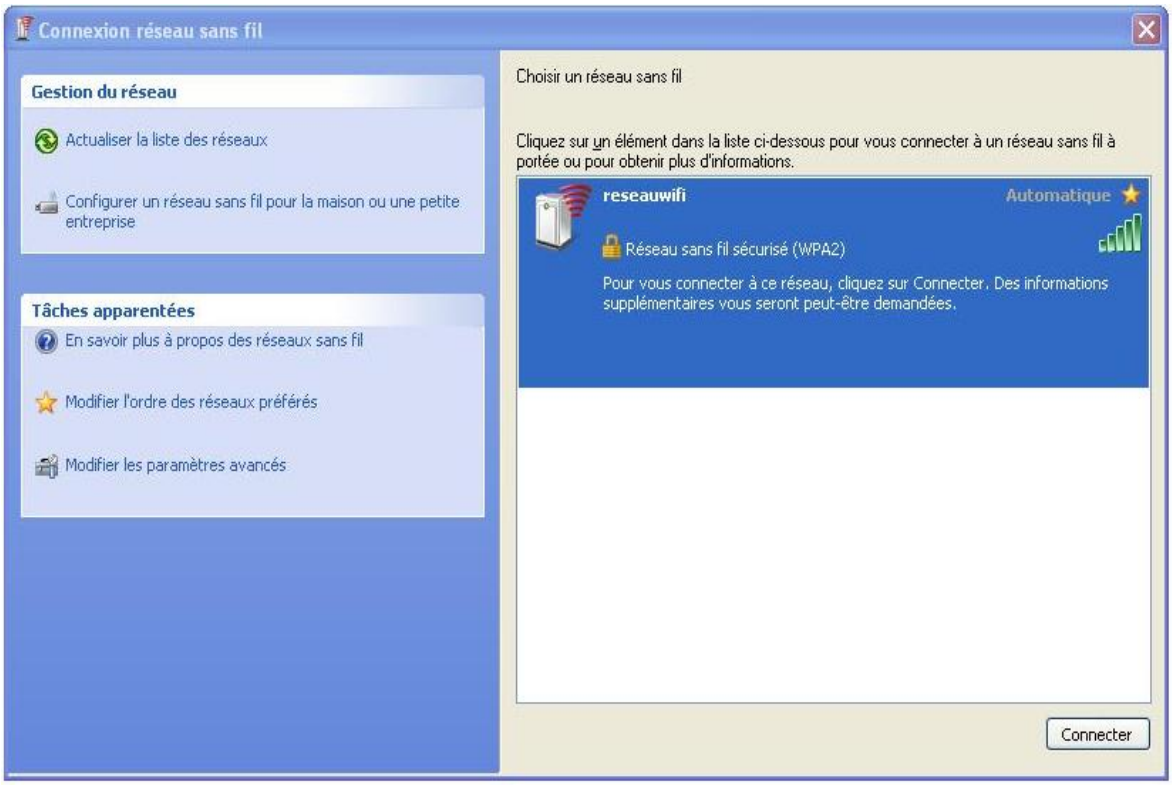

Figure III.37 : Réseau détecté par la carte

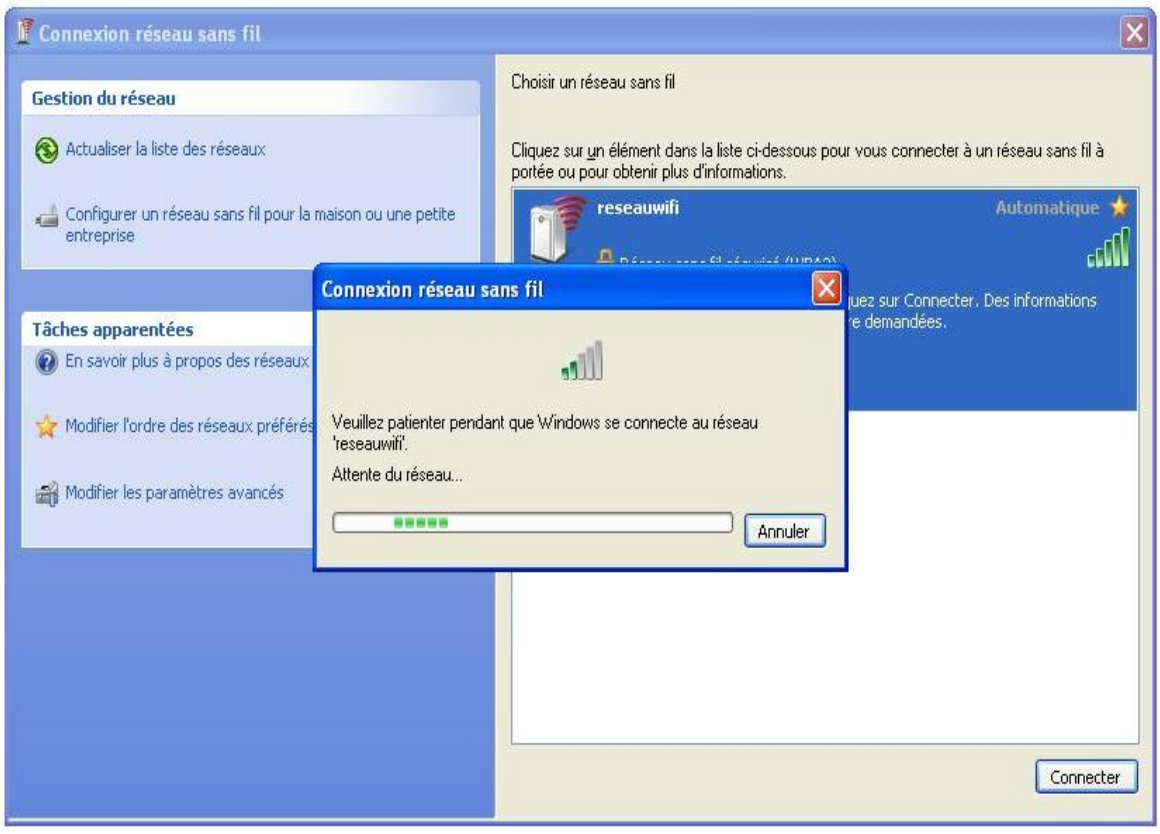

Figure III.38 : Tentative de connexion

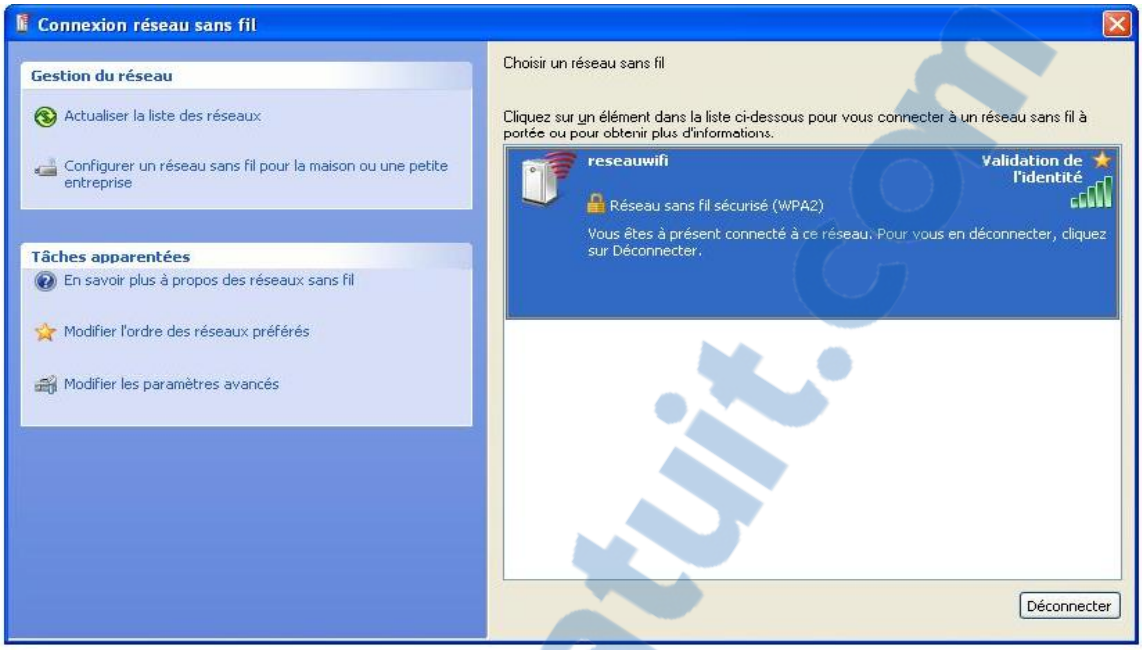

Figure III.39 : Validation de l'identité

Lorsqu'on arrive à s'associer avec le point d'accès et que le radius nous répond :

Radius affiche les échanges des messages EAP entre lui et le client wissame.

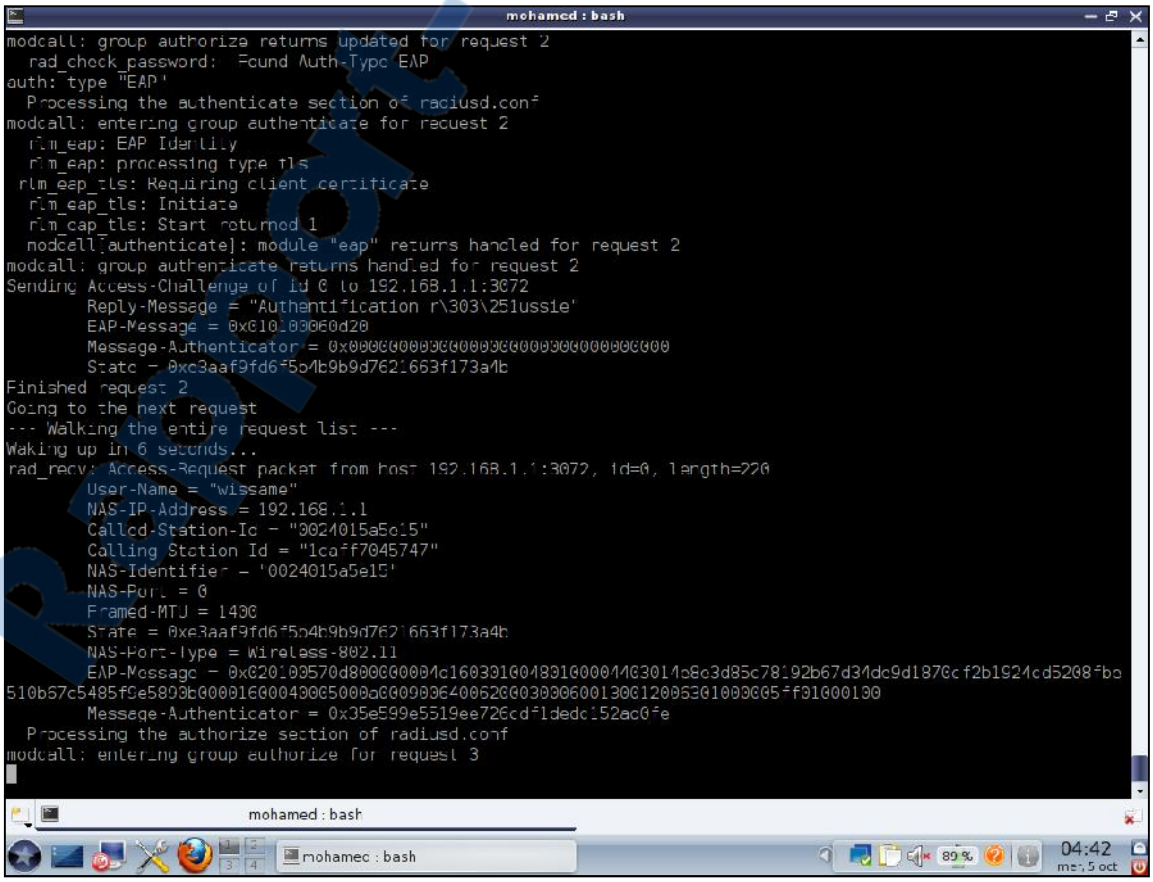

Figure III.40 : Echanges des messages EAP entre le serveur radius et le client wissame

Et en même temps chez le client apparait la fenêtre suivante :

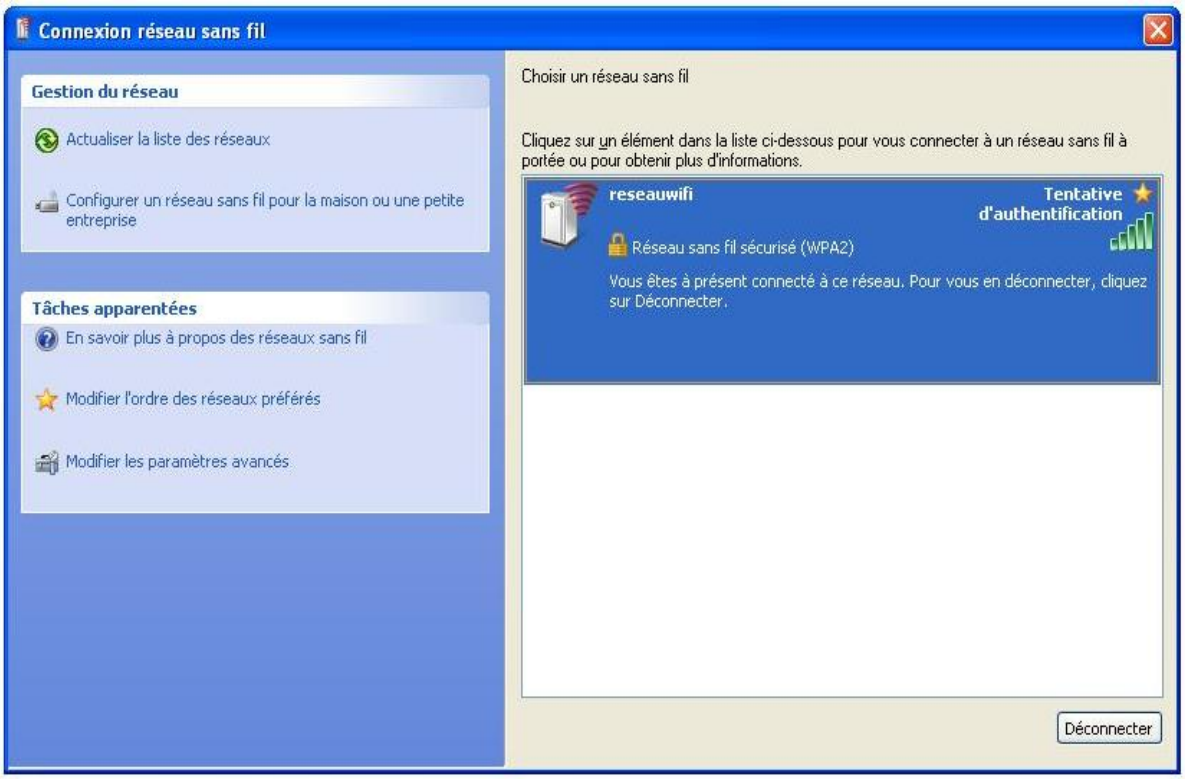

Figure III.41 : Attente de l'authentification

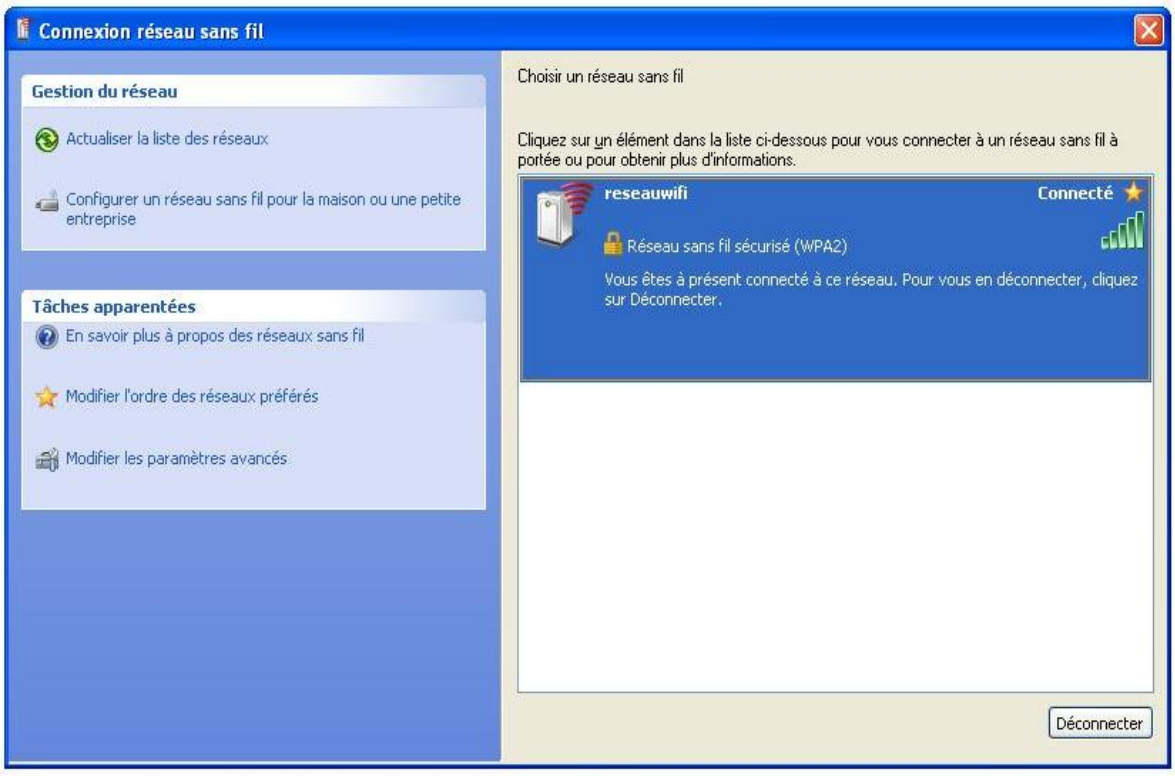

Figure III.42 : Réussite de l'authentification et passage à l'état connecté

Figure III.43 : Etat de connexion réseau sans fil

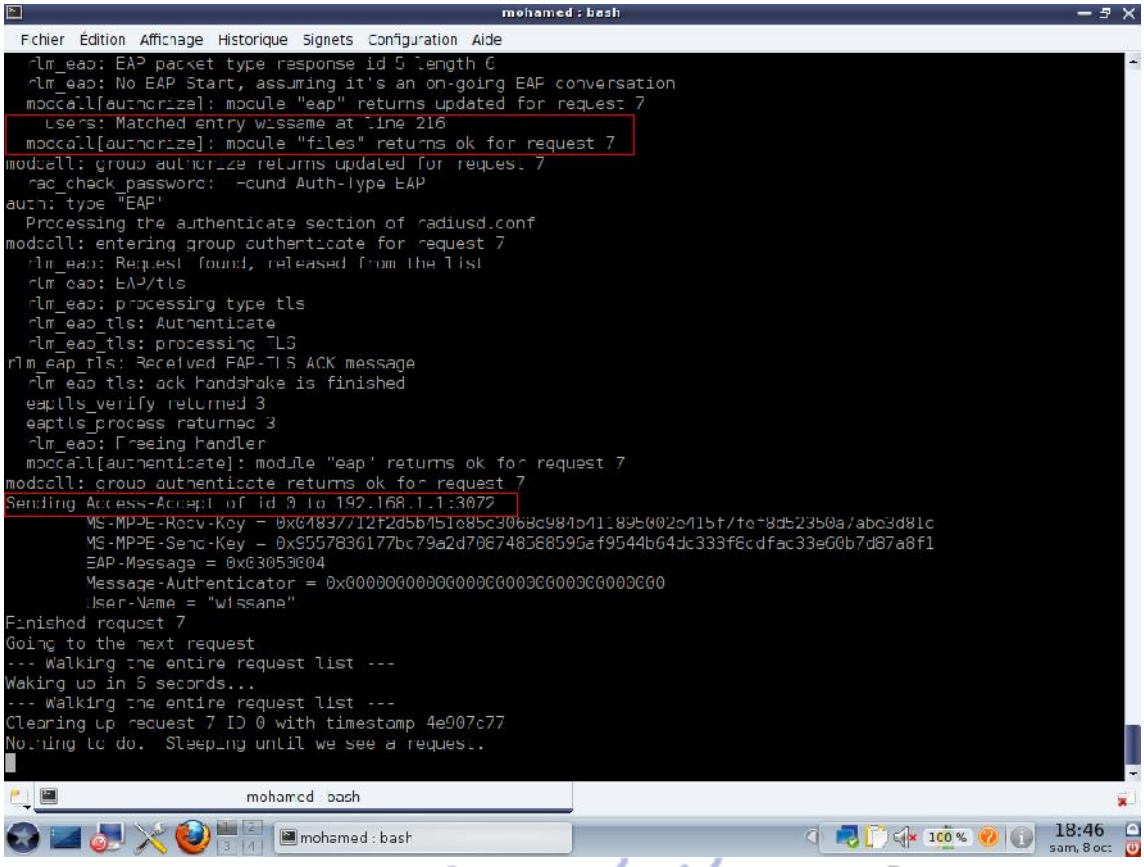

Figure III.44 : Autorisation accepté de serveur pour le client wissame

Pour s'assurer que tout fonctionne bien, on va essayer de faire un partage des fichiers entre le poste serveur et le poste client; (on a trouvé le manuel de configuration de samba pour les partages sous mandriva sur **[23]).**

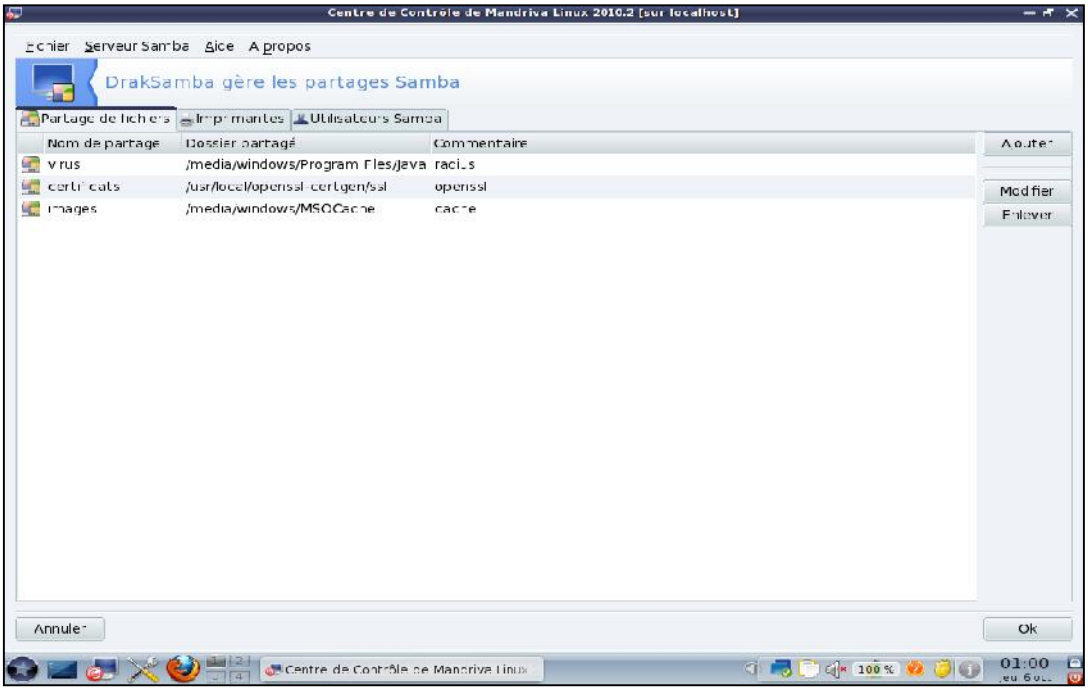

Figure III.45 : Fichiers à partager sur le poste client

Sur le poste client, assurez-vous que le pare-feu autorise les partages des fichiers, cochez « partage de fichiers et d'imprimantes »

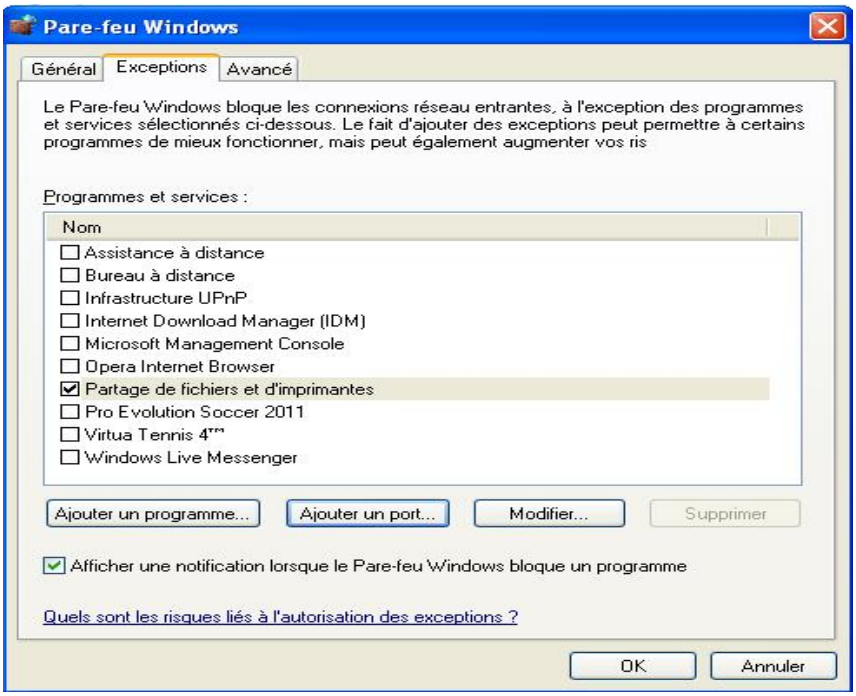

Figure III.46 : Autorisation de partage des fichiers

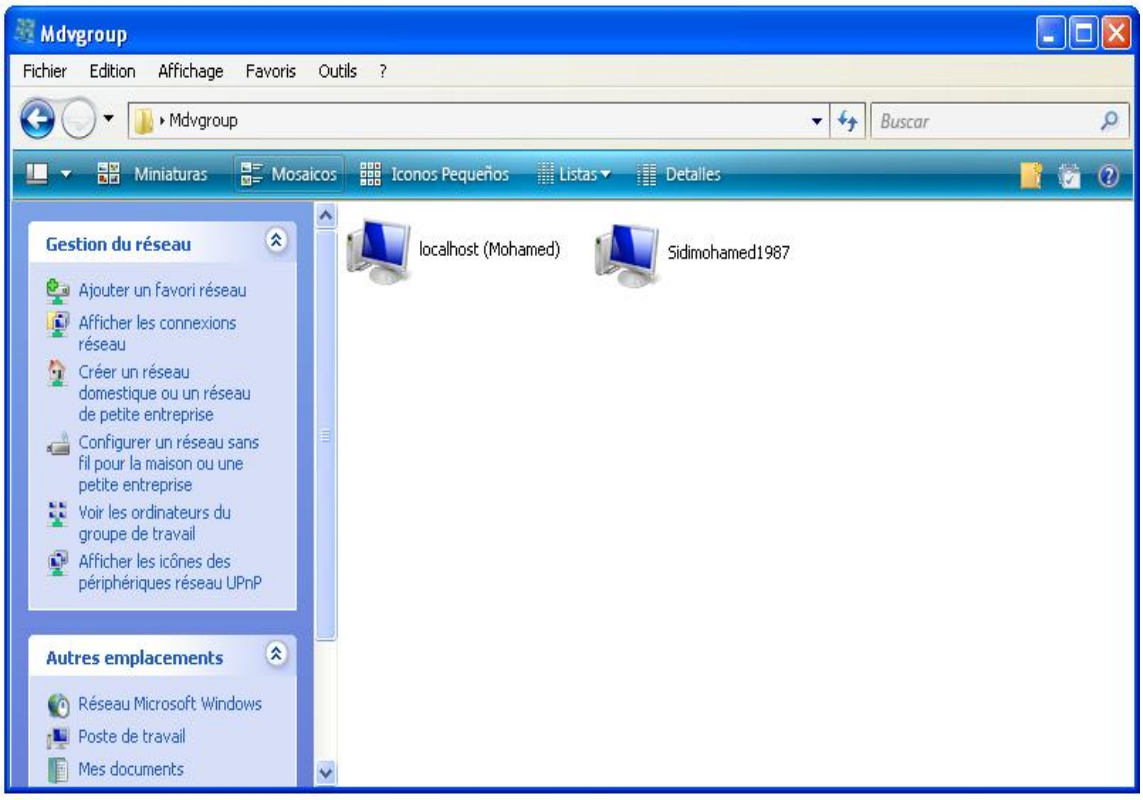

Figure III.47 : Usagers du réseau

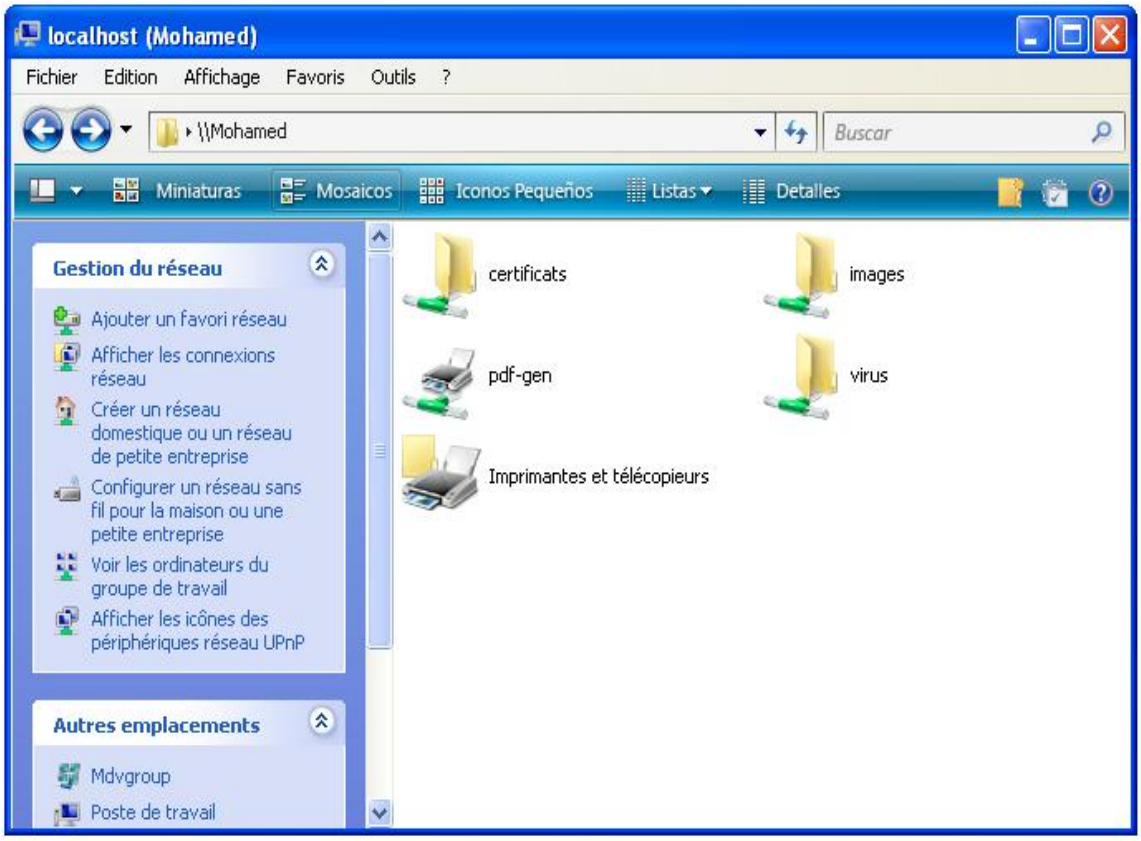

Figure III.48 : Fichiers partagé sur le poste client

Dés qu'il ya d'autres clients connectés sur le réseau, ils peuvent partager des fichiers entre eux.

D'autres solution pour s'assurer de la réussite de connexion c'est d'utilisé le ping entre le serveur et client connecté.

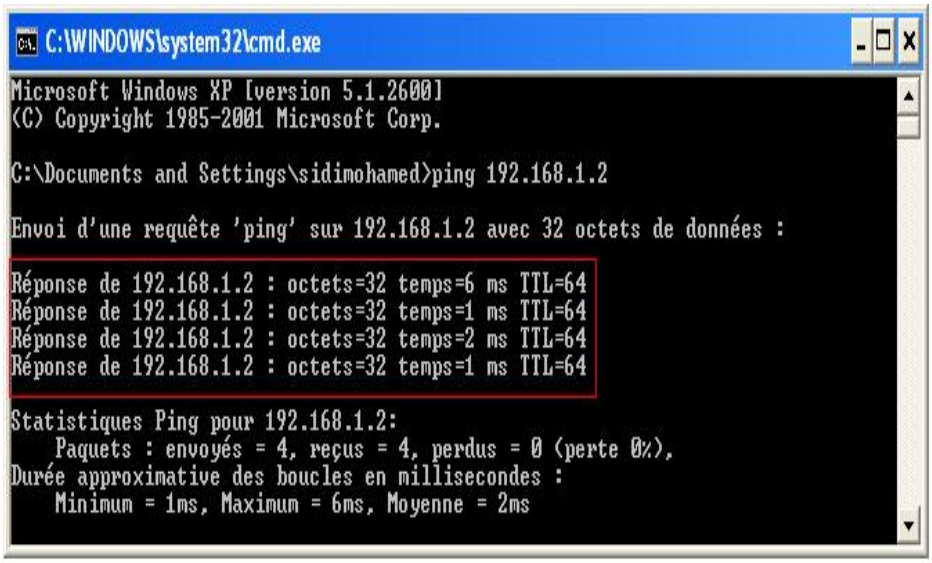

Figure III.49 : Réussite de ping du client vers le serveur

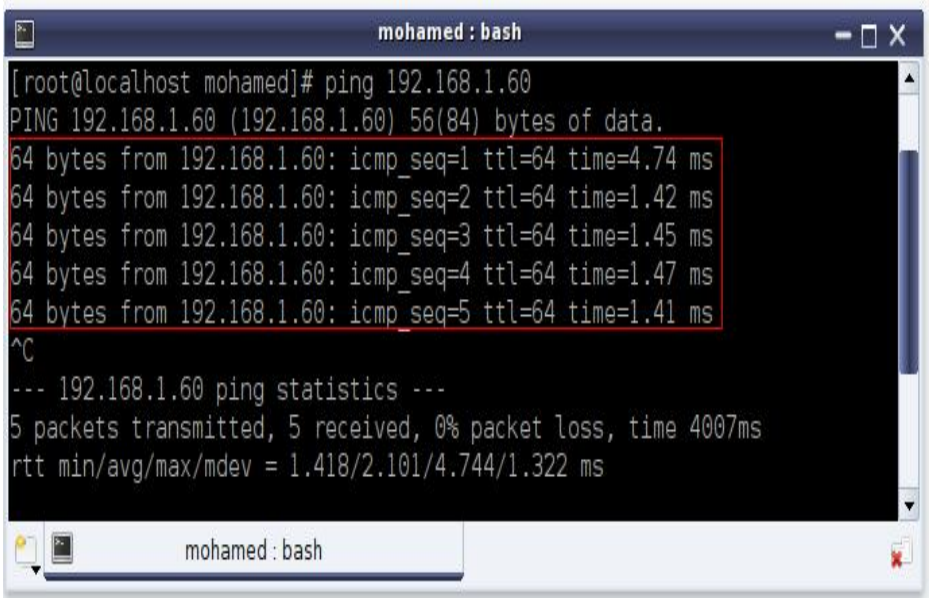

Figure III.50 : Réussite du ping du serveur vers le client

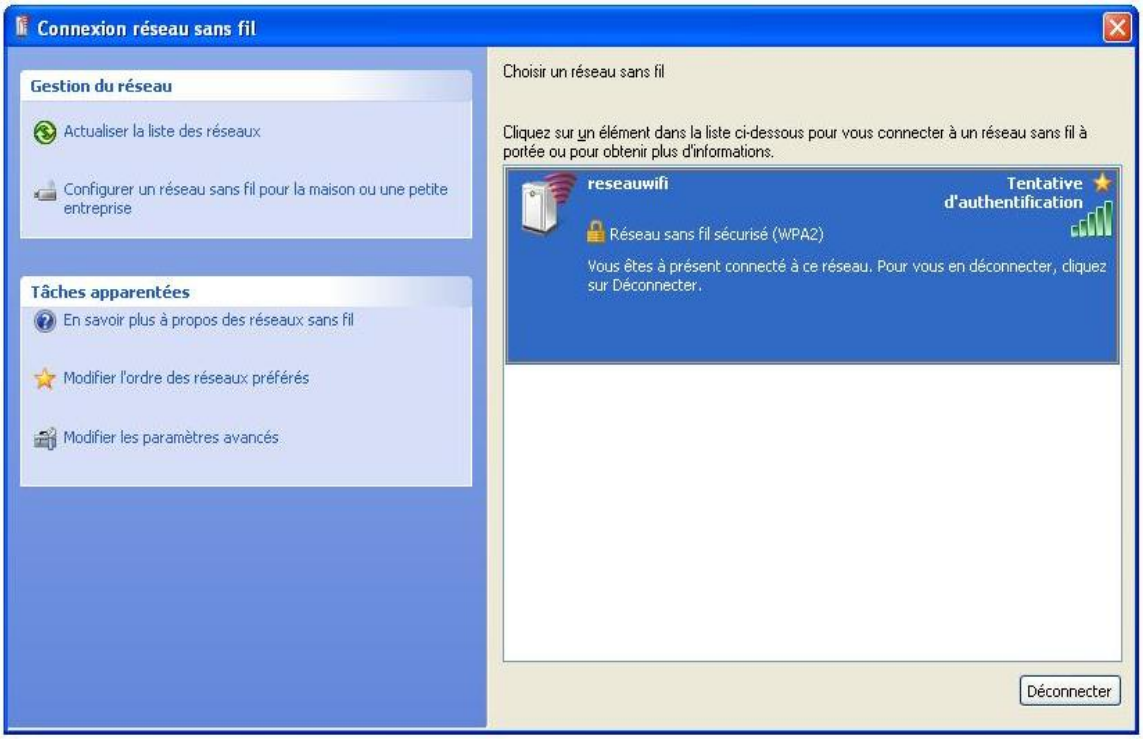

Figure III.51 : Tentative d'un pirate

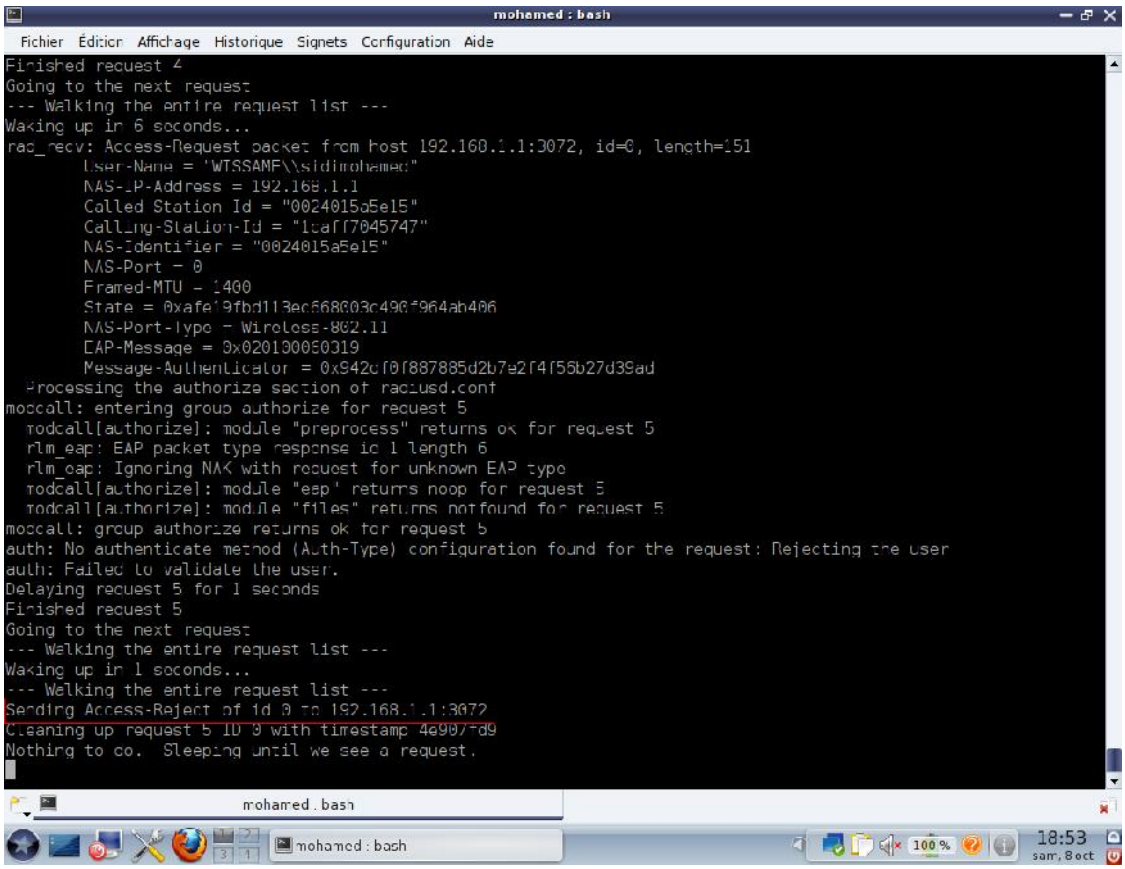

Figure III.52 : Autorisation rejeté du serveur pour le pirate

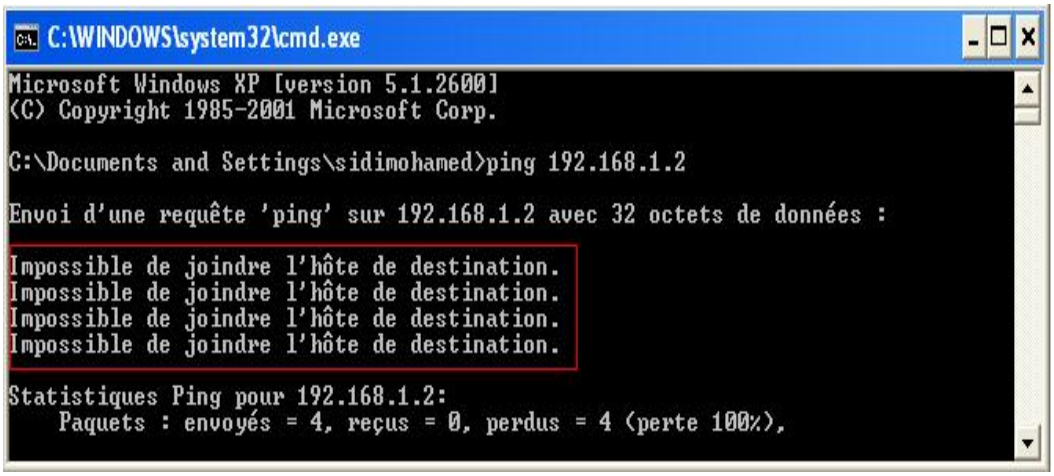

Figure III.53 : Echec du ping

Conclusion

On remarque que le réseau est maintenant sécurisé et que les usagers qui ne sont pas enregistrés dans le serveur comme étant des usagers autorisés, ne pourront pas accéder au réseau, ni même percevoir son existence.

Dans le cas ou la personne est en possession du SSID du réseau, elle ne pourra quand même pas y accéder sans les certificats qui sont installés aussi bien, dans les postes clients que dans le serveur.

L'échange des informations d'authentification, se fait de manière crypté et par un protocole amélioré, qui pour le moment n'a pas été cassé. En plus du fait que le protocole d'authentification 802.1x a donné de très bons résultats pour les réseaux filaires, à travers l'utilisation de serveur d'authentification sous linux, qui comme on le sait ne craint pas les virus.

Conclusion générale

Depuis leur apparition, les réseaux ont connu un franc succès, beaucoup de travaux ont traité ce sujet. Par contre, la sécurité dans les réseaux sans fil reste un domaine vaste et encore fertile pour les chercheurs et les développeurs.

Dans ce travail de PFE, on a passé en revue le fonctionnement général du réseau sans fil en particulier le Wi-Fi, puis son mécanisme de sécurité, avec tous les protocoles mis au point dans le but de le sécuriser.

Ce travail a été mené à bien et après plusieurs problèmes de gestion et d'installation, on a fini par sécuriser un réseau test, constitué d'un PC, un AP, et d'un serveur d'authentification radius.

En conclusion, ce travail qui est très intéressant et enrichissant du point de vue expérience acquise, peut être amélioré, en ne se contenant pas d'une authentification par certificats, mais par login et mot de passe.

Bibliographie

[1]: Administration réseau sous linux ,3eme édition, tony bautts, terry dawson &gregor n. purdy ; novembre 2006.

[2]: http://www.scribd.com/doc/469106/Informatique-Cours-Reseau-Sans-Fil-La-Technologie-Wifi

[3]: Architecture et sécurité de Wi-Fi. Mémoire de fin d'études présenté par PHILIPPART Raphaël ; année académique 2002-2003

[4]: http://www.securite-informatique.gouv.fr/gp_article250.html

[5]: http://www.memoireonline.com/06/10/3578/m_Le-reseau-informatique-dans-la-chaine-de-production-dune-societe-de-presse10.html;

[6]: http://www.commentcamarche.net/contents/wifi/wifiintro.php3; 21 novembre 2010

[7]: http://s208270930.onlinehome.fr/wordpress/?p=7779; octobre 2009

[8]: Analyse et simulation du déploiement d'un réseau sans fil à l'ULB. Mémoire de fin d'études présenté par Michel Duchateau en vue de l'obtention du grade d'Ingénieur Civil Electricien, spécialisé en Télécommunications. Année académique 2004-2005

[9]: http://www.commentcamarche.net/faq/3020-wifi-cours-d-introduction; 23 juin 2011

[10]: BALLESTEROS.M. (Les technologies sans fil) .EIVD, juin 2002.

[11]: Jon Edney and William A. Arbaugh, Real 802.11 Security, Wi-Fi Protected Access and 802.11i; septembre 2004

[12]: Joel Conover, Anatomy of IEEE 802.11b Wireless, aout 2000 http://www.networkcomputing.com/1115/1115ws2.html;

[13]: http://www.doc-etudiant.fr/Informatique/Reseaux-informatiques/Expose-Reseaux-sans-fil-WiFi-7439.html

[14]: http://www.pouf.org/documentation/securite/html/node1.html; 25 Aout 2004

[15]: http://guide-wifi.blogspot.com/2004/01/la-securite-wifi.html; 5 Janvier 2004

[16]: Guy Pujolle : « sécurité wifi » octobre 2004. Edition Eyrolles.

[17]: http://ditwww.epfl.ch/SIC/SA/publications/FI00/fi-sp-00/sp-00-page5.html; 5 septembre 2000

[18]: http://www.aidenet.com/encyclopedie/crypto/certificat.htm

[19]: Services d'Authentication et Annuaires ; Abdelghani MAZOUZI ; UFR Informatique ; UCB Lyon1 ; 14 décembre 2009

[20]: Les firewalls par Alban Jacquemin et Adrien Mercier; 15 février 2004 http://www.frameip.com/firewall/

[21]: Serge Bordères. Authentification réseau avec Radius. EYROLLES, 2007.

[22]: http://wapiti.telecom-lille1.eu/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2005/sert-deprey/pres.htm

[**23]:** http://www.gilbertetchristine.fr/article-partage-samba-sur-plusieurs-pc-mandriva-57684930.html; 25 septembre 2010

Abstract

Wi-Fi networks, based on the IEEE 802.11 b/g standards, have become very popular in recent years. Many users have installed Wi-Fi networks at home, and numerous corporations have added Wi-Fi access points to their wired networks, giving employees easier access to corporate data and services. Hackers can decrypt and read data on a wireless link protected by built-in WEP encryption, and may even be able to access the data on a wired network through a Wi-Fi access point. We assess Wi-Fi network security in one city, analyze alternative security techniques, and suggest ways to secure such networks.

الخلاصة

على الرغم من مميزات الشبكة اللاسلكية, إلا أن هناك ثغرات في السنوات الأخيرة, انتشر استخدام الشبكات اللاسلكية في المنازل والمؤسسات والشركات. ونادرا ما نجد جهاز كمبيوتر من دون خاصية الشبكة اللاسلكية. وعلى غرار نظائرها من الشبكات السلكية, فإن الشبكات اللاسلكية عرضة للاختراق وأكثر عرضة للمشاكل نتيجة لوجود ثغرات أمنية قد تسبب مشاكل في الشبكة. وهذه المشاكل قد تؤثر سلبا على مستخدميها سواء كانوا أفراد أو شركات. ولكن بأخذ الحيطة ومعرفة الثغرات الموجودة في الشبكة وإتباع الإجراءات المناسبة لسدها, فإن ذلك يساهم في توفير بيئة عمل أمنة تحقق الهدف من استخدام تلك الشبكات.