Thème :

AUTHENTIFICATION DANS LES RÉSEAUX WIFI PAR LE PROTOCOLE RADIUS

Réalisé par :

Fèten RIDENE Epse RAISSI & Adel RAISSI

Université Virtuelle de Tunis

PROJET DE FIN D'ETUDES

En vue de l'obtention du titre de

Licence Appliquée en Sciences et Techniques de l'Information et des Communications

Encadré par :

Mr Mohamed HAMDI

Année Universitaire:

2010/2011

Plan du Rapport

Dédicace de Fèten RIDENE Epse RAISSI à :

** Mon cher papa « MESKA » : Que Dieu bénisse son âme et l'amène au Paradis*

** Ma chère maman « SOUSOU »*

** Mon mari et binôme : ADEL*

** Toute ma belle famille RAISSI*

** SAMSOUMI, RANNOUNTI, NOUNOU*

** Tous ceux qui m'aiment et que j'aime…*

Je dédie ce modeste travail

Dédicace de Adel RAISSI à :

** Mon cher père Med SALAH*

** Ma chère mère ZOUHAIRA*

** Mes frères et sœurs*

** Ma chère femme et binôme : Fèten*

** Toute ma belle famille RIDENE*

** Saïda, Fayçal, Azzedine et Hammond*

** Toua(te)s mes collègues à L-SAT NOKIA*

Spécialement à SAMER

** Tous ceux qui m'aiment et que j'aime…*

Je dédie ce modeste travail

Remerciements

Nous soussignés, le binôme réalisant ce Projet de Fin d'Etudes : Fèten RIDENE E^{pse} RAISSI et Adel RAISSI, étudiants en LASTIC3, que nous tenons fortement à remercier tous ceux qui nous ont aidé à avoir cette chère et honorable occasion pour approfondir notre niveau de connaissance au domaine de la sécurité des réseaux, nous facilitant ainsi la prise en charge d'un cas réel, ayant le but d'authentifier et de sécuriser un réseau.

Nous remercions donc, tous ceux qui nous ont aidés, en particulier :

* UVT qui nous a attribué cette honorable chance

* Notre encadreur : Monsieur Mohamed HAMDI

* Tous nos collègues qui n'ont épargné aucun effort pour nous aider, à savoir nos collègues à Sup'Com et à L-SAT NOKIA, vu que leurs remarques et leurs consignes ont été pour nous d'un grand apport.

*L'Ecole Supérieure des Communications de Tunis : Sup'Com, et l'Institut Supérieur des Etudes Technologiques en Communications de *Tunis : ISET'COM,* dont les supérieurs nous ont fourni le lieu de travail nécessaire et le matériel dont nous avons besoin, pour bien réussir la réalisation de notre Projet de Fin d'Etudes dans les plus confortables conditions.

* Enfin nos meilleurs et vifs remerciements s'adressent aux membres du jury pour avoir accepté d'évaluer ce projet.

Fèten RIDENE et Adel RAISSI

Etablissement d'accueil: Sup'Com

Créée en 1998, et placée sous la *double tutelle* du *Ministère de l'Enseignement Supérieur et de la Recherche Scientifique (Université de Carthage)* et du *Ministère de l'Industrie et de la Technologie (Secrétariat d'Etat des Technologies de la Communication)*, membre du *Réseau Méditerranéen des Ecoles d'Ingénieurs*, *admise à la Conférence des Grandes Ecoles (CGE), au mois de décembre 2008 en tant que membre associé, première école associée de l'Institut Télécom à l'international*, Sup'Com est une école d'ingénieurs qui a pour vocations :

- La formation d'ingénieurs de haut niveau scientifique et technique, aptes à concevoir, mettre en ouvre et gérer les services, les systèmes et les réseaux de télécommunications.
- La contribution à l'effort national relatif à la recherche scientifique et technologique dans le domaine des technologies de l'information et la communication (TIC).
- La formation continue ou qualifiante des cadres supérieurs dans le domaine des TIC.

Etablissement d'accueil : Sup'Com

TABLE DES MATIÈRES

Liste des Figures

AVANT PROPOS

Dans le cadre de l'obtention du certificat de la *Licence Appliquée en Sciences de l'Information et de Communication*, au sein de *l'Université Virtuelle de Tunis*, nous étions appelés à réaliser un projet de fin d'études, dans un milieu industriel, dans notre cas, nous étions accueillis par un établissement académique : l'Ecole Supérieure des Communications de Tunis : *Sup'Com*, située au Technopôle EL GHAZELA. Notre projet a duré quatre mois : de Mars à Juin 2011.

Dans ce contexte, se situe le présent travail, qui consiste à authentifier et sécuriser l'accès à un réseau WiFi, et ce à travers le protocole d'authentification RADIUS.

Le travail consiste à mettre en place un réseau sans fils, qui doit respecter les normes de sécurité, dans le but de minimiser le risque d'attaques, en garantissant l'authentification et l'identification des utilisateurs grâce au protocole RADIUS.

Ce projet nous a été d'une grande utilité, vu qu'il nous a permis de :

- ☞ Nous familiariser sur le plan pratique avec les différentes tâches et opérations effectuées, afin de sécuriser un réseau sans fils dans le cadre académique.
- ☞ Avoir une idée sur la méthode adéquate de maintenir un réseau sans fil en sécurité, évitant ainsi -grâce à des systèmes et des protocoles bien déterminés- toute tentative illégale d'accès ou de modification des bases de données privées et secrètes des clients authentifiés (étudiants, enseignants, services technique et administratif, visiteurs…).

INTRODUCTION GÉNÉRALE

Dans l'objectif de garantir une meilleure accessibilité aux services réseau, plusieurs architectures de communication modernes ont privilégié l'abandon des câbles de transmission au profit des liaisons radio. Ces liaisons peuvent être soit du type *infrarouge*, *Bluetooth* ou *Hertziennes.* Nous parlons donc des **liaisons sans fils,** qui ont pris une grande ampleur avec l'apparition de concentrateurs qui permettent de connecter simultanément plusieurs nœuds entre eux. Il peut s'agir d'ordinateurs, d'imprimantes, de terminaux GSM ou de périphériques divers. Les liens radio sont même utilisés pour interconnecter des réseaux. A l'échelle d'un réseau local, l'utilisation de l'air libre comme support de transmission, consiste au déploiement des réseaux WiFi, régis par les normes IEEE 802.11.

Les technologies dites « sans fils », la norme 802.11g en particulier, facilitent et réduisent le coût de connexion pour les réseaux de grandes tailles. Avec peu de matériel et un peu d'organisation, de grandes quantités d'informations peuvent maintenant circuler sur plusieurs centaines de mètres, sans avoir recours à une compagnie de téléphone ou decâblage.

La mise en œuvre des réseaux sans fils est facile, mais la sécurité des données qui y sont transmises n'est pas toujours assurée. Ceci est dû, en grande partie, aux vulnérabilités intrinsèques du lieu radio.

Une attaque -qui a pour but d'intercepter les communications sans fils entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis- peut avoir lieu si le canal n'est pas sécurisé. L'attaquant est alors capable d'observer, d'intercepter et de modifier les messages d'une victime à l'autre. Son intrusion est facilement possible, quand le réseau en question n'est pas assez sécurisé d'autant plus facile que l'accès au réseau ouvert. Cet utilisateur malveillant peut accéder au réseau sans fils qu'il attaque, tout en utilisant une fausse identité. Il peut par exemple, modifier un message

M partant d'un expéditeur X au destinataire Y selon l'attaque dite *MAN IN THE MIDDLE,* qui lui permet de remplacer le message M par un autre message M' après l'avoir modifié, sans que X et Y ne s'en rendent compte.

Ce type d'attaque, et plusieurs autres, dont notamment le vol des informations du type propriétés intellectuelles, le déni de service et l'Usurpation d'Identité, nous ont appelés à étudier ces vulnérabilités d'authentification des réseaux WiFi, et à trouver des solutions potentielles, basées sur les protocoles d'authentification, en prenant Radius comme solution adéquate.

RADIUS (Remote Authentification Dial-In User Service), est un protocole client-serveur, permettant de centraliser des données d'authentification. L'opération d'authentification est initiée par un client du service RADIUS, qui est dans notre cas un point d'accès réseau sans fils. Le poste utilisateur transmet une requête d'accès à un client RADIUS pour entrer sur le réseau. Ce client (ou point d'accès) se charge de demander les informations identifiant l'utilisateur, qui seront dans notre cas : le nom d'utilisateur (login), le mot de passe et l'adresse Mac de la carte réseau WiFi, à travers laquelle, un étudiant, un personnel, ou même un visiteur passager de Sup'Com, pourra se connecter.

Pour réaliser ce projet, nous avons commencé par effectuer des recherches, pour étudier :

- ☞ Les faiblesses des réseaux WiFi, et notamment les possibilités techniques de se connecter sous une fausse identité.
- ☞ Les types d'attaques qui peuvent avoir lieu dans un environnement académique.
- ☞ Les mécanismes de protection –existants- des réseaux WiFi, et leur efficacité par rapport aux attaques visant l'authentification.

Après avoir effectué ces recherches, et pour pouvoir choisir le protocole d'authentification qui conviendra à nos besoins, nous avons effectué :

- Une étude comparative des protocoles d'authentification pour les réseaux WiFi.
- Une revue des services d'authentification applicatifs disponibles pour les réseaux WiFi.

Sur la base de cette étude, nous avions proposé une architecture qui permet de subvenir aux besoins de Sup'Com, en termes de protection contre l'usurpation d'identité.

Le coût de la solution, en termes d'effort de déploiement, a été aussi pris en compte, lors de la conception de cette architecture.

Enfin, pour que cette étude théorique soit évaluée, nous avons effectué les étapes suivantes :

- La mise en place d'un réseau de test, qui permet de simuler l'environnement réel.
- L'évaluation des performances de la solution proposée.

CHAPITRE 0 : PRÉSENTATION DE L'ÉTABLISSEMENT D'ACCUEIL

0.1- Infrastructure sans fils de l'Université Sup'Com :

L'usage du réseau WiFi à l'Ecole Supérieure des Communications de Tunis (Sup'Com), requiert une validation d'identité basée sur l'identifiant et le mot de passe de l'utilisateur : étudiant, membre du personnel de l'Université ou visiteur : dans ce dernier cas, il est nécessaire de connecter à ce réseau une personne extérieure (ne disposant donc pas d'un identifiant) et pour laquelle, nous allons créer un compte temporaire.

Sup'Com se dote déjà d'une infrastructure sans fils couvrant très largement les sites de l'Institution. Cette infrastructure doit permettre aux personnes disposant d'ordinateurs portables, de se déplacer dans les locaux de Sup'Com, tout en conservant une connexion réseau avec les facilités qui y sont associées (mail, accès internet, ...).

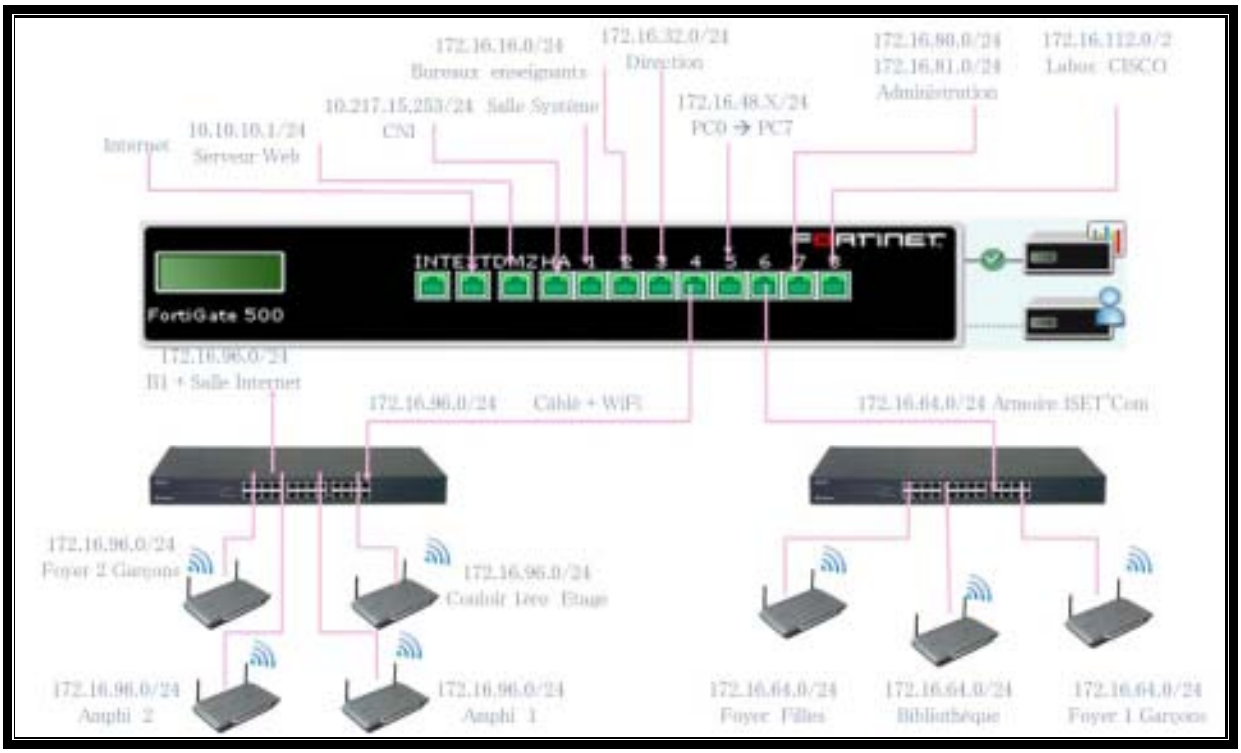

Figure 0.1 : Plan du réseau WiFi faisant partie du réseau Sup'Com

L'utilisation de cette infrastructure est autorisée pendant toute l'année universitaire, mais les examens de Travaux Pratiques et de Travaux Dirigés, sont obligatoirement passés sur des PCs de bureau,

utilisant une connexion câblée, qui assure plus de performance et plus de fiabilité.

Actuellement, tous les postes équipés de carte WiFi supportant les normes 802.11b ou 802.11g doivent pouvoir se connecter. Les avantages de cette connexion sont notoires: toute activité sur le réseau WiFi de Sup'Com est chiffrée (cryptée). Pour mieux la sécuriser, nous pouvons rendre cette connexion authentifiée et chiffrée (pas d'usurpation d'identité). Ceci limitera donc, considérablement, les risques d'espionnage : l'utilisateur ouvre son navigateur web, et tente d'accéder à une page de son choix. Il reçoit alors immédiatement une demande d'authentification et doit fournir son identifiant et son mot de passe, et obtiendra ainsi l'accès au réseau.

C'est donc pour proposer d'approfondir le niveau de sécurité du réseau WiFi, que nous avons effectué ce projet de fin d'études, visant sur le fait de trouver des solutions potentielles d'authentification, et ce en étudiant les différents types d'attaques possibles et en cherchant la solution adéquate.

CHAPITRE 1 : ETUDE GÉNÉRALE SUR LA SÉCURITÉ DES RÉSEAUX WIFI

1.1-FAIBLESSES DES RÉSEAUX WIFI :

Les ondes radioélectriques ont intrinsèquement une grande capacité de se propager dans toutes les directions avec une portée relativement grande. Il est ainsi très difficile d'arriver à confiner les émissions d'ondes radio dans un périmètre restreint. Ainsi les ondes se propagent également d'un étage à un autre (avec de plus grandes atténuations). La principale conséquence de cette propagation incontrôlée des ondes radio, se résume dans la facilité que peut avoir une personne non-autorisée d'écouter le réseau, éventuellement en dehors de l'enceinte du bâtiment où le réseau sans fils est déployé.

C'est là où le bât blesse, qu'un réseau sans fils peut être très bien installé : dans une entreprise par exemple, sans que cela ne soit explicitement autorisé par les administrateurs ! En effet, il suffit à un employé de brancher un point d'accès sur une prise réseau pour que toutes les communications du dit réseau soient rendues « publiques » dans le rayon de couverture du point d'accès.

1.2- ATTAQUES POSSIBLES CONTRE LES RÉSEAUX WIFI :

1.2.1-L'intrusion réseaux :

Lorsqu'un point d'accès est installé sur le réseau local, il permet aux stations d'accéder au réseau filaire et éventuellement à Internet si le réseau local y est relié. Un réseau sans fils, non-sécurisé, représente de cette façon un point d'entrée royal pour le pirate au réseau interne d'une entreprise ou d'une organisation. Outre le vol ou la destruction d'informations présentes sur le réseau et l'accès à internet gratuit pour le pirate, le réseau sans fils peut également représenter une aubaine pour ce dernier dans le but de mener des attaques sur Internet.

En effet, étant donné qu'il n'y a aucun moyen d'identifier le pirate sur le réseau, l'entreprise -ayant installé le réseau sans fils- risque d'être tenue responsable de l'attaque.

1.2.2-Le Wardriving :

Etant donné qu'il est très facile de réaliser des « écoutes » sur les réseaux sans fils, une pratique simple consiste à circuler dans la ville avec un ordinateur portable (voire un assistant personnel) équipé d'une carte réseau sans fils, il s'agit du *war-driving*. Des logiciels spécialisés dans ce type d'activité, permettant même d'établir une cartographie très précise en exploitant un matériel de géo-localisation (GPS= Global Positionning System).

Les cartes établies permettent ainsi de mettre en évidence les réseaux sans fils déployés non sécurisés, offrant même parfois un accès à internet ! De nombreux sites capitalisant ces informations ont vu le jour sur internet, si bien que des étudiants londoniens ont eu l'idée d'inventer un « langage des signes », dont le but est de rendre visibles les réseaux sans fils en dessinant à même le trottoir des symboles à la craie indiquant la présence d'un réseau WiFi, il s'agit du « *war-chalking* » (francisé en craieFiti ou craie-fiti). Deux demi-cercles opposés désignent ainsi un réseau ouvert offrant un accès à Internet, un rond signale la présence d'un réseau sans fils ouvert sans accès à un réseau filaire et enfin un W encerclé met en évidence la présence d'un réseau sans fils correctement sécurisé.

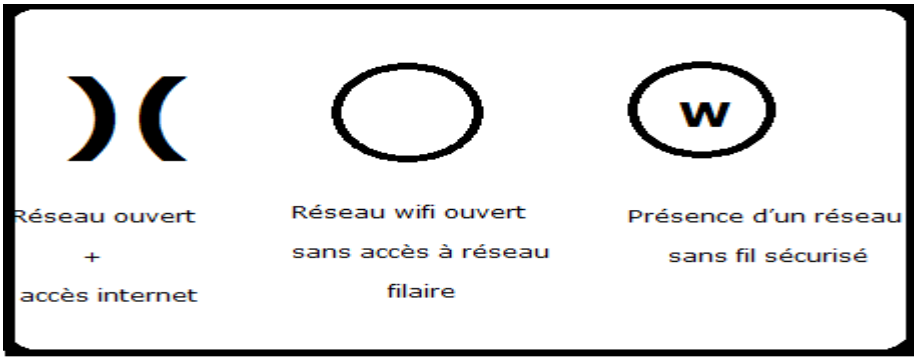

Figure 1.1 : War-Chalking

1.2.3- Les risque sur un réseau WiFi

Les risques liés à la mauvaise protection d'un réseau sans fils sont multiples :

- ✓ L'interception de données, consistant à écouter les transmissions des différents utilisateurs du réseau sans fils.
- ✓ Le détournement de la connexion, dont le but est d'obtenir l'accès à un réseau local ou à internet.
- ✓ Le brouillage des transmissions, consistant à émettre des signaux radio de telle manière à produire des interférences.
- ✓ Les dénis de service rendant le réseau inutilisable en envoyant des commandes factices.

Toutes ces menaces sont expliquées ci-dessous.

1.2.3.1-L'interception des données :

Par défaut un réseau sans fils est non sécurisé, c'est-à-dire qu'il est ouvert à tous et que toute personne se trouvant dans le rayon de portée d'un point d'accès peut potentiellement écouter toutes les communications circulant sur le réseau. Pour un particulier la menace est faible car les données sont rarement confidentielles, si ce ne sont pas les données à caractères personnel. Pour une entreprise en revanche, l'enjeu stratégique peut être très important.

1.2.3.2-Le brouillage radio :

Les ondes radio sont très sensibles aux interférences, c'est la raison pour laquelle un signal peut facilement être brouillé par une émission radio, ayant une fréquence proche de celle utilisée dans le réseau sans fils. Un simple four à micro-ondes peut ainsi rendre totalement inopérable un réseau sans fils lorsqu'il fonctionne dans le rayon d'action d'un point d'accès.

1.2.3.3-Le déni de service :

La méthode d'accès au réseau de la norme 802.11 est basée sur le protocole *CSMA/CA*, consistant à attendre que le réseau soit libre avant d'émettre. Une fois la connexion établie, une station doit s'associer à un point d'accès afin de pouvoir lui envoyer des paquets. Ainsi, les méthodes d'accès au réseau et d'association étant connues, il est simple pour un pirate d'envoyer des paquets demandant la dissociation de la station. Il s'agit d'un déni de service, c'est-à-dire envoyer des informations de telle manière à perturber volontairement le fonctionnement du réseau sans fils.

D'autre part, la connexion à des réseaux sans fils est consommatrice d'énergie. Même si les périphériques sans fils sont dotés de fonctionnalités leur permettant d'économiser le maximum d'énergie, un pirate peut éventuellement envoyer un grand nombre de données (chiffrées) à une machine de telle manière à la surcharger. En effet, un grand nombre de périphériques portables (assistant digital personnel, ordinateur portable,…) possèdent une autonomie limitée, c'est pourquoi un pirate peut vouloir provoquer une surconsommation d'énergie de telle manière à rendre l'appareil temporairement inutilisable, c'est ce que l'on appelle un *déni de service sur batterie.* D'autres techniques peuvent bien mener au même résultat.

1.3-Exemple d'une attaque sur les réseaux WiFi : ARP Spoofing

Ettercap est une suite d'outils dont le but principal est d'effectuer des attaques par «*Man In The Middle* » sur un réseau local. Il peut être utilisé comme une invite de commandes ou tout en étant une interface graphique. Une fois placé, il permet de :

- ☞ Infecter, remplacer et supprimer des données dans une connexion.
- ☞ Découvrir des mots de passe pour des protocoles comme FTP, http, POP3, SSH1,…

- Fournir aux victimes de faux certificats SSL dans des sessions HTTPS.
- Etc. …

Des plugins sont aussi disponibles pour des attaques comme le DNS Spoofing (usurpation DNS).

1.3.1-Qu'est ce qu'une attaque par « *man in the middle* » ?

C'est un type d'attaque, lors de laquelle, un pirate place sa machine sur le chemin logique entre deux autres machines qu'il veut attaquer. Une fois dans cette position, il peut alors lancer un grand nombre d'attaques, particulièrement dangereuses.

Il y a plusieurs types d'attaques pour devenir « *man in the middle* ». Nous allons voir dans cette partie du chapitre, des attaques basées sur le protocole ARP.

Le protocole ARP est utilisé pour traduire des adresses IP (ex : 172.16.112.74) en adresses physiques de carte réseau, autrement dites : adresse MAC (ex : 00-30-4f-54-40-a7). Quand un équipement essaye d'accéder à une ressource réseau, il va d'abord envoyer des requêtes vers les autres équipements, pour connaître l'adresse MAC qui est associée avec l'adresse IP qu'il veut atteindre. Cet équipement va garder l'association IP – MAC, comme adresse dans son cache (le cache ARP), et ce pour accélérer de nouvelles connexions vers cette même adresse IP.

L'attaque survient, quand une machine demande aux autres, de trouver l'adresse MAC associée à une adresse IP. Le pirate va alors répondre au demandeur avec des paquets, indiquant que l'adresse IP est associée à sa propre adresse MAC. Par ce biais, il va court-circuiter la vraie réponse d'association IP–MAC venant d'une autre hôte. Cette attaque est référencée en tant qu'Usurpation ARP (*ARP poisoning ou ARP Spoofing*). Elle n'est possible que si le pirate et les victimes sont à l'intérieur du même domaine de broadcast qui est défini au niveau d'une hôte par une adresse IP et un masque de sous réseau, dans notre cas :

172.16.112.70 (l'adresse du point d'accès) remplacera l'adresse 172.16.112.75 (l'adresse de la machine attaquante ou pirate), sachant que le masque de sous réseau est : 255.255.0.0.

Dans notre projet, nous avons appliqué cette attaque -schématisée ci dessous- où une machine avec l'adresse IP 172.16.112.75, atteint des ressources Internet à partir d'un réseau local. Après l'usurpation ARP, la machine, effectuant l'attaque par Ettercap, sera placée en tant que « *man in the middle* », mettant la machine 172.16.112.72 comme victime d'Usurpation.

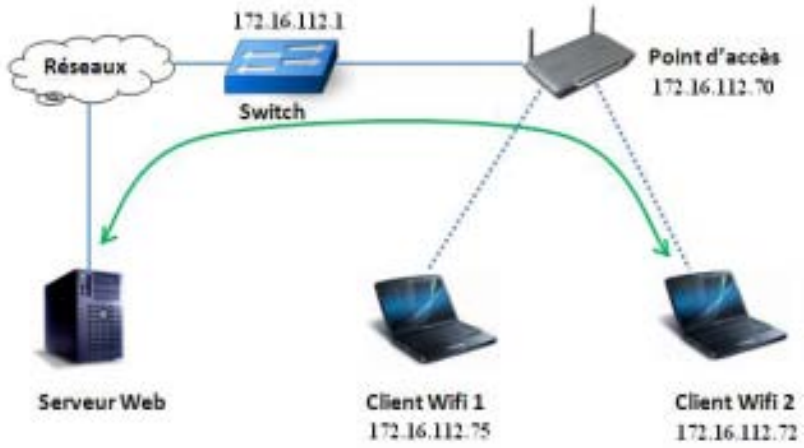

Figure 1.2 : Réseau WiFi avant Usurpation

Il est bon de rappeler les informations à propos du comportement de la machine Ettercap après ce schéma :

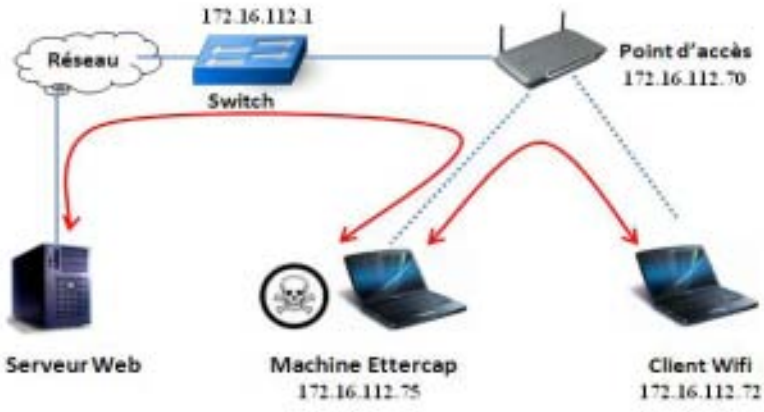

Figure 1.3 : Réseau WiFi après Usurpation⇔ Attaque « Man In The Middle : MITM »

Chaque fois qu'Ettercap démarre, il désactive la redirection IP (IP forwarding) dans le noyau, et commence lui-même à rediriger des paquets. Il peut *ralentir les performances réseaux entre les deux hôtes en raison du temps de traitement sur sa machine*.

Ettercap a besoin des privilèges *root,* pour ouvrir les sockets de la couche liaison de données LLS (*Link Layer Sockets*). Après la phase d'initialisation, les privilèges root ne sont plus nécessaires, Ettercap les modifie en no body. Si Ettercap doit écrire ou créer des fichiers journaux (*log files*), il doit être exécuté dans un dossier avec les permissions appropriées.

Ainsi, le but de notre démonstration d'Ettercap dans ce chapitre, était de montrer le danger des attaques « *man in the middle* » par Usurpation ARP. Nous allons maintenant montrer des exemples d'attaques réalisées avec Ettercap. Et enfin, nous profiterons de quelques contre-mesures, inventées pour lutter contre ces attaques par usurpation ARP.

1.3.2- Usurpation de l'adresse MAC

Avant d'effectuer l'attaque, nous avons lancé la commande **arp-a,** et nous avons trouvé que l'adresse IP du poste attaquant est: 172.16.112.75. C'est cette adresse qui sera remplacée par celle du point d'accès 172.16.112.70. Sachant que le serveur DHCP est configuré pour attribuer automatiquement des adresses IP entre 172.16.112.71 et 172.16.112.90.

La figure suivante, nous donne le résultat de la commande arp –a, avant que l'attaque ait lieu.

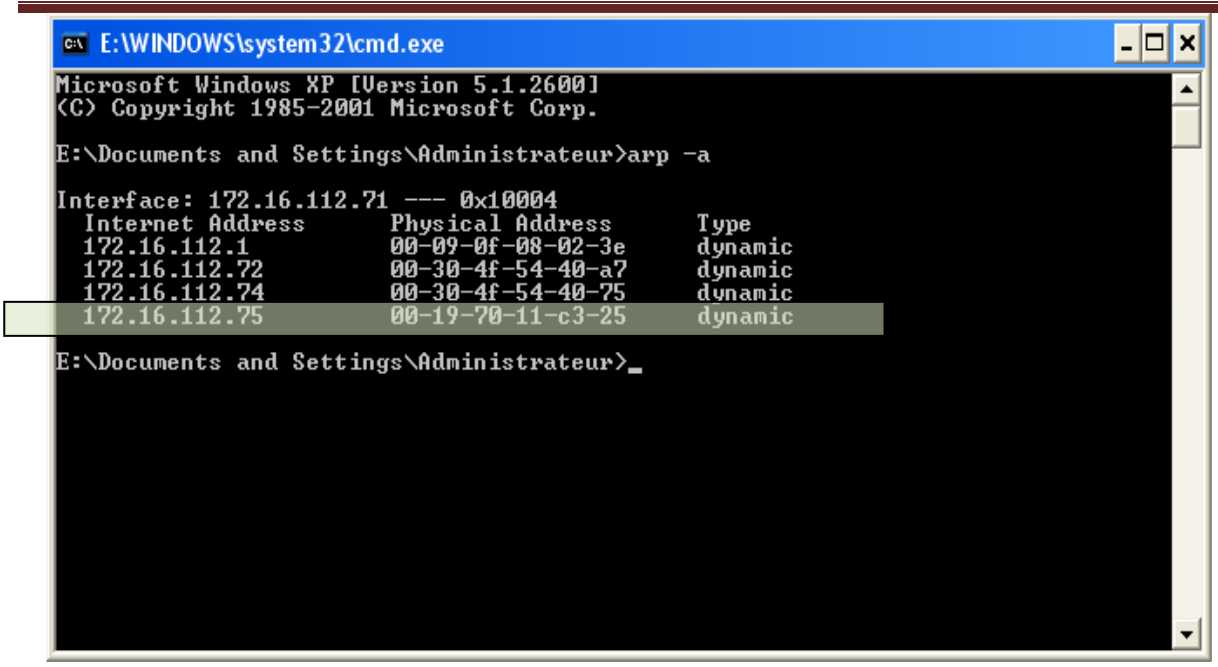

Figure 1.4 : arp avant l'attaque

Une fois l'usurpation a eu lieu, nous allons la comparer en lançant la commande **arp-a**, pour voir la différence.

Nous pouvons le vérifier aussi par la commande **IP config** qui montre l'adresse IP du PC attaquant et son adresse physique, avant d'effectuer l'attaque, pour en déduire plutard la différence :

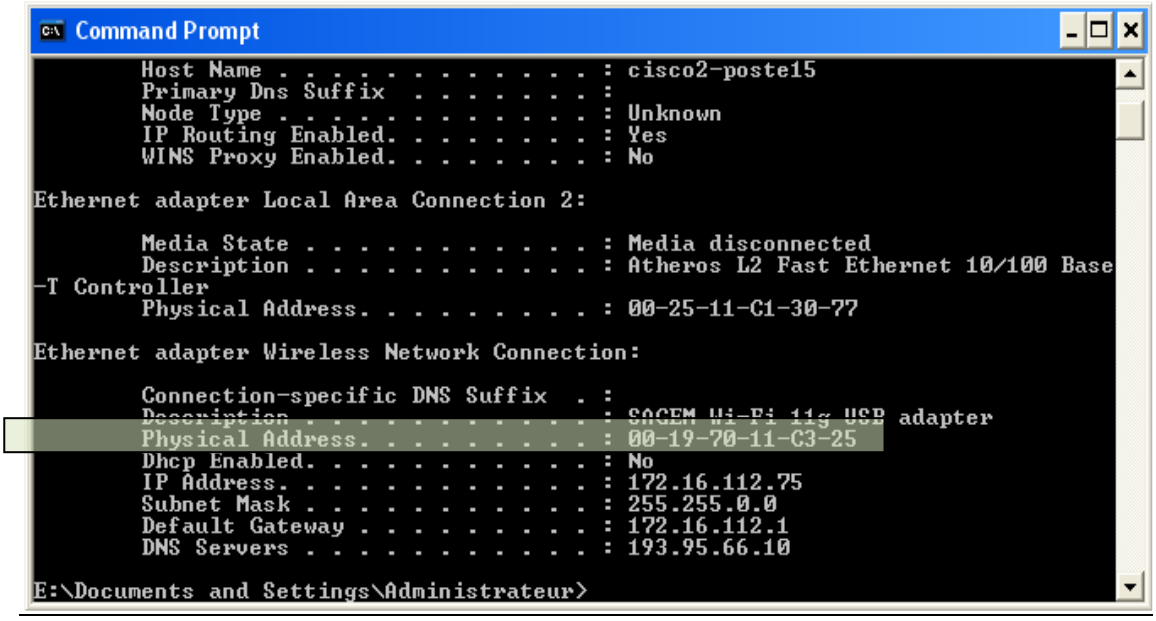

Figure 1.5 : Mac réelle de l'attaquant

On trouve alors Ettercap en mode graphique, et depuis le menu **Sniff**, on clique sur **Unified sniffing**

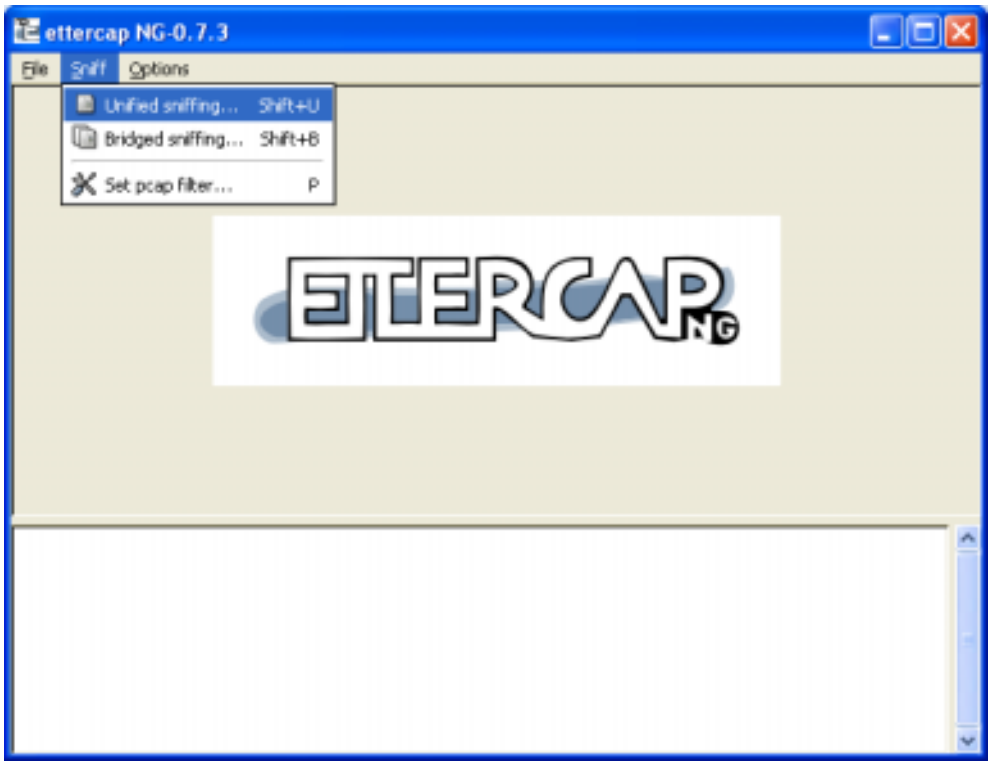

Figure 1.6 : Unified Sniffing

Ça mènera à l'apparition d'une liste de choix pour sélectionner la carte réseau à travers laquelle on se connecte (dans notre cas WiFi nous allons sélectionner la clé WiFi SAGEM, installée sur le poste du bureau pour tester l'accès sans fils.

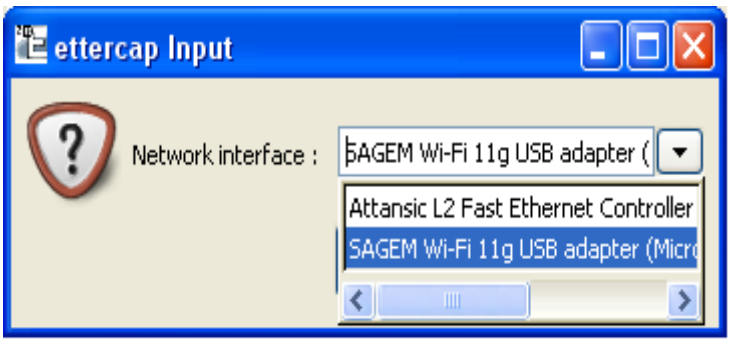

Figure 1.7: Carte WiFi attaquante

Ettercap nous affiche ainsi le résultat suivant :

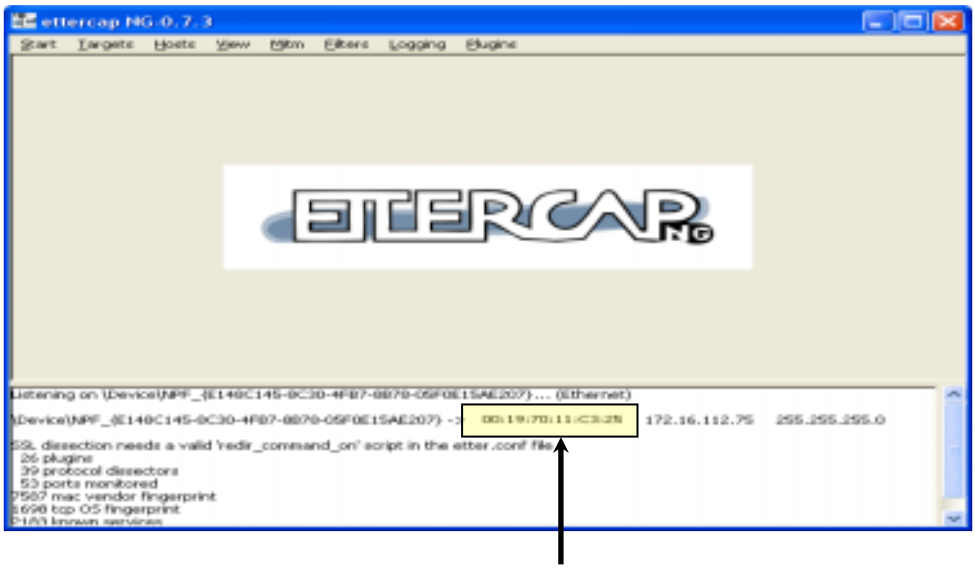

Figure1.8 : Mac de l'attaquant qui sera modifiée

On y trouve l'adresse IP de la machine en question (l'attaquant) et le masque de sous-réseau, sur lequel elle est configurée.

Et nous allons maintenant scanner le sous réseau pour découvrir des hôtes en cliquant sur le menu **Hosts** puis sur **Scan for hosts**.

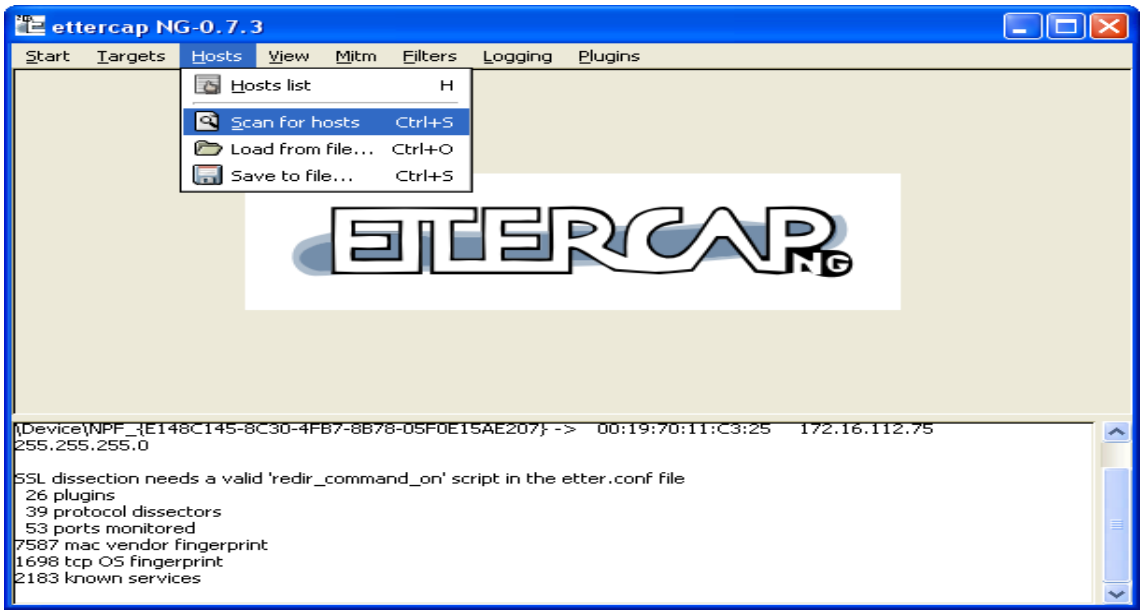

Figure 1.9 : Détection des hôtes connectées pour en choisir la victime

Puis on clique sur le menu **Hosts** et le sous menu **Hosts List** : ça nous affichera la liste des adresses IP des machines détectées sur la même plage d'adresse. On en sélectionnera la passerelle par défaut (le

point d'accès ayant l'adresse : 172.16.112.70) et on l'ajoute à **target1** en cliquant sur **Add to Target1**, son adresse IP sera attribuée au PC attaquant pour remplacer la sienne.

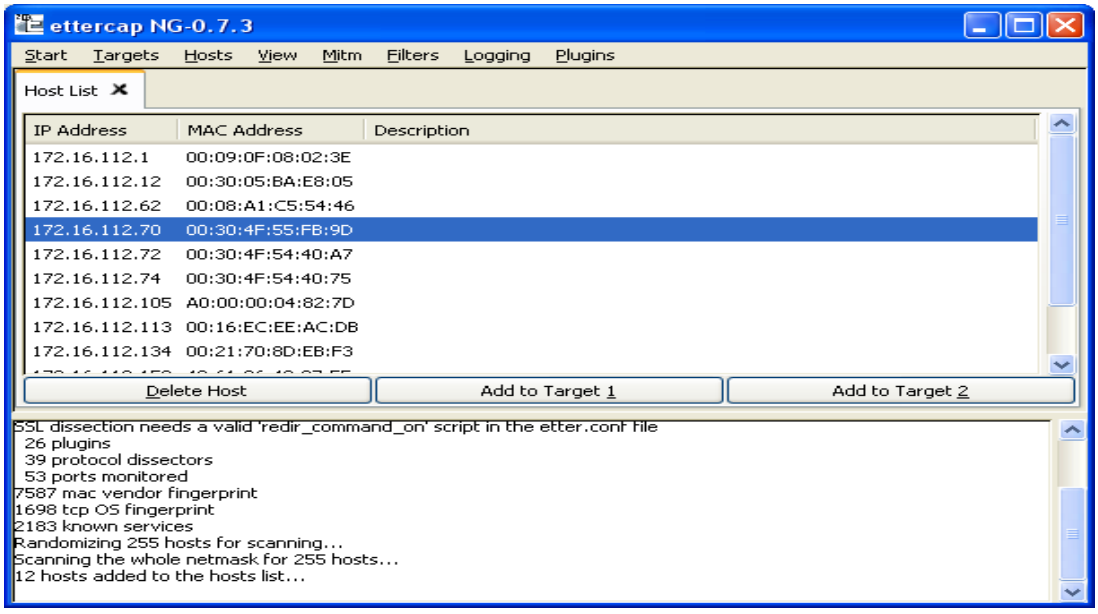

Figure 1. 10 : Target 1

Puis on sélectionne la machine à usurper (à empoisonner) : 172.16.112.72 et on l'ajoute à **Target 2** en cliquant sur **Add to Target 2**

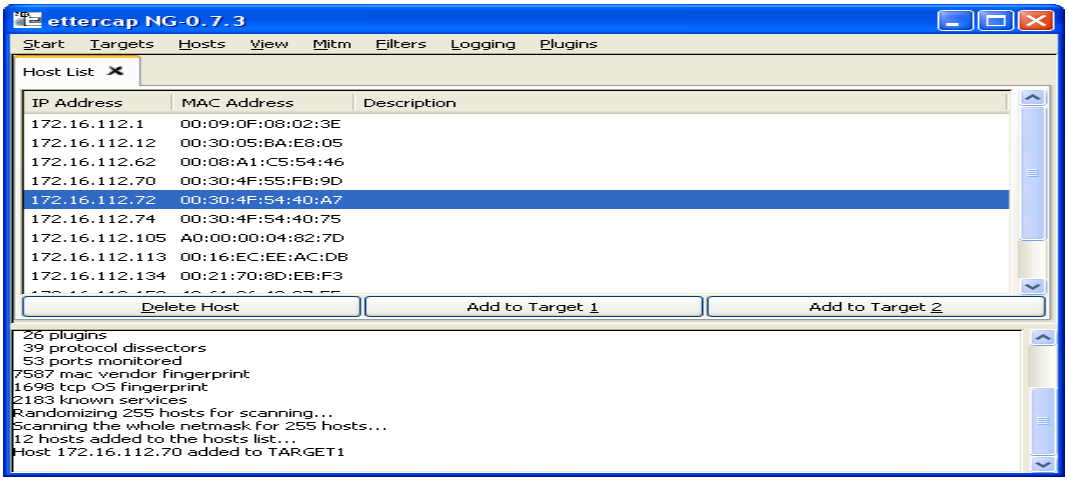

Figure 1. 11 : Target 2

N.B : Si on ne choisit aucune machine en cible (Target2), toutes les machines à l'intérieur du sous-réseau seront usurpées.

Nous allons maintenant vérifier les cibles (**Targets**) en cliquant sur le menu **Target** puis le sous menu : **Current Targets**.

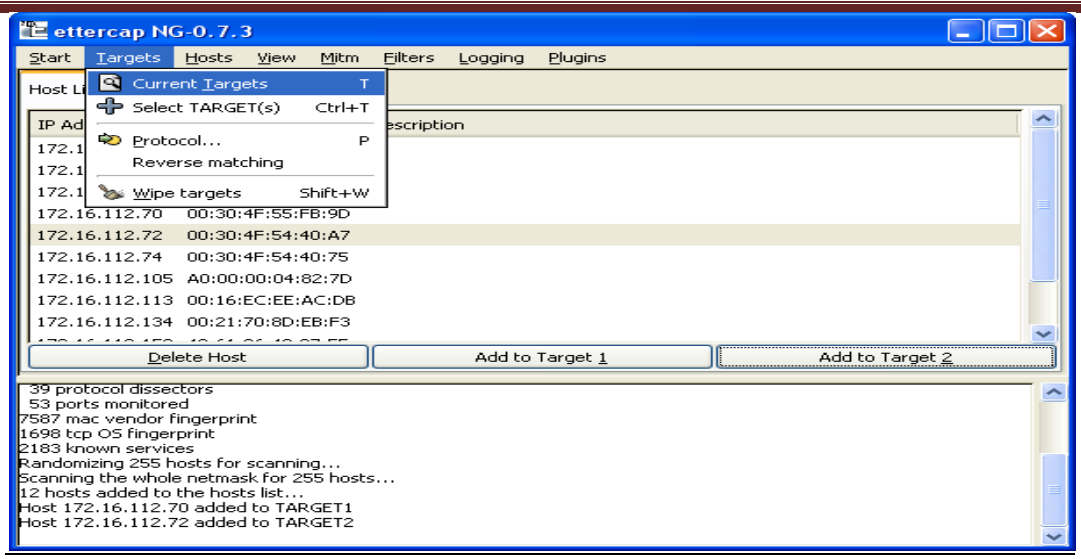

Figure 1.12.1 : Current Targets

Ca mènera au résultat suivant :

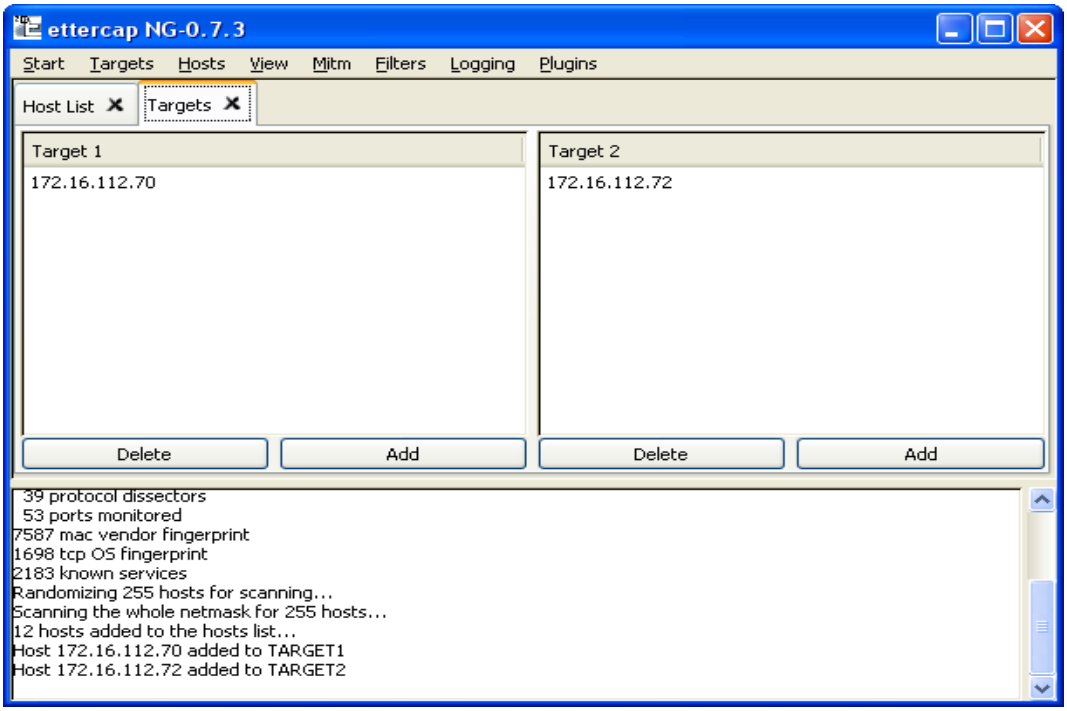

Figure 1 .12.2: Current Targets

Et maintenant nous allons démarrer l'usurpation en cliquant sur le menu **Mitm** puis sur le sous-menu **Arp poisonning :**

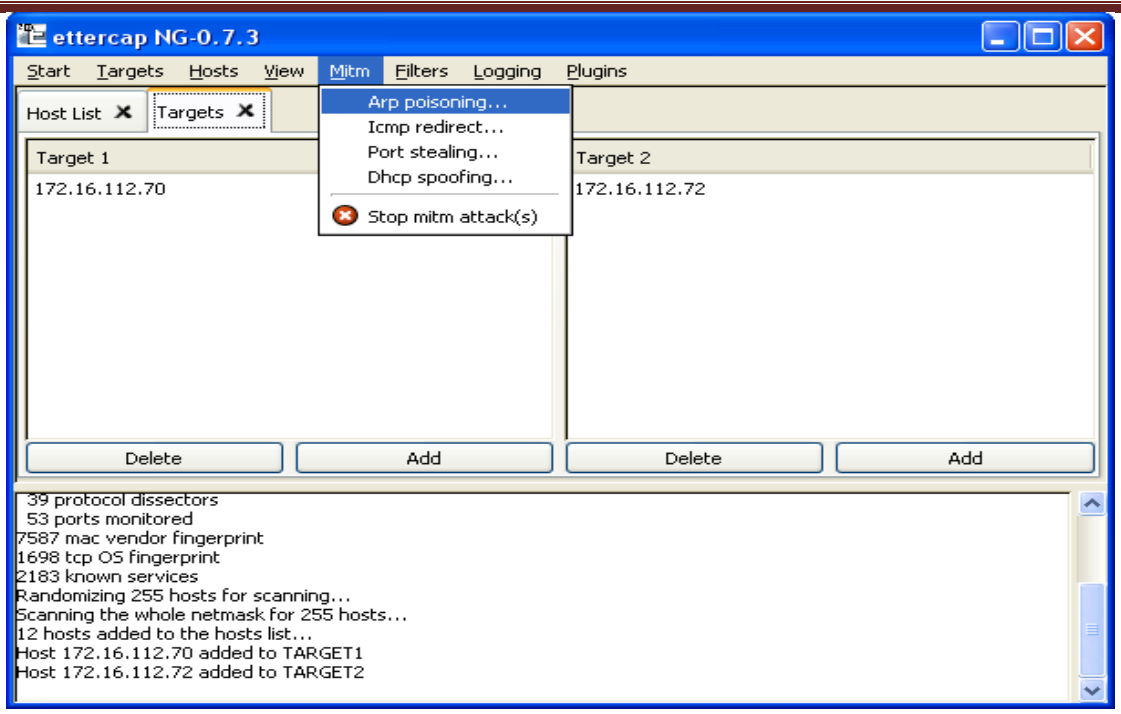

Figure 1.13 : Arp poisonning

La fenêtre suivante apparaîtra alors, pour nous permettre de choisir le type d'attaque :

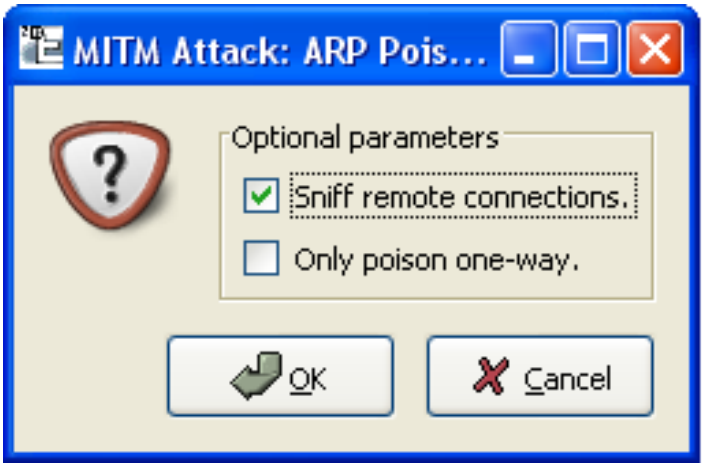

Figure 1.14: Choix de l'attaque

On y sélectionne *sniff remote connections,* et on exécute le *sniffer* pour collecter des statistiques en cliquant sur le menu **Start** et le sous menu **start sniffing**.

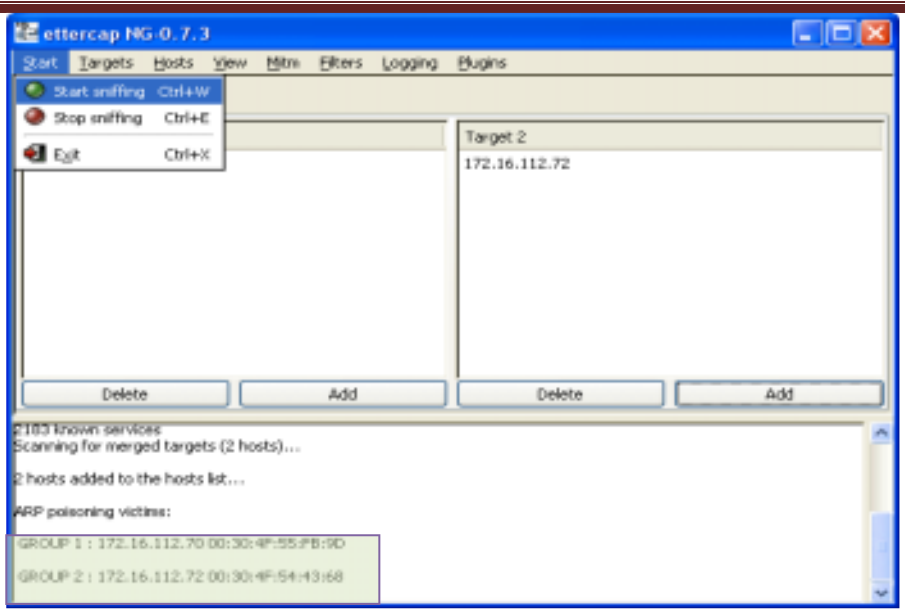

Figure 1.15 : Start Sniffing

Ca nous affiche l'adresse physique du point d'accès qui sera attribuée à la machine attaquante pour remplacer la sienne et celle de la victime avec son MAC aussi.

Enfin, en cliquant sur le menu **Plugins** puis sur **chk_poison**, ça nous confirmera que l'usurpation a bien réussi.

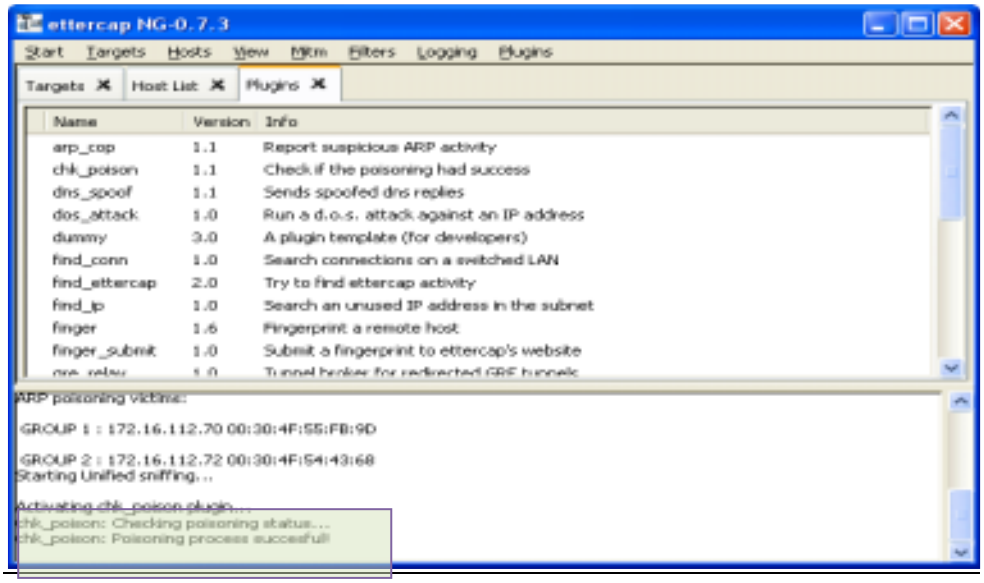

Figure 1.16 : Chk_poison « successfull »

On relance alors la commande **arp –a** de nouveau, pour la comparer avec celle qu'on a lancée avant l'attaque, et ça nous donne le résultat suivant :

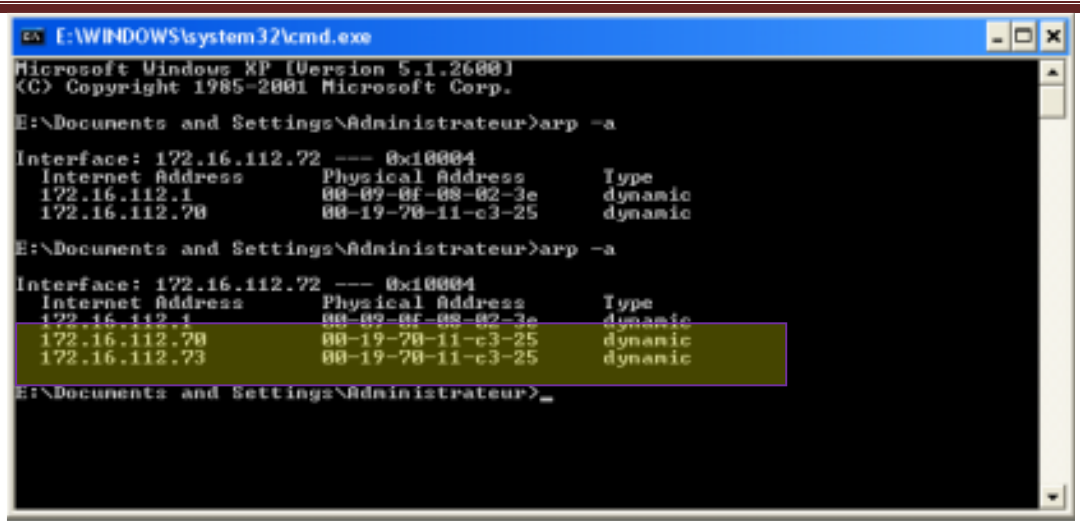

Figure 1.17 :L'adresse MAC du point d'accès attribuée à l'attaquant

On en déduit donc, que l'adresse MAC du point d'accès, a été la même adresse MAC attribuée au PC attaquant, dont l'adresse IP est 172.16.112.73.

1.4-Les mécanismes de la sécurité disponibles pour les réseaux WiFi

1.4.1-Aspects de base de la sécurité des réseaux :

La sécurité d'un système d'information consiste à mettre en œuvre des protections permettant d'assurer les trois propriétés suivantes :

1.4.1.1-La confidentialité des données : (Protection contre l'écriture non-autorisée) :

Elle correspond à la prévention de la divulgation non-autorisée de l'information.

Assurer la confidentialité, c'est faire de sorte que les informations soient inaccessibles ou incompréhensibles, pour des tiers qui ne possèdent pas les privilèges requis.

1.4.1.2-L'intégrité des données (protection contre la modification) :

Assurer l'intégrité des données consiste à la prévention de modification non-autorisée de l'information, par un utilisateur non autorisé à le faire, que l'opération soit réalisée de manière intentionnelle ou non.

1.4.1.3-Disponibilité des services (Détection d'utilisation illégale) :

L'accès et l'utilisation des services doivent toujours être possibles pour les personnes habilitées à le faire, dans le temps le plus bref, en tenant compte des ressources du système. Toute utilisation des ressources, destinée à ralentir ou à bloquer le système, doit pouvoir être détectée et contrecarré.1.4.2-Définition de l'authentification :

1.4.2-Définition de l'Authentification

1.4.2.1-Au sens linguistique :

Nom du verbe authentifier, qui veut dire certifier la vérité, l'exactitude de quelque chose.

1.4.2.2- Au sens réseaux de communication :

L'authentification est une procédure qui consiste, pour un réseau de communication, à vérifier l'identité d'une entité (personne, groupe, ordinateur…), afin d'autoriser l'accès de cette dernière à des ressources (systèmes, réseaux, applications…).

L'authentification, dans son sens technologique, permet donc de valider l'authenticité de l'entité en question. Alors que l'identification revient simplement à soumettre une identité que l'authentification est à même de prouver.

1.4.2.3- Fondement de l'authentification :

Au niveau d'un réseau sécurisé, un utilisateur non-identifié ne doit pas pouvoir se connecter ; on doit alors utiliser un protocole d'authentification pour lui vérifier l'identité des entités autorisées à utiliser les ressources protégées.

Sécuriser le système d'information est de plus en plus difficile, surtout à l'heure où le nombre d'applications et le degré d'ouverture vers l'extérieur croissent.

Définir les entités autorisées à accéder au système d'information constitue l'une des bases de la sécurité. Une telle procédure, dite contrôle d'accès, est étroitement liée à l'authentification dans la mesure où l'identité des entités autorisées doit être vérifiée afin de faire face aux usurpateurs.

L'authentification englobe souvent des concepts et des approches différentes. Il y a plusieurs moyens d'authentification, qui sont généralement regroupés en trois grandes catégories :

- ☞ Ce que l'on connaît : un mot de passe, un code PIN …

- ☞ Ce que l'on a : une carte à puce, un certificat …
- ☞ Ce que l'on est : la biométrie.

L'authentification par mot de passe est utilisée en grande majorité dans les systèmes sécurisés, car elle est la plus simple à mettre en place. Nous verrons néanmoins les autres possibilités d'authentification et les avantages.

Sachant que les services définissent l'ensemble des opérations accessibles par des protocoles, les services d'authentifications regroupent donc l'ensemble des opérations pour s'authentifier, quel que soit le protocole et quelle que soit la couche OSI.

1.4.2.3.1-Chiffrement :

Il implique un mécanisme de distribution de clés et participe directement à divers services : la confidentialité, l'intégrité (en permettant la détection de la modification des données) et l'authentification (en protégeant le système contre les tentatives non autorisées de connexion).

Il convient de distinguer le chiffrement de voie obtenu par la mise en place de boîtes « sur les lignes » et en laissant les données en clair au niveau des hôtes et des nœuds du réseau.

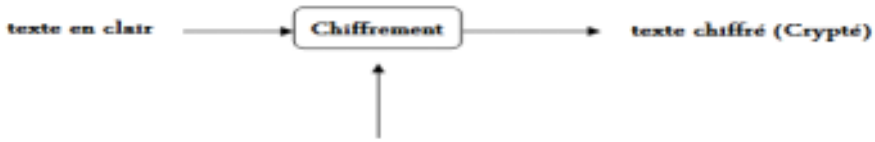

Figure 1.18 : Chiffrement

Et le chiffrement de bout en bout ait lieu, en laissant en clair uniquement les informations de routage. Le chiffrement peut être symétrique (*DED : data encryption standard*) ou asymétrique (*RSA : Rivest Shamir Adleman*=algorithme de cryptographie)

1.4.2.3.2-Echange d'authentification :

Lorsque les entités homologues et les moyens de communication sont considérés comme sûrs, l'identification de l'entité homologue est suffisante, elle peut être obtenue par un mot de passe. Ce dernier est efficace contre les erreurs mais pas contre les malveillances.

1.4.2.3.3-Signature avec ou sans notarisation :

Lorsque les identités se font mutuellement confiance, mais pas au moyen de communication, il convient d'employer une combinaison d'employer une combinaison de mot de passe + chiffrement pour s'authentifier mutuellement.

Lorsque les entités n'ont pas confiance aux moyens de communication, les mécanismes de signature numérique deviennent très nécessaires. La notarisation améliore la sécurité du système, dans la mesure où elles l'assurent aux entités, grâce à un tiers : le notaire, auquel elles se fient, l'intégrité, l'origine, la date, la destination, des données.

Le tiers, doit acquérir les informations nécessaires, par des communications protégées, et doit aussi les conserver.

1.4.2.3.4-Le contrôle d'accès :

Il utilise l'identité authentifiée des entités ou des informations fiables pour déterminer leur droit d'accès à une ressource. Il peut enregistrer sous forme de trace d'audit et signaler toute tentative non autorisée d'accès. Il peut mettre en jeu les listes maintenues par des centres ou par l'entité accédée : des mots de passe, des jetons utilisés pour distribuer les droits d'accès, des certificats -dis libellés -indiquant la sensibilité des données.

1.4.2.3.5- L'intégrité :

Elle s'obtient par l'utilisation des codes de détection d'erreur, des codes de contrôle cryptographique et de la numérotation des unités de données.

1.4.2.3.6- Bourrage :

Dans certains cas, l'accroissement du flux d'information entre deux entités, peut être significatif pour un tiers. Pour s'en protéger, on effectue un bourrage de voie. La ligne sera constamment utilisée, entre 2 émissions de messages dépourvus de sens.

Ces messages –inutiles seront éliminés à l'arrivée. Ils devront être variables et non identifiables comme message de bourrage par un ennemi. On utilisera pour cela 1 générateur de messages adéquat.

1.4.2.3.7- Contrôle de routage :

Ce sont les systèmes extrémistes ou les réseaux peuvent être amenés à sélectionner une route plus sûre, après détection d'une attaque persistante, ou pour tenir comte de la sensibilité des données.

CONCLUSION

Dans ce chapitre, nous avons présenté la problématique essentielle de notre projet, à savoir la sécurisation des réseaux WiFi, et ce en présentant un aperçu général sur ce type de réseaux.

Nous avons aussi discuté les attaques auxquelles ils sont sujets, en prenant l'Usurpation comme exemple.

Enfin, nous avons discuté d'une manière sommaire les solutions de sécurité qui sont aptes à être utilisées, et ce en focalisant notre intérêt sur les solutions d'authentification au vu des caractéristiques des systèmes WiFi.

Dans le chapitre suivant, nous proposerons donc une description plus détaillée des solutions potentielles.

CHAPITRE 2 : PROTOCOLES D'AUTHENTIFICATION POUR LES RÉSEAUX WIFI

2.1-SOLUTIONS POTENTIELLES :

Les protocoles ou les mécanismes d'authentification décrits dans ce chapitre, ont tout d'abord été des protocoles de la deuxième couche du model OSI (appelée liaison), puisqu'ils ont été initialisés par le Protocole PPP qui permet l'ouverture de session sur le réseau RTC. Actuellement, ils sont également utilisés dans la couche réseau grâce au passage de PPP à PPPoA (over ATM) et PPPoE (over Ethernet) qui sont principalement utilisés pour ouvrir des connexions ADSL.

Cependant, ces mécanismes sont les briques de nombreux serveurs et applications d'authentifications comme RADIUS, TACACS+, Kerberos,…

2.1.1- PAP

Le protocole PAP (Password Athentication Protocol), utilisé avec le Protocole PPP, permet d'identifier un utilisateur auprès d'un serveur PPP en vue d'une ouverture de connexion sur le réseau.

Après une phase de synchronisation entre le client et le serveur pour le définir l'utilisation du Protocole PPP et PAP, le processus d'authentification se fait en deux étapes :

- ☞ Le client envoie son nom PAP ainsi que son mot de passe en clair.
- ☞ Le serveur qui détient une table de noms d'utilisateurs et de mots de passe vérifie que le mot de passe correspond bien à l'utilisateur et valide ou rejette la connexion.

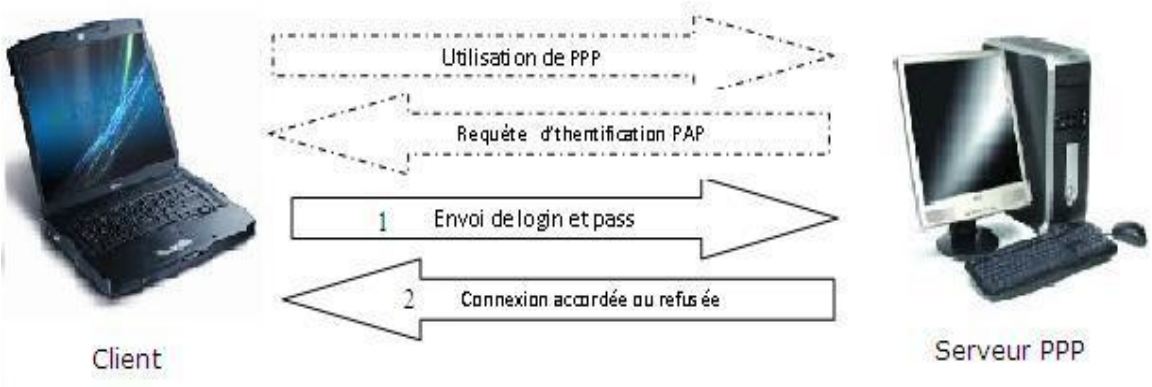

Figure2.1 : Les 2 étapes d'authentification du protocole *PAP*

PAP est le plus simple des Protocoles d'authentification, il est donc très facile à implémenter. Mais étant donné que le mot de passe circule en clair sur le réseau, c'est aussi le moins sécurisé, il est donc fortement déconseillé. D'autre part, même si le mot de passe est crypté, il est toujours possible d'utiliser un sniffer afin de capturer la requête d'authentification et la réutiliser pour s'authentifier, c'est ce qu'on appelle : *attaque par rejeu.*

2.1.2- CHAP

Contrairement au Protocole *PAP*, le Protocole *CHAP* (Challenge Handshake Authentification Protocole) permet une authentification sécurisée par hachage *MD5 (Message Digest 5)*. MD5 et une fonction de hachage cryptographique permettant d'obtenir l'empreinte numérique d'un message à partir de laquelle il est impossible de retrouver le message original. Ainsi, en envoyant l'empreinte du mot de passe au serveur, le client peut montrer qu'il connaît bien le mot de passe sans avoir à réellement l'envoyer sur le réseau.

Après le même type de synchronisation que pour le Protocole PAP, le mécanisme d'authentification est basé sur un CHALLENGE en 3 étapes :

☞ Le serveur envoie au client un nombre aléatoire de 16bits ainsi qu'un compteur incrémenté à chaque envoi.

☞ Le client génère une empreinte MD5 de l'ensemble constitué reçu puis il envoie cette empreinte.

☞ Le serveur calcule également de son coté l'empreinte MD5 grâce au mot de passe du client stocké localement puis il compare son résultat à l'empreinte envoyée par le client. Si les deux empreintes sont identiques, le client est bien identifié et la connexion peut s'effectuer sinon, elle est rejetée.

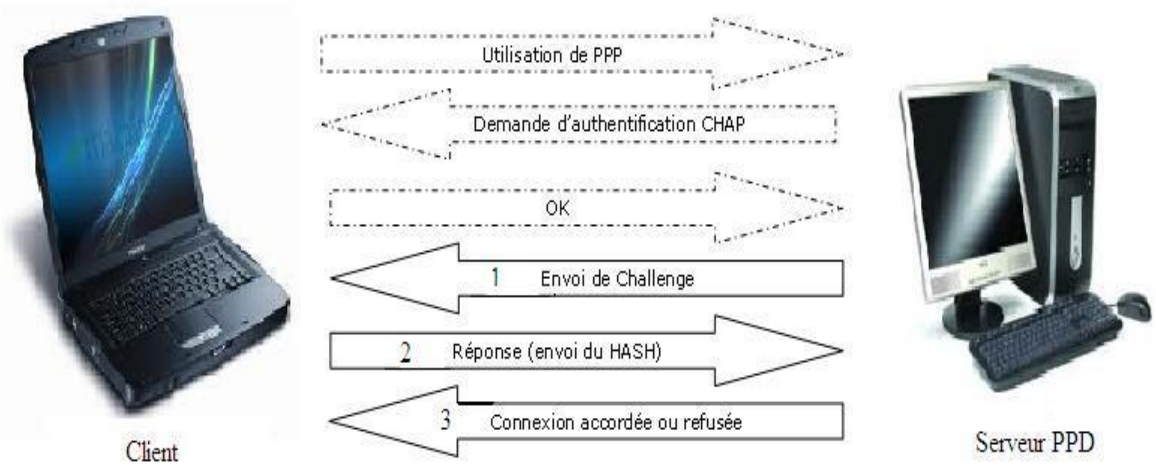

Figure 2.2 : les 3 étapes d'authentification du protocole *CHAP*

Ce mécanisme d'authentification procure à CHAP deux avantages :

Tout d'abord, si la requête d'authentification envoyée par le client est interceptée, elle ne pourra pas être rejouée, en effet chaque empreinte calculée par le client est unique envoi par le serveur.

D'autre part, lors d'une session établie par le Protocole CHAP, le serveur envoie régulièrement des challenges au client de façon à identifier son identité, cette mesure de TACACS supplémentaire permet donc de se prémunir des détournements de session.

2.1.3- MS-CHAP

MS-CHAP (Microsoft Challenge Handshake Authentification Protocol) est la version spécifique de CHAP mise au point par Microsoft. Plus qu'une simple version prioritaire, MS-CHAP apporte également quelques améliorations à CHAP. Un des principaux inconvénients de CHAP est que le serveur doit détenir les mots de passe des utilisateurs en clair pour pouvoir vérifier l'empreinte MD5 envoyée par les clients, ce qui constitue

une vulnérabilité potentielle en cas de compromission du serveur. Pour remédier à cette faiblesse, le Protocole MS-CHAP intègre une fonction de hachage propriétaire permettant de stocker sur le serveur un hash intermédiaire du mot de passe.

Ainsi, en travaillant uniquement avec ce hash intermédiaire au lieu du mot de passe, le client et le serveur peuvent réaliser le même type de procédure que celle du CHAP, ainsi, le mot de passe e clair n'a plus besoin d'être stocké sur le serveur.

Puis malgré l'avancée du Protocole MS-CHAP par rapport à CHAP, Microsoft créa une seconde version su Protocole (MS-CHAP-v2) pour résoudre deux principales faiblesses de MS-CHAP-v1, d'une part le fait que le client ne puisse pas vérifier l'authenticité du serveur sur lequel il veut se connecter et d'autre part que l'algorithme de hachage propriétaire utilisé soit très vulnérable à des attaques par brute-force.

Voici le fonctionnement du processus d'authentification mutuelle fournit par MS-CHAP-v2 :

- ☞ Le serveur d'accès disant envoie une demande de vérification au client contenant une identification de session I et une chaine C1 générée aléatoirement.
- ☞ Le client envoie alors une réponse contenant : son nom d'utilisateur, une chaîne aléatoire C2 et un hash de l'ensemble formé par la chaîne C1, l'identificateur de session I et son mot de passe.
- ☞ Le serveur vérifie la réponse du client et il renvoie une réponse contenant : une chaîne indiquant le succès ou l'échec de l'authentification, et un hash de l'ensemble formé par 3 éléments : la chaîne C2, l'identificateur de session I et son mot de passe.
- ☞ Le client vérifie à son tour la réponse d'authentification et établit la connexion en cas de réussite.

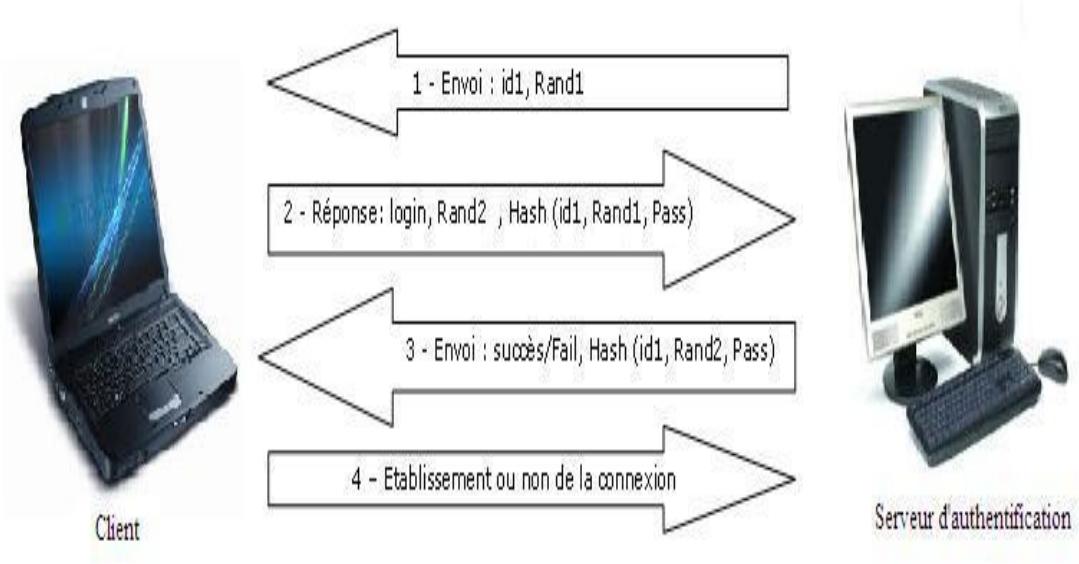

Figure 2.3 : Les étapes d'authentification du protocole *MS-CHAP-v2*

Cette méthode d'authentification est bien mutuelle car elle permet effectivement au client d'être sûr de l'identité du serveur car seul le serveur peut lui renvoyer son mot de passe dans le hash à l'étape 3.

2.1.4- EAP

EAP (Extensible Authentification Protocol) n'est pas directement un mécanisme d'authentification comme le sont PAP ou CHAP, il s'agit en réalité d'une extension du Protocole PPP qui a permis d'universaliser et de simplifier l'utilisation des différents Protocoles dans le cadre des réseaux sans fils et les liaisons Point-A-Point. EAP contient une douzaine de méthodes d'authentification, les plus utilisées étant EAP-MD5, EAP-TLS, EAP-TTLS, LEAP ou encore EAP-AKA pour l'UMTS.

Il faut distinguer des types de trafics EAP : celui entre le client et le point d'accès : EAP over LAN (utilisant un média 802.11a, b ou g) et celui entre le point d'accès et le serveur d'authentification : EAP over RADIUS.

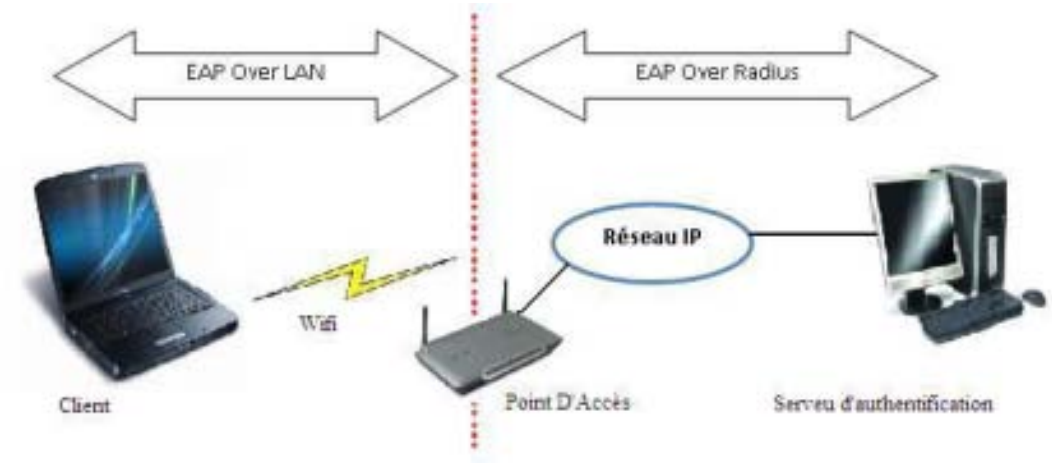

Figure 2.4 : Différents types de trafic *EAP*

2.2- SERVICES D'AUTHENTIFICATION APPLICATIFS

2.2.1 – RADIUS

RADIUS ou *Remote Authentication Dial-In User* est une norme de l'IETF (Internet Engineering TASK Force). C'est un Protocole d'authentification standard Client / serveur qui permet de centraliser les données d'authentification : Les politiques d'autorisations et de droits d'accès, traçabilité. Ce processus doit être relié à une source d'informations, qui est souvent un annuaire LDAP.

Auparavant, les noms et les mots de passe des utilisateurs devaient être dupliqués sur chaque serveur pouvant être accédé à distance (par un modem RTC par exemple).

L'arrivé de RADIUS permit aux fournisseurs d'accès Internet d'authentifier les utilisateurs distants connectés, à partir d'une seule base utilisateurs. Ce Protocole avait particulièrement un sens avant l'ADSL illimité, car il permettait de mesurer le temps précis de connexion des abonnés et facturer en conséquence.

L'identification sur les sites Web peut aussi être gérée par RADIUS. Apache est sans doute le client RADIUS le plus répandu (le module mod_auth_RADIUS permet à Apache de valider une authentification en interrogeant un serveur RADIUS).

Aujourd'hui, ce protocole est aussi souvent utilisé pour les connexions à Internet sans fils (WLAN - avec le Protocole 802.1X qui assure l'identification par port pour l'accès à un réseau). On le retrouve aussi au sein de la téléphonie sur IP comme outil de gestion des connexions, autour du Protocole SIP notamment. Dans ce cas, l'annuaire SIP chargé de l'authentification communique avec le serveur RADIUS en utilisant ce Protocole.

Son fonctionnement est décrit par la figure suivante :

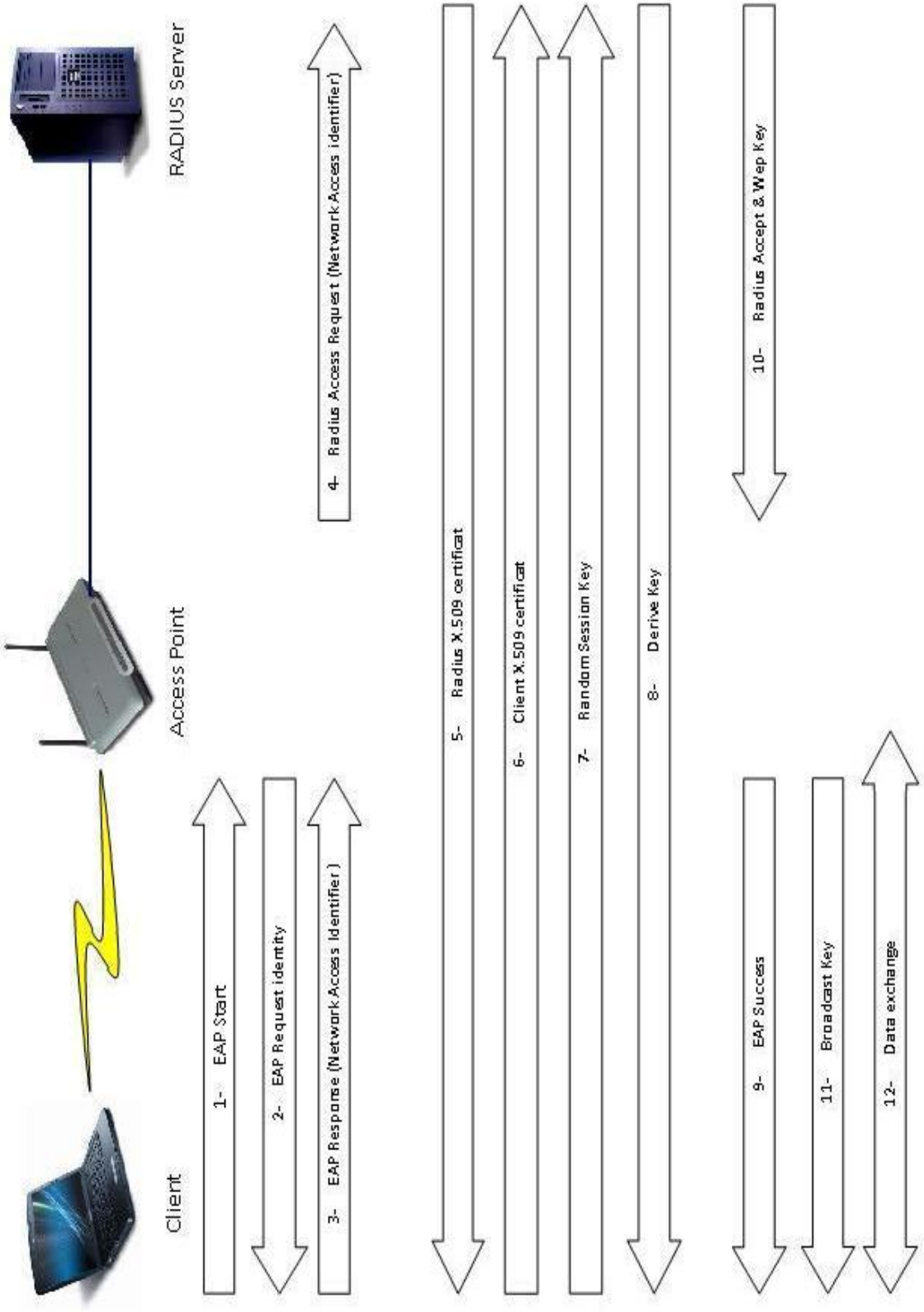

Figure 2.3 : RADIUS : EAP-TLS

Nous expliquons les étapes symbolisées sur le schéma comme suit :

1) EAP START : le client, associé physiquement au point d'accès, envoie un message EAP START : c'est sa démarche d'accès directe en tapant une adresse sur un navigateur web.

2) EAP REQUEST identity : comme réponse, le point d'accès demande au client de s'identifier, il envoi au client une requête d'authentification.

3) Le client répond alors à cette demande d'identité qui lui est attribuée par le point d'accès, par son identifiant, en tapant son nom d'utilisateur et son mot de passe (login).

4) Puis, le point d'accès transmet la requête EAP (repose) dans une demande s'accès RADIUS : le même message du client vers le point d'accès est transféré du point d'accès vers le serveur RADIUS.

5) Ainsi, le serveur initie le processus d'authentification et envoie son certificat qui confirme l'appartenance du client au groupe identifié.

6) La station vérifie le certificat du serveur RADIUS et lui envoie on certificat.

Le client génère une valeur aléatoire, puis l'émet au serveur RADIUS en la chiffrant avec la clé.

7) Le point d'accès envoie la clé de broadcast avec la clé Wep du RADIUS.

8) Maintenant, il y aura des échanges de données publiques du serveur RADIUS.

9) Le serveur RADIUS construit à partir de la valeur aléatoire une clé Wep qui est envoyée.

10) Le serveur RADIUS envoie un message RADIUS « ACCEPT » ou « refuse » ou « CHALLENGE » au point d'accès.

11) Le point d'accès envoie un message EAP SUCCESS.

12) Echange de données.

Le Protocole RADIUS présente néanmoins certaines limites :

☞ Il a été conçu au départ pour des identifications sur des liaisons lentes et peu sûres. Le choix du Protocole UDP (port 1812) conduit à des échanges laborieux basés sur des temporisations de réémission et des échanges d'accusé de réception.

☞ Sécurité relative reposant sur le secret partagé. Certaines implémentations lentes limitent en plus sa taille.

☞ Chiffrement de l'attribut User-Password par une fonction de hachage MD5, plutôt réservé pour des opérations de signature.

☞ Le rejeu des réponses du serveur possible.

☞ PAS de mécanisme d'identification du serveur. Il est ainsi possible de se faire passer pour un serveur RADIUS et de récolter les noms et mots de passe des utilisateurs.

☞ Les normes qui compètent le Protocole RADIUS sont les Protocoles d'authentification PAP, CHAP ou EAP.

☞ Microsoft : le service d'authentification IAS pour Windows Serveur 2000/2003, et NPS (Network Policy Server) pour Windows Server Vista.

☞ Communauté du libre : Open RADIUS et Free RADIUS.

☞ IAS (Internet Authentification Service) est le service d'authentification Internet sur Windows 2000 (Serveur IAS) et Windows Server 2003 (serveur IAS). C'est une implémentation Microsoft du serveur RADIUS : Le service IAS joue le rôle du serveur RADIUS. Il effectue une authentification, une autorisation et une gestion des comptes centralisés des connexions pour de nombreux types d'accès réseau (accès sans fils, accès par commutateur d'authentification, accès par connexion à distance et VPN). En tant que proxy RADIUS, le service IAS peut envoyer les messages d'authentification et de gestion de comptes à d'autres serveurs RADIUS.

NPS (Network Policy Server) est l'implémentation d'un serveur et proxy RADIUS sur Windows Serveur Vista. Il remplace le service

d'authentification Internet (IAS) de Windows Server 2003. Cette nouvelle implémentation effectue toutes les fonctions déjà présentes sans fils et pour les connexions basées sur 802.1X.

De plus, NPS effectue une évaluation du bon fonctionnement du réseau et réserve un accès limité ou illimité pour les clients NAP.

NAP (Network Access TACACS) est une nouvelle TACACS de l'accès réseau dans Windows Server Vista. Il offre de nouvelles possibilités au niveau stratégie de sécurité : Par exemple il peut demander que les entités du réseau possèdent les dernières mises à jour du système d'exploitation et les derniers fichiers de signature antivirus. En fonction de cela, les entités auront plus ou moins de droits sur le réseau. Ces entités sont appelées client NAP. NPS prend en charge aussi l'envoi du trafic RADIUS via IPv6 (RFC 3162).

2.2.2- TACACS+

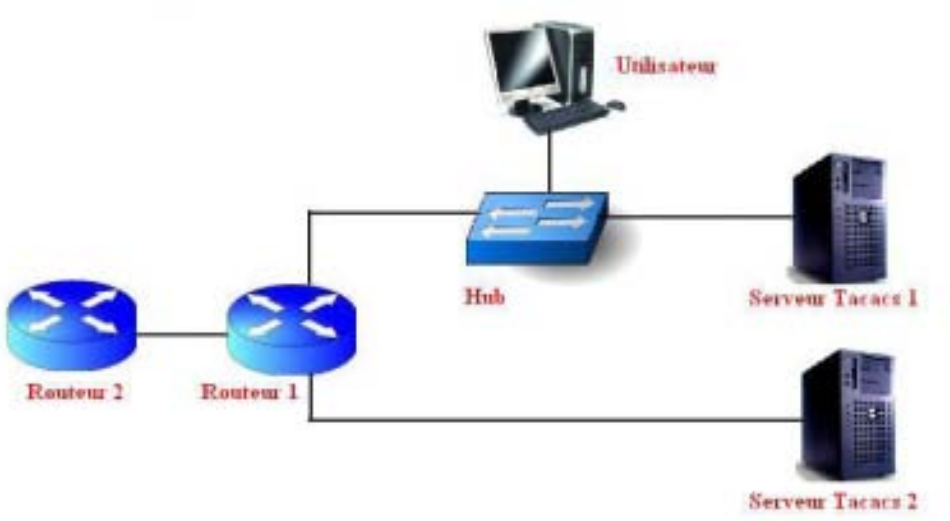

Figure 2.4.1 : Une des architectures supportées par TACACS

Tout comme RADIUS, TACACS+ (Terminal Access Controller Access Control System Plus) est un serveur d'authentification permettant de centraliser les autorisations d'accès dans un réseau. Ce Protocole inventé par CISCO Système a remplacé TCACS et X TACACS mais n'est pas basé sur ceux-ci.

TACACS+ supporte différents types d'architectures, par exemple, si un utilisateur utilise une connexion point à point, c'est le serveur d'accès qui va jouer le rôle de client TACACS+pour interagir avec le serveur.

Figure 2.4.2: Terminal Access Controller Access Control System Plus

En revanche, si l'utilisateur utilise une connexion WiFi, c'est le point d'accès qui va jouer le rôle de client TACACS. D'autres parts, TACACS peut être utilisé pour s'authentifier sur un matériel CISCO, C'est ce dernier qui va interroger le serveur RADIEUS

La particularité de TACACS+ par rapport aux serveurs d'authentification traditionnelle est ça séparation Protocolaire des trois fonctions AAA (Authentication, Authorization, Accounting). En effet, TACACS+permet d'utiliser des technologies différentes, que ce soit pour déterminer l'identité d'une personne, de déterminer ses droits, ou encore de gérer l'enregistrement des logs.

La phase d'authentification peut supporter plusieurs Protocoles comme des technique de type PAP (login – mot de passe) ou encore TACACS+, une session suit toujours le même Protocole : le client envoie une requête START au serveur décrivant le type de session initié, plus initiée, puis, de paires de messages de types REQUEST>REPONSE contenant des paires « attributs-valeur». La RFC ne définit

d'implémentation spécifique pour le stockage des informations relatives aux comptes utilisateur le serveur TACACS+peut aussi bien utiliser des fichiers systèmes (/ etc. / passwd), des bases de données, des cartes à puce ou encore d'autres serveurs d'authentification comme Kerberos.

TACACS+ est donc un serveur d'authentification relativement simple mais il couvre quand même l'ensemble des fonctions AAA et de plus il peut s'intégré à tout type d'infrastructure de part sa liberté d'implémentation.

2.2.3- Kerberos

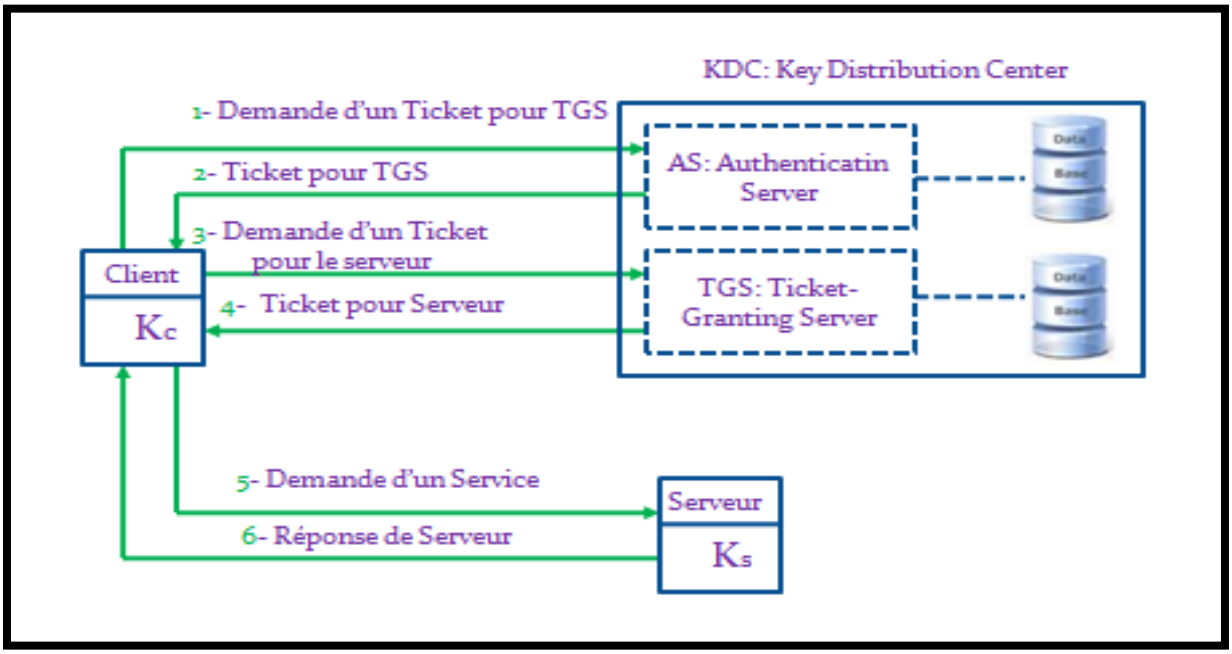

Figure 2.5 : Etapes d'Authentification KERBEROS

Légende de la figure 2.5 :

- Le client a sa propre clé privée Kc.
- Le serveur a sa propre clé privée Ks.
- Le TGS a sa propre clé privée KTGS et connaît la clé privée du serveur Ks.
- L'AS connaît les clés privées du client et de TGS.
- TGS et AS sont deux entités de confiance.

Kerberos est un Protocole d'authentification réseau standardisé par l'IETF. L'objectif de Kerberos est double : sécuriser un échange sur un

réseau non sécurisé et avoir une authentification fiable de l'utilisateur. Il est basé sur deux entités :

☞ Le serveur d'authentification (AS : Authentication Server) qui prend en charge toute la partie authentification pur du client. C'est lui seul qui peut permettre au client de communiquer au TGS (grâce à un ticket d'accès).

☞ Le serveur de distribution de tickets –TGS : Ticket Granting Server) prend en charge les demandes d'accès aux services des clients déjà authentifié. L'ensemble des infrastructures serveur de Kerberos AS et TGS est appelé le centre de distribution de clés (KDC : Key Distribution Center). Ils sont généralement regroupés sur le même serveur.

Dans Kerberos, tous les tiers doivent prouver leur identité : on utilise des mécanismes d'authentification mutuelle. Le Protocole est basé sur des tickets horodatés et chiffrés. Les échanges reposent sur un système de cryptographie (algorithme DES) à base de clés symétriques.

Kerberos partage avec chaque client du réseau une clé secrète faisant office de preuve d'identité.

Le client désire accéder au serveur pour obtenir un service. Ce serveur est représenté dans la figure 2.7 par l'Application Server.

☞ AS_ REQ : le client s'identifie auprès de l'AS à l'aide d'un mot de passe ou d'une carte à puce.

☞ L'AS vérifie dans sa base (par exemple AD) que me client existe. Il génère une clé de session Kc, TGS.

☞ Puis il envoie au client AS_REP :

- Une clé de session Kc, TGS chiffrée avec Kc, qui fera office de mot de passe temporaire pour chiffrer les communications suivantes.
- Un ticket d'accès T1 au service de délivrement de ticket, chiffré avec KTGS (que le client ne peut donc pas chiffrer). Il

contient notamment l'heure de l'opération, sa durée de validité, l'adresse de la machine cliente ainsi que la clé de session Kc, TGS.

☞ TGS_REQ : le client fait une demande de ticket auprès du TGS. Le client lui transmet :

- Le ticket d'accès T1 que l'AS lui avait donné.
- Un identifiant contenant des informations sur le client avec la date d'émission, chiffrées avec la clé de session Kc,TGS.

☞ Le TGS :

- Déchiffre avec se clé, le ticket d'accès T1. Il obtient la clé de session Kc,TGS. Le TGS est maintenant certain que le client a bien obtenu le T1 de l'AS.
- Déchiffre alors les informations que le client avait précédemment chiffrées avec la clé de session. Il vérifie que la durée de la validité est correcte. Puis le TGS_REP qui comprend :
- Un ticket T2 pour accéder au serveur d'application. Il est chiffré avec la clé privé de ce serveur Ks.
- Une seconde clé de session Kc, les communications entre le serveur et le client. Cette clé a été chiffrée avec la clé initiale Kc,TGS.

☞ Le client déchiffre la seconde clé de session Kc,s avec Kc,TGS. Il envoie AP_REQ au serveur d'application deux informations :

- Un nouvel identifiant chiffré avec Kc,s.
- Le ticket d'accès T2.

☞ Le serveur d'application vérifie que le ticket est valide en déchiffrant T2 avec Ks. Il obtient Kc,s. Le serveur peut alors vérifie la

cohérence entre les deux informations. Par exemple il vérifie que la demande est conforme à ce qui est autorisé par le ticket. Une réponse positive ou négative AP_REP est envoyée au client.

Les points forts de Kerberos :

- Le transit des mots de passe sur le réseau est chiffré. Il permet aux utilisateurs de s'authentifier une fois pour toutes lors du login. Ils pourront après utiliser tous les services d'accès à distance sans avoir à fournir à chaque fois leur login et mot de passe. Ils sont en fait toujours authentifiés de manière transparente par Kerberos pour eux.

- Séparation des rôles : l'AS et TGT. C'est la base de Kerberos. Mais dans la réalité, ces deux rôles sont regroupés en une même entité (KDC).

- Impossible de rejouer un échange deux fois de la même manière (grâce au timestamps).

- Les points faibles de Kerberos :

- Le chiffrement symétrique nécessite un partage des clés entre l'AS et le client.

- Les horloges doivent être parfaitement synchronisées : en effet, l'anti-rejeu s'appuie sur le « timestamps ».

- L'authentification mutuelle n'est pas disponible lors du premier échange entre l'AS et le client. Le client ne peut pas certifier que l'AS et bien celui qu'il prétend être.

En revanche, le client peut exiger que le serveur d'application s'authentifie à son tour (lors de la dernière étape). Ce dernier s'exécute en renvoyant la date courante (plus récente que celle du précédent message du client) chiffrée avec Kc,s. Etant donné que seuls le client et le serveur connaissent Kc,s, le client peut raisonnablement penser que c'est bien le serveur qui lui répond.

Kerberos est le mécanisme d'authentification par défaut dans Windows pour vérifier l'identité d'un utilisateur ou d'un ordinateur. Les

rôles de l'AS et TGS sont pris en compte par le contrôleur de domaine, en s'appuyant sur l'annuaire Active Directory.

Suite à cette étude comparative, nous avons préféré d'essayer RADIUS comme protocole, à travers lequel, nous essayerons de mieux sécuriser le réseau sans fil de Sup'Com. C'est ce que nous expliquerons avec plus de détail dans le chapitre suivant, qui montre notre étude de cas.

CHAPITRE 3 : ETUDE DE CAS

3.1- ARCHITECTURE DE LA SOLUTION PROPOSÉE :

Après avoir étudié, et comparé les trois protocoles mentionnés dans le chapitre précédent, à savoir TACACS, KERBEROS et RADIUS, nous avons choisi ce dernier, pour réaliser et atteindre le but principal de notre projet : améliorer le réseau WiFi en garantissant le maximum possible de sécurité.

Pour ce fait, l'établissement d'accueil Sup'Com nous a fourni les équipements nécessaires pour mettre en place un réseau test, il s'agit de :

- 4 ordinateurs de bureaux dans le laboratoire cisco2 avec Windows XP SP3 comme système d'exploitation valable pour le serveur et les clients
- 3 clés USB-WIFI, pour les tester comme des clients WiFi (laptops)
- 1 point d'accès Planet Wap-4000
- Les câbles -paires torsadées- dont nous avons fait des câbles directs (grâce aux pinces et connecteurs RJ45)

3.1.1- Réseau WiFi de Sup'Com :

Sup'Com dispose d'une couverture WiFi, à laquelle les étudiants, les personnels et les visiteurs peuvent avoir accès libre mais sécurisé, plusieurs points d'accès sont disponibles :

- Au niveau des amphis
- Au niveau de l'administration
- Au niveau des labos Cisco
- Au niveau des salles de Conférences

Un accès au réseau WiFi peut être accordé également à des personnes extérieures, provisoirement, lors de l'organisation d'un colloque ou d'un challenge par exemple. De même, une couverture WiFi provisoire peut être mise en place, lors de l'organisation d'un événement.

3.1.2-Pré-requis

Pour se connecter au réseau WiFi, l'utilisateur doit être équipé d'un ordinateur contenant une carte WiFi, intégrée pour les générations actuelles des ordinateurs, en ajoutant une carte PCMCIA si le WiFi n'est pas intégré, ou simplement en branchant une clé WiFi à son poste.

3.1.3- Actions

- Se connecter au réseau sans fils portant le nom du point d'accès le plus proche
- Lancer un navigateur
- S'authentifier sur la fenêtre de connexion qui apparaît

3.1.4- Utilisations possibles ?

- Navigation web et consultation de la messagerie électronique
- Mise à jour du système d'exploitation dont le client dispose
- Transfert de fichiers (selon les droits autorisés)

3.2- DESCRIPTION DU RÉSEAU DE TEST :

3.2.1- Configuration du point d'accès WiFi :

Nous avons alors mis en place ce réseau WiFi -minimisé-, en branchant le point d'accès par un câble direct, qui connecte le point d'accès à une prise RJ45 du laboratoire, ou même tout en étant branché directement au Switch de ce labo.

Pour configurer ce point d'accès WiFi, nous devons lui ajouter les paramètres suivants :

- SSID ou ESSID : c'est le Service Set IDentifier. En WiFi, c'est un identifiant de 32 caractères, propre à chaque réseau et qui est présent en tête des messages. Le SSID désigne le réseau auquel est attaché le poste.
- Son type d'utilisation, dans notre cas il s'agit d'un point d'accès
- Son nom, nous l'avons nommé WAP-4000 comme ça marque l'indique
- Et bien évidemment son identifiant unique : son adresse mac, qui lui est attribuée par défaut depuis le fournisseur.

La figure suivante nous montre la configuration et le paramétrage de notre point d'accès :

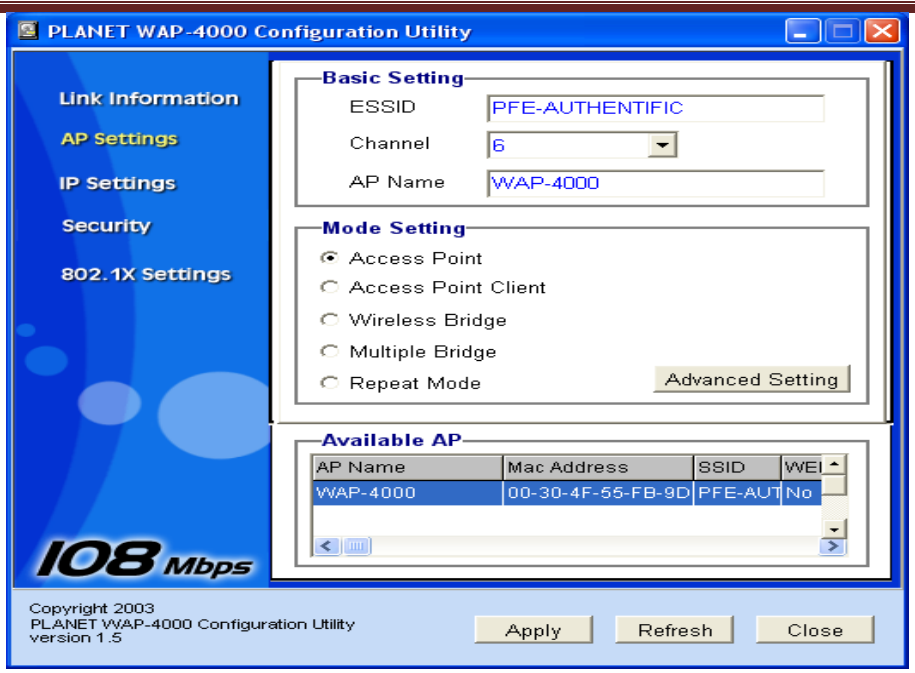

Figure 3.1 : Paramétrage du point d'accès

Puis, nous avons effectué le paramétrage IP, configurant notre point d'accès comme un serveur DHCP, qui attribue les adresses IP aux clients automatiquement, tout en étant limité à une plage d'adresse bien déterminée : 172.16.112.71 jusqu'à 172.16.112.99, et ce pour éviter le conflit d'adresses, puisque la plage 112 est utilisée dans les labos cisco.

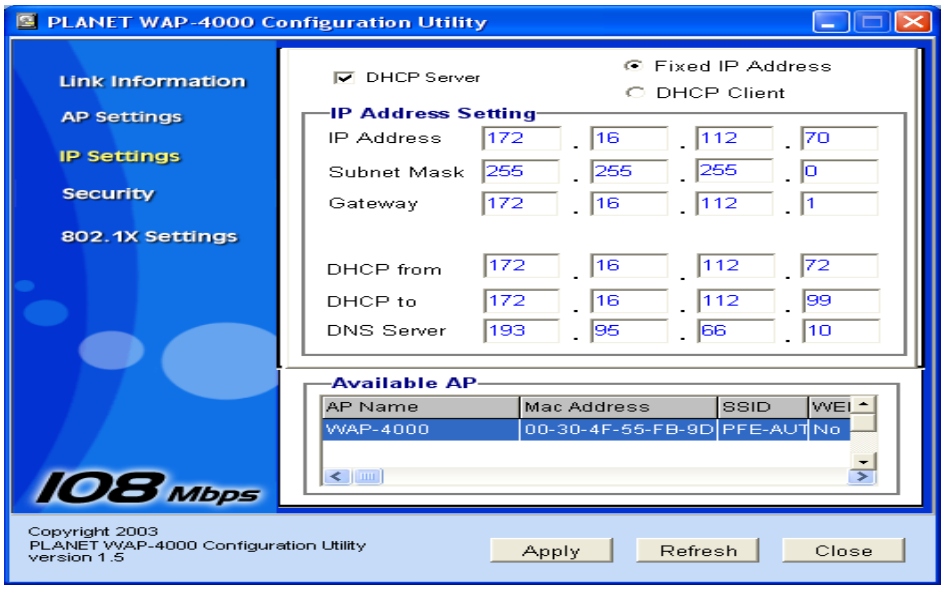

Figure 3.2 : Paramétrage de l'adressage IP

Nous rappelons que les adresses 172.16.112.70 et 172.16.112.71 ne sont pas incluses dans la plage d'adressage DHCP, car elles sont déjà attribuées au point d'accès et au serveur Radius.

Maintenant, nous allons paramétrer le 802.1X : c'est un standard lié à la sécurité des réseaux informatiques, mis au point en 2001 par l'IEEE (famille de la norme IEEE 802), qui permet de contrôler l'accès aux équipements d'infrastructures réseau.

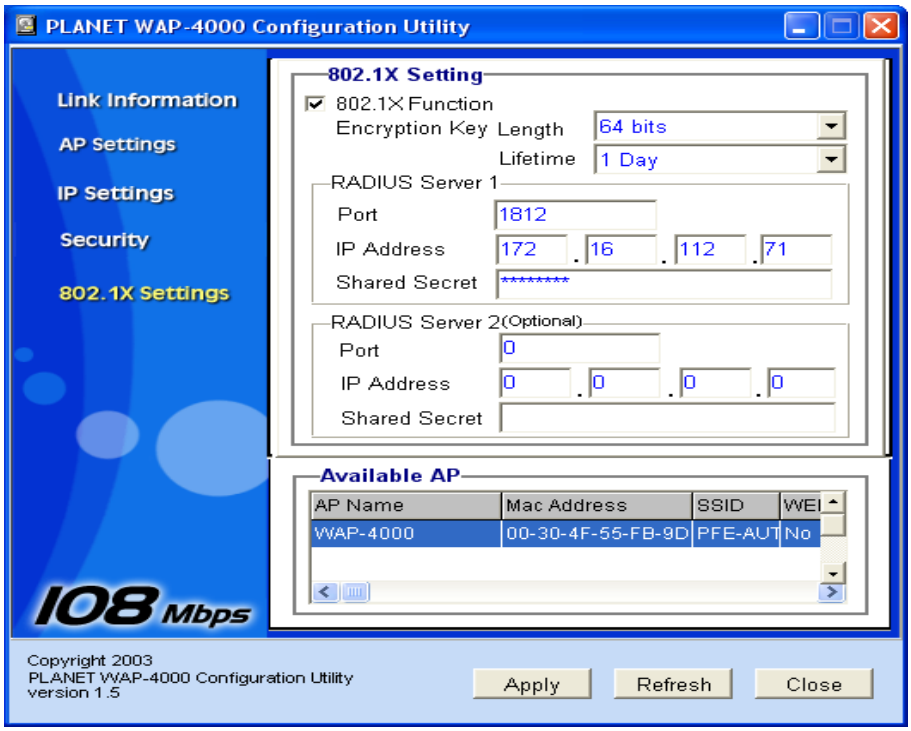

Figure 3.3 : Paramétrage 802.1x

N.B : ce paramétrage ne peut être effectué que si le point d'accès est branché directement au réseau grâce à un câble direct, nous pouvons l'effectuer en utilisant son driver, ou même en utilisant l'adresse IP qui lui est attribuée par défaut de la part du fabriquant, qui est généralement 192.168.1.1, en saisissant cette adresse dans la barre d'adresses du navigateur web. Et dans notre cas, nous avons remplacé 192.168.1.1 par 172.16.112.70 en configurant le point d'accès.

3.2.2- Configuration du serveur Radius :

Parmi les buts principaux de notre projet, nous avons voulu prouver que nous n'avons pas besoin d'un système d'exploitation –serveur- comme Windows 2003 ou 2008 server ou Windows NT, ces versions des systèmes d'exploitation de serveurs, contiennent Radius par défaut dans le dossier système I386, il n'est pas installé automatiquement avec le système d'exploitation, mais peut être ajouté par la suite en activant des fonctionnalités Windows.

Pour utiliser comme serveur un poste contenant Windows XP Sp3 comme OS, nous devons alors ajouter un programme qui nous permettra de le rendre un serveur d'authentification, nous avons alors choisit ClearBox Enterprise Server™ 5.6.

Après l'avoir installé, nous devons configurer notre serveur Radius, au début, nous avons suivi le WIZARD, étape par étape, l'ajout de notre point d'accès comme client se fait ainsi :

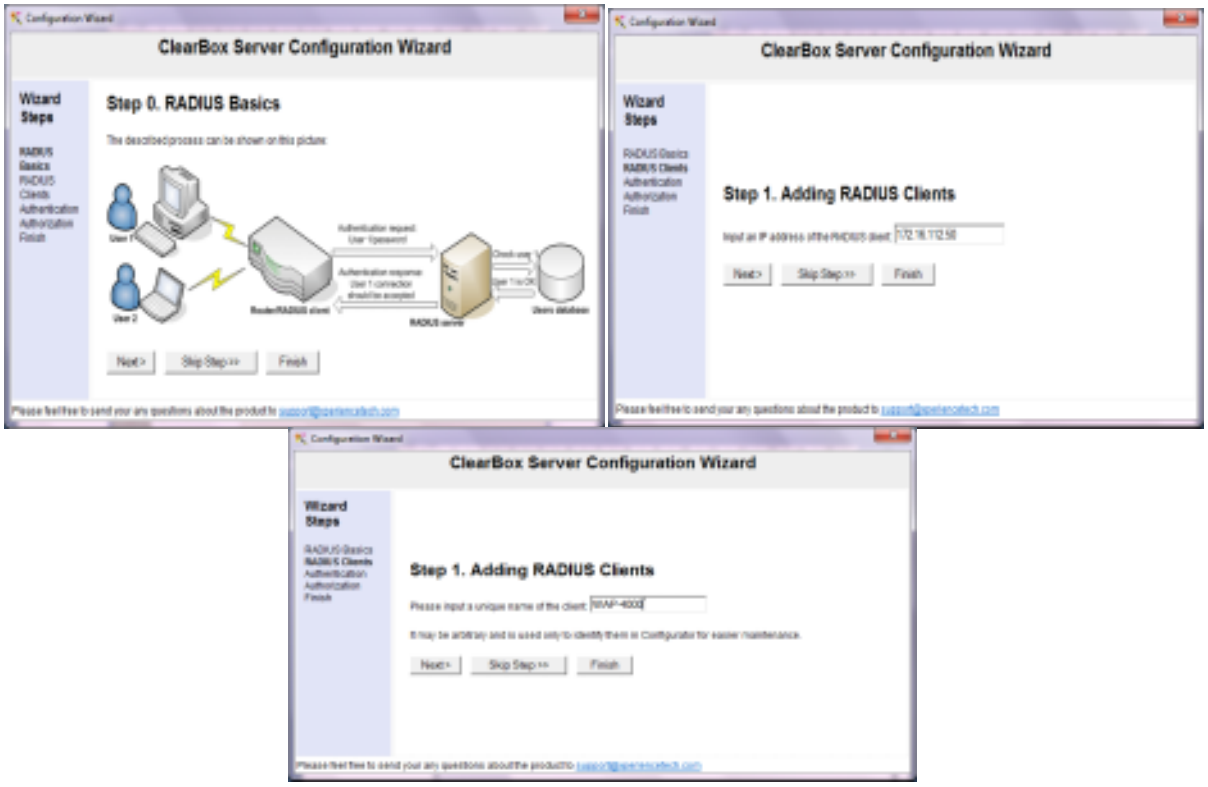

Figure 3.4 : Configuration Radius à travers son Wizard

Mais suite aux nombreuses applications que nous avons effectuées, aux fautes que nous avons appris à ne plus commettre, nous nous sommes habitués à effectuer la configuration et le paramétrage nous même, sans avoir besoin du Wizard ; ainsi, nous sommes passés par les étapes suivantes :

Après avoir fouillé le Help de ClearBox Enterprise Server™ 5.6, nous avons commencé par la configuration du serveur (le poste contenant Windows XP SP3 comme OS), et ce en ajoutant un nouveau client Radius : la boîte de dialogue ci-dessous permet de mettre en place un nouveau client Radius, à travers lequel, les demandes d'authentification seront envoyées au serveur : il s'agit de notre point d'accès WiFi baptisé sous le nom WAP-4000 et ayant comme adresse IP : 172.16.112.70

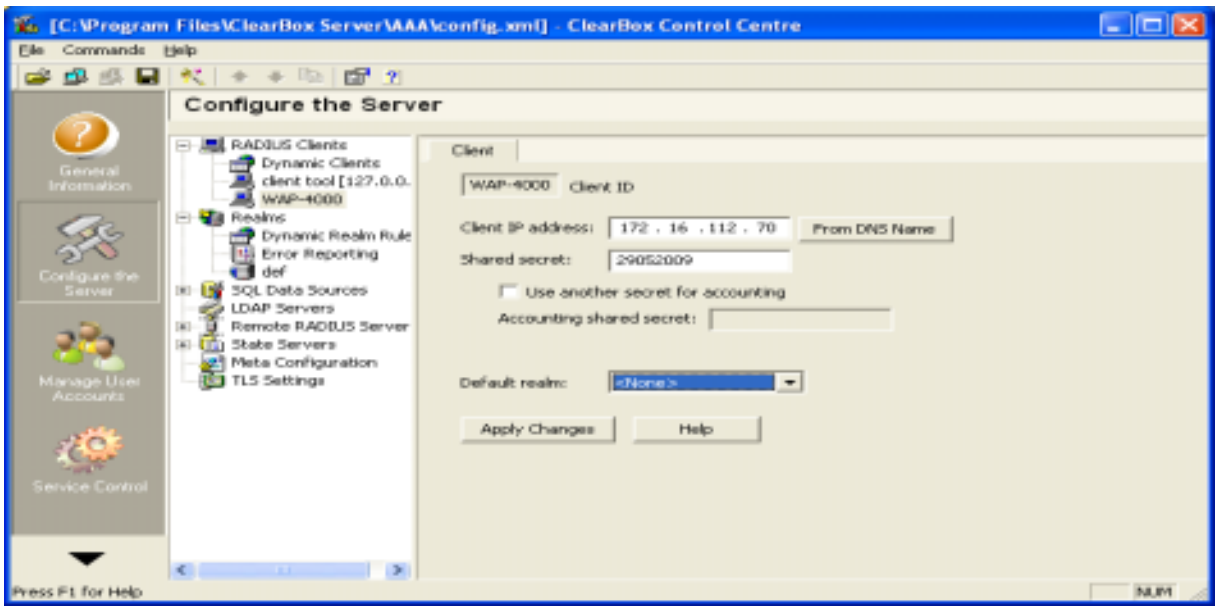

Figure 3.5 : Ajout du point d'accès WiFi sur ClearBox

Puis nous devons sélectionner un certificat, afin de fournir des services de sécurité réseau de confiance aux clients sans fils ; le serveur ClearBox enverra ainsi son certificat numérique obligatoire, sachant que le canal TLS est établi dans tous les protocoles WAP (PEAP, EAP-TLS, etc.) : c'est ce qui est requis pour que l'authentification réussie.

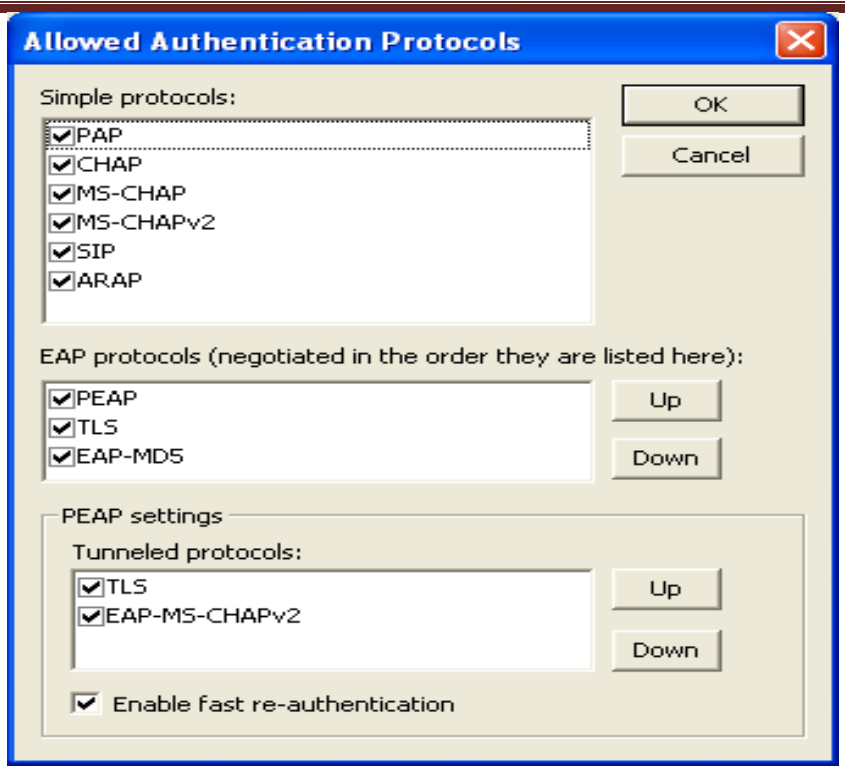

Figure 3.6 : Choix des protocoles d'authentification autorisés

Nous allons maintenant choisir le type de base de données dans laquelle nous allons intégrer pour chaque utilisateur que nous allons authentifier : un user name, un password et l'adresse mac du laptop depuis lequel il va se connecter, et puisque notre cas de test sera limité à un petit nombre d'utilisateurs créé : les 3 clés WiFi que Sup'Com nous a fourni et notre pc portable contenant le WiFi intégré, nous allons reporter donc le choix du type de la base de données que nous allons utiliser, quand nous passerons en cas réel, car nous aurons besoin d'un type de base de données qui supporte un grand nombre d'utilisateurs : les étudiants d'une école supérieure, le personnel, les visiteurs et les utilisateurs temporaires durant des conférences ou des séminaires, en attendant que notre projet voit le jour et entre en vigueur, nous allons choisir Microsoft Access comme type de base de données, dans laquelle nous allons saisir les identifiants uniques des clés WiFi dont nous disposons pour notre projet.

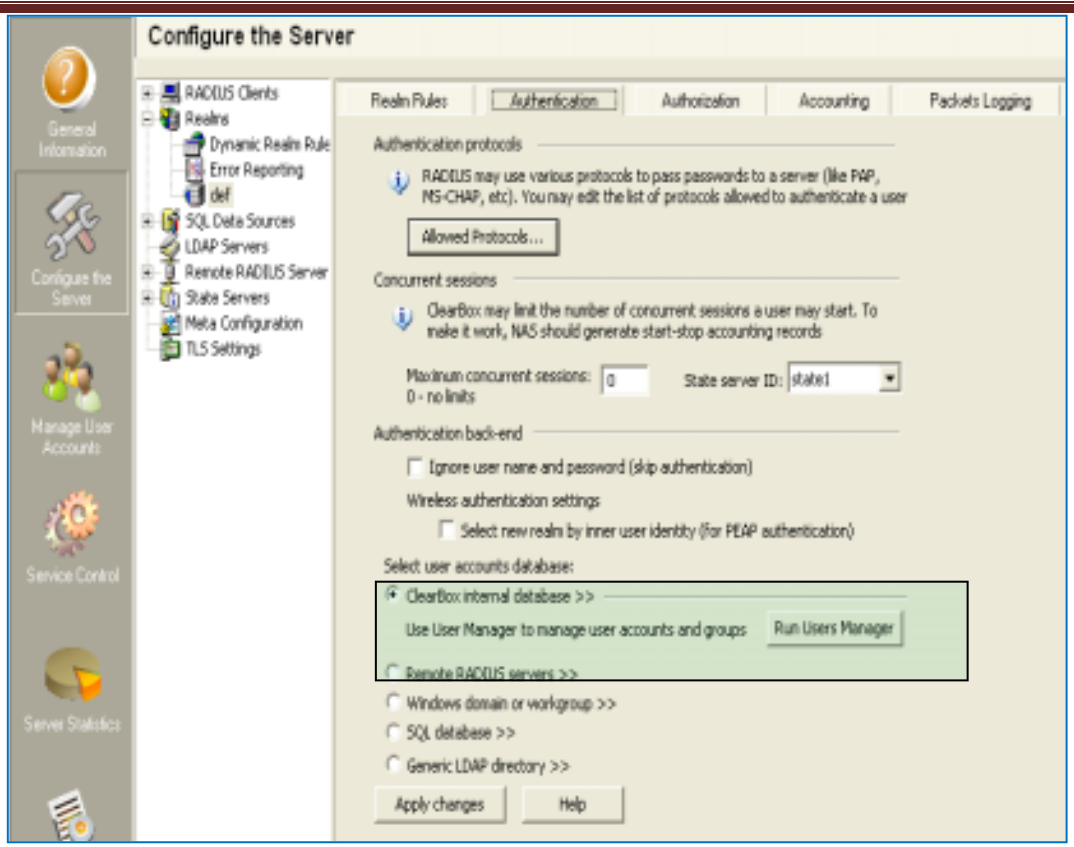

Figure 3.7 Choix du type de base de données

Une fois la base de données créée et enregistrée sur le serveur radius, nous commençons l'ajout des utilisateurs.

Il faut noter que nous pouvons créer plusieurs types d'utilisateurs, selon le degré de liberté dont il bénéficieront, en autorisant des applications et des sites et en bloquant d'autres.

Sur cette liste déjà créée pour deux clés WiFi, nous ajoutons ma carte WiFi intégrée en suivant ces étapes :

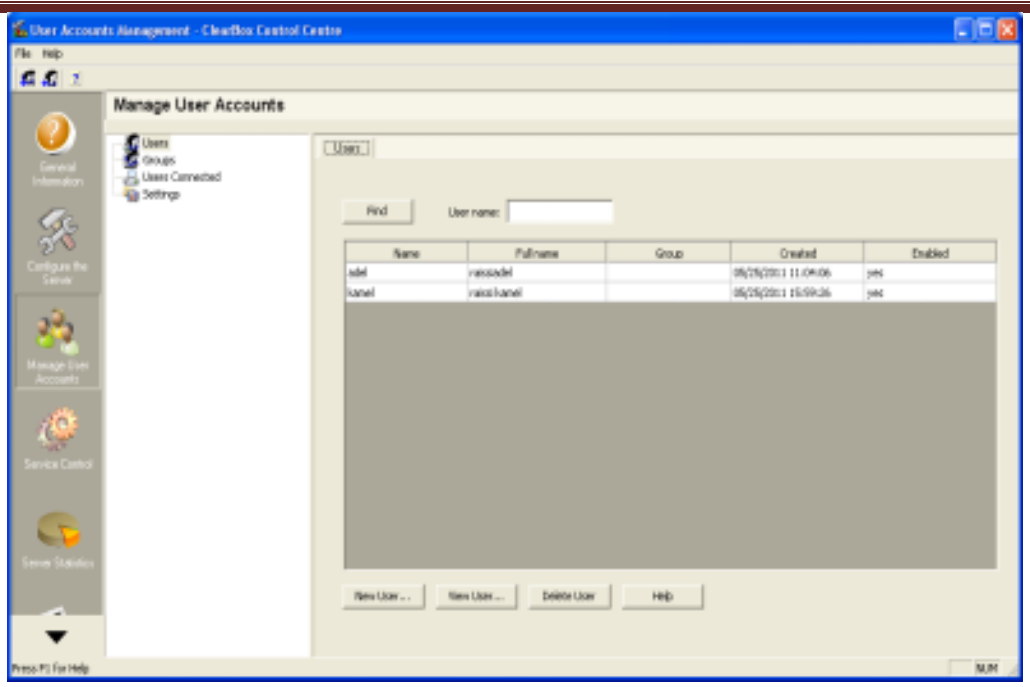

Figure 3.8 liste des adresses mac déjà configurées

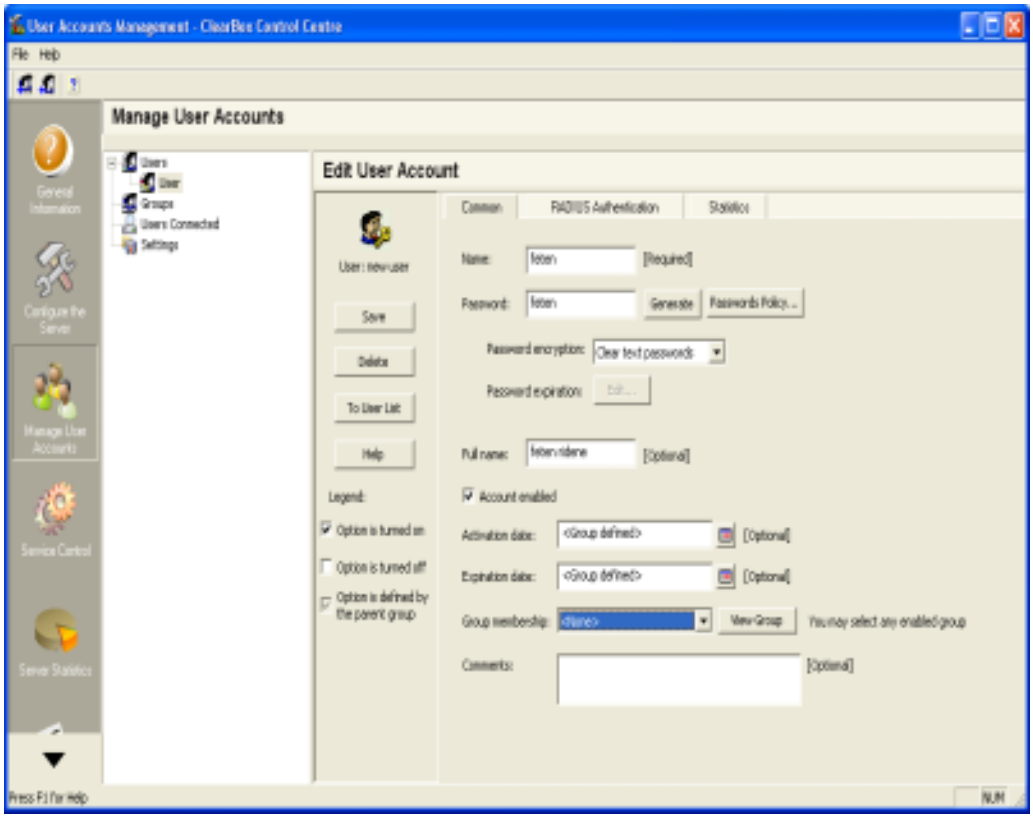

Figure 3.9 ajout d'un nouvel utilisateur

Nous ajoutons d'abord les informations de l'utilisateur, le nom d'utilisateur et le mot de passe que nous lui attribuons, le mot de passe peut être attribué manuellement ou automatiquement (bouton generate).

Nous allons maintenant ajouter l'adresse mac de la carte WiFi à authentifier :

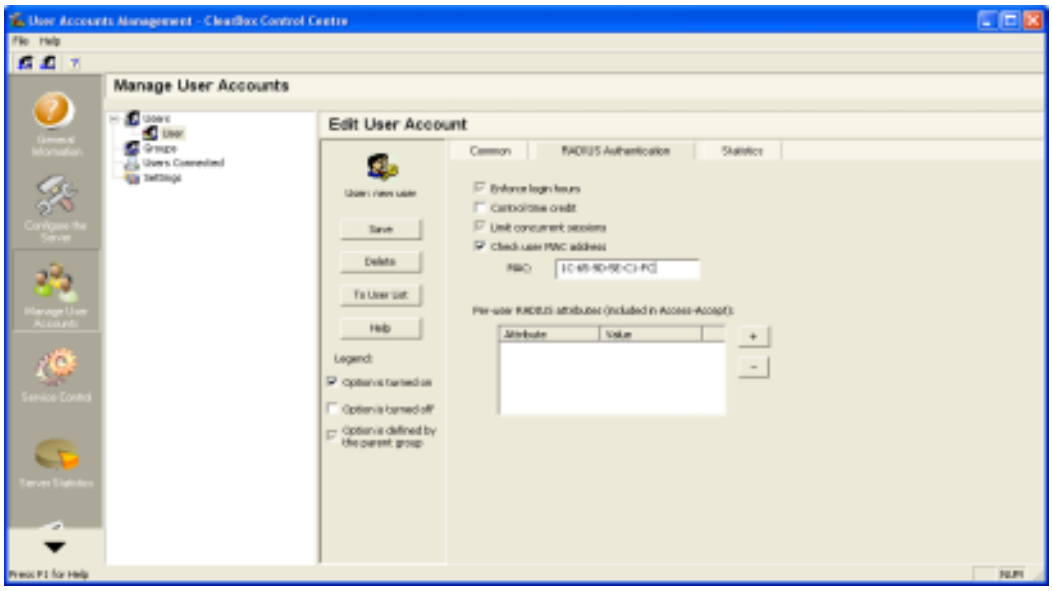

Figure 3.10 : ajout de l'adresse MAC (id unique du client)

Après avoir inséré la liste des utilisateurs, nous allons créer le certificat du serveur :

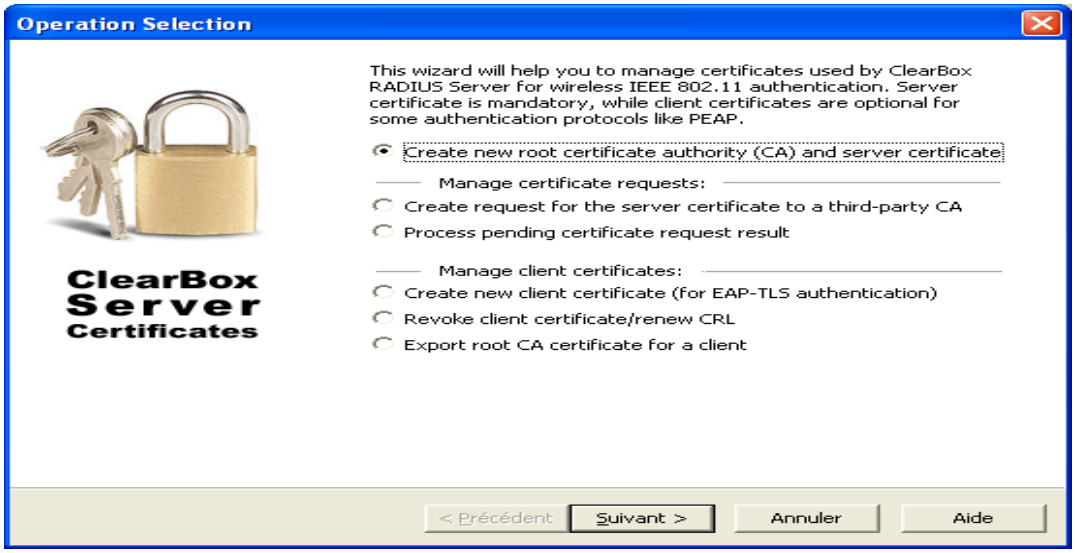

Figure 3.11 : Création du certificat serveur

Nous attribuons alors un nom de domaine à notre serveur : certif.Sup'Com.rnu.tn, un mot de passe qui crypte la clé privée, nous serons appelés à entrer ce mot de passe plutard, le certificat sera donc valide pendant 365 jours ou, une fois expiré, il doit être renouvelé :

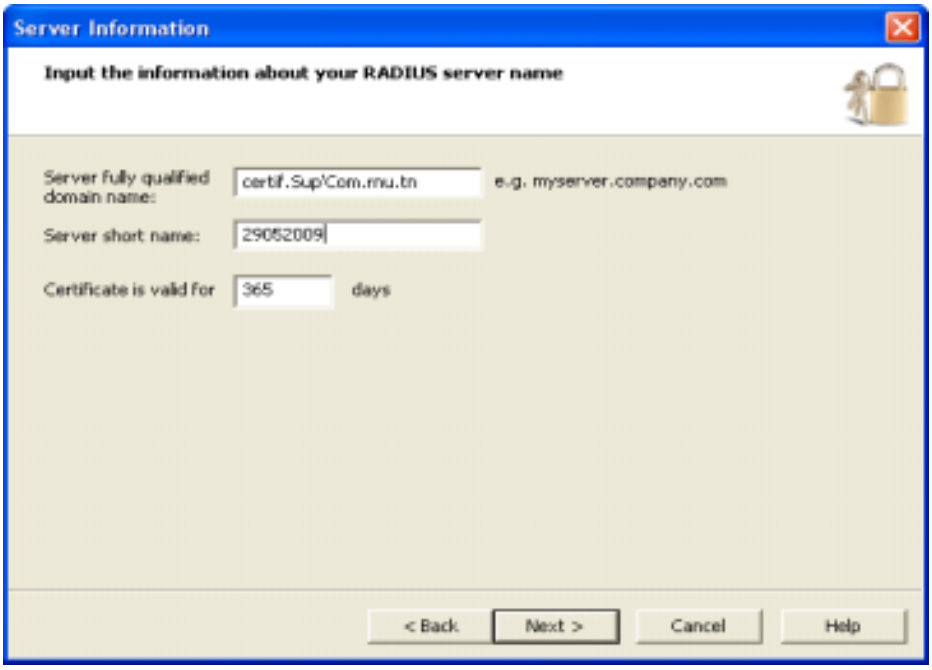

Figure 3.12 : Insertion des informations du serveur

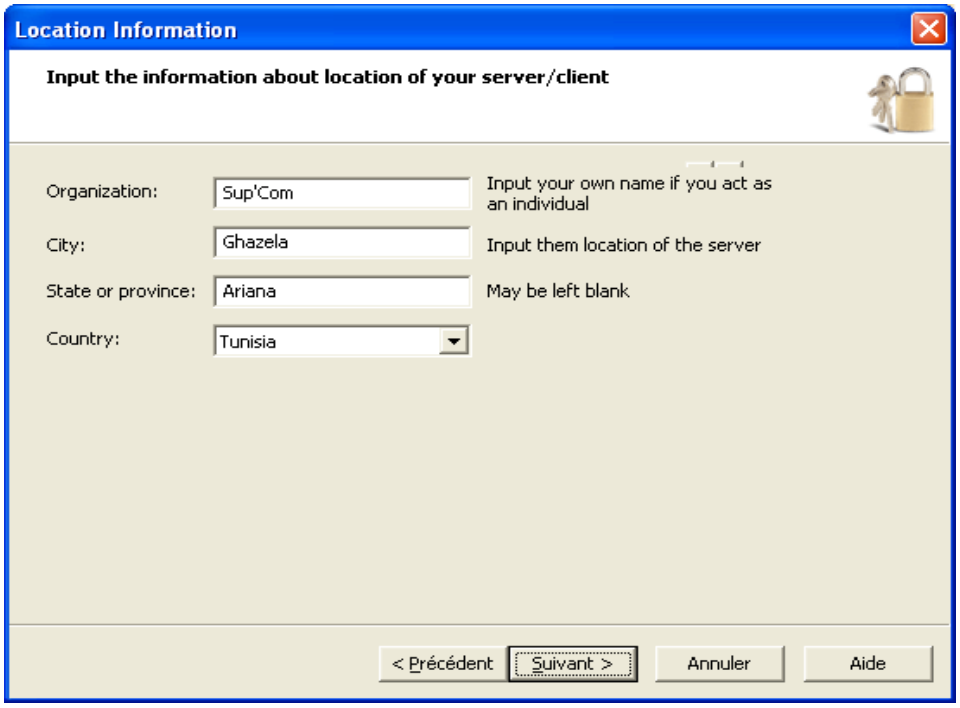

Figure 3.13 : Insertion des informations de localisation du serveur

Nous allons maintenant sauvegarder le certificat :

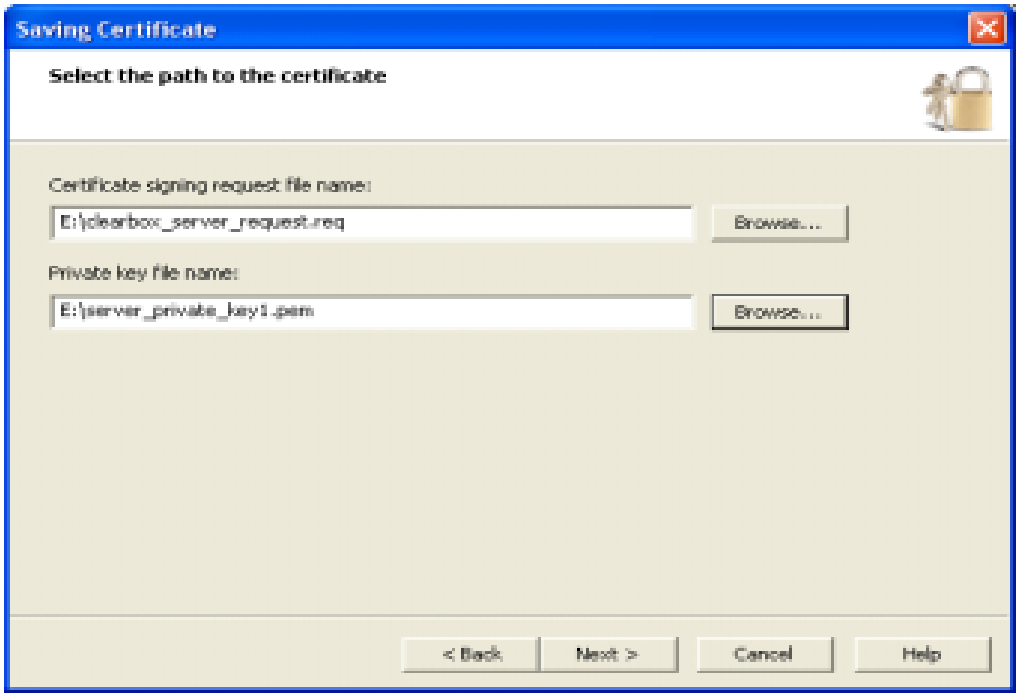

Figure 3.14 : Sauvegarde du certificat

Cela signifie que la racine et les certificats de serveur CA ont été créés avec succès

Figure 3.15 : Succès de création du certificat du serveur

La dernière étape consiste à sélectionner le certificat du serveur dans le configurateur, nous le lançons alors en sélectionnant TLS Server Settings, puis en cliquant sur Select certificate :

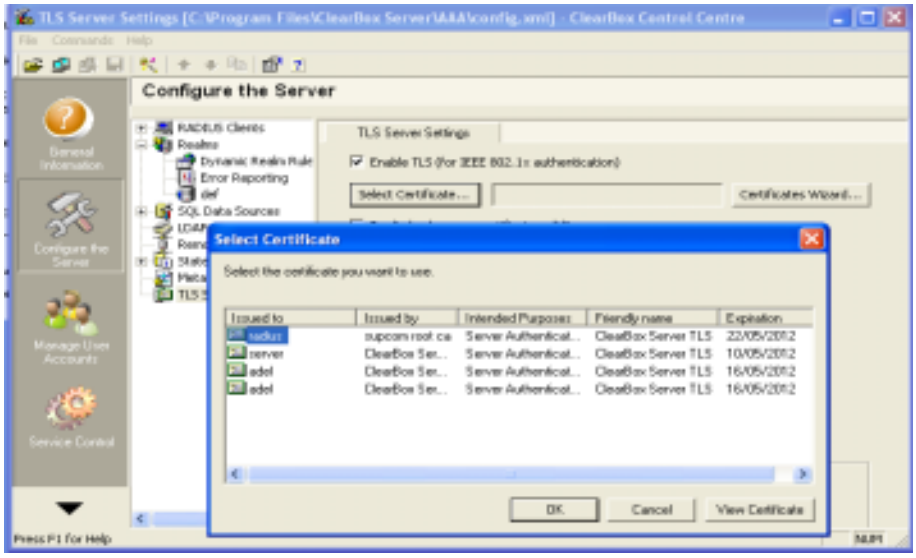

Figure 3.16 Succès de création du certificat du serveur

Nous cliquons alors sur « apply changes », enregistrons les modifications à travers la barre d'outils, et nous redémarrons le service ClearBox.

N.B :nous ne devons jamais supprimer les fichiers de certifications créés, et surtout, nous devons garder ca.pem privé (il vaut mieux limiter les autorisations d'accès, et laisser seulement l'administrateur y accéder).

Afin de fournir des services de sécurité réseau de confiance aux clients sans fils, ClearBox Server doit être en mesure de s'identifier aux clients « cryptographiquement », il leur envoie alors son certificat numérique au cours de leurs tentatives de connexion. Nous allons alors créer une demande de certificat de serveur.

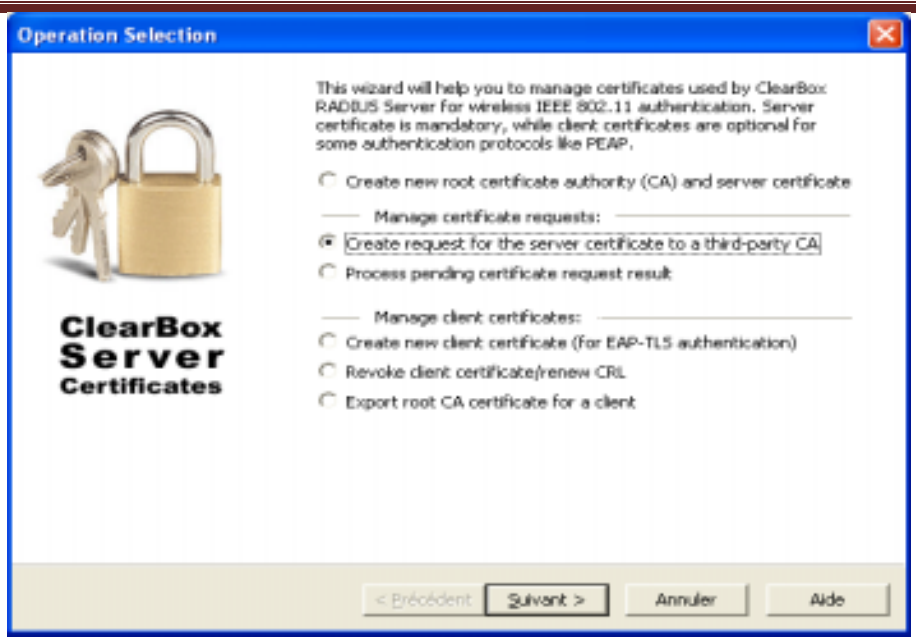

Figure 3.17 : Création de demande de certificat serveur

Après avoir introduit les informations relatives au serveur, nous allons enregistrer la demande de signature de certificat ainsi que la clé privée :

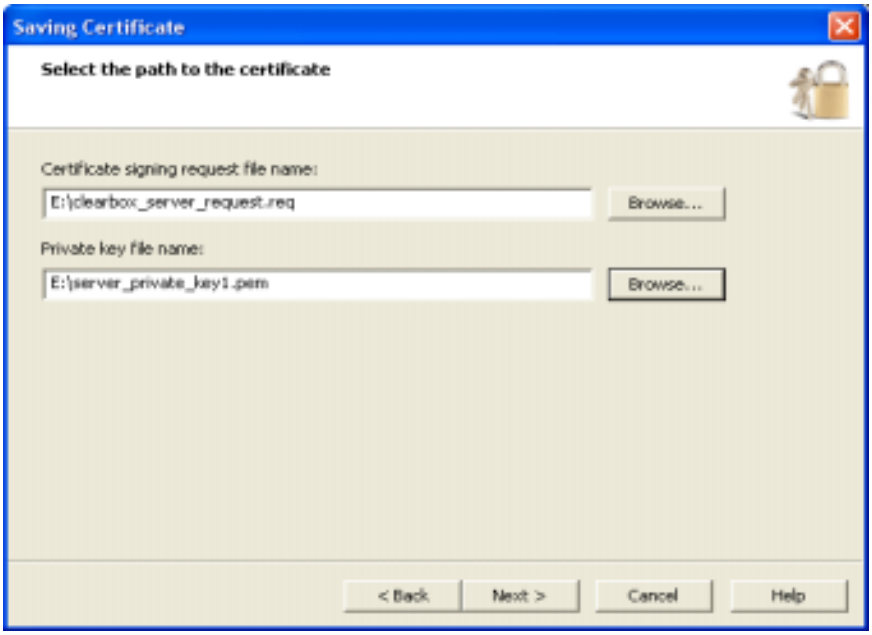

Figure 3.18 : enregistrement de demande de signature du certificat

Le succès de l'enregistrement du certificat sera confirmé, et nous devrons, une fois que ce certificat est reçu, l'installer aussi bien que la clé privée dans la machine client.

Figure 3.19 : Succès de l'enregistrement de la demande de signature du certificat

Après avoir créé le certificat, nous allons procéder à l'installer, nous relançons alors le gestionnaire des certificats, et sélectionnons la troisième étape :

Figure 3.20 : 3ème étape de certification

Nous allons alors spécifier la localisation des deux fichiers : le certificat et la clé privée qui ont été enregistrés précédemment, en y ajoutant le mot de passe de la clé privée que nous avons déjà attribué

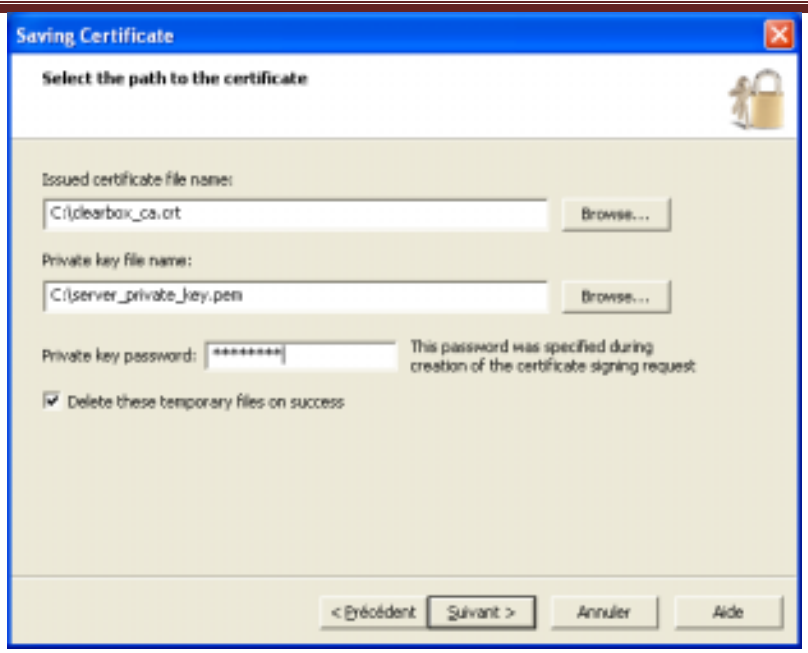

Figure 3.21 : Sélection du chemin du certificat et de la clé

En cliquant alors sur le bouton 'suivant', nous allons trouver que le certificat du serveur Radius est bien installé et prêt à l'emploi.

Maintenant, nous allons créer le certificat client : certains protocoles d'authentification, comme EAP-TLS, exigent que l'utilisateur doive présenter son certificat numérique à un serveur d'authentification pour s'identifier. Cela conduit à la nécessité d'une infrastructure à clé publique qui exige un certificat numérique pour le seul serveur. Quoi qu'il en soit, si nous prévoyons d'utiliser EAP-TLS, un certificat client peut être obtenu auprès des autorités de certifications existantes. Pourtant nous avons créé notre propre autorité de certification et avons émis le certificat du serveur nous-mêmes.

Nous relançons alors l'assistant de certificats et sélectionnons la 4ème option :

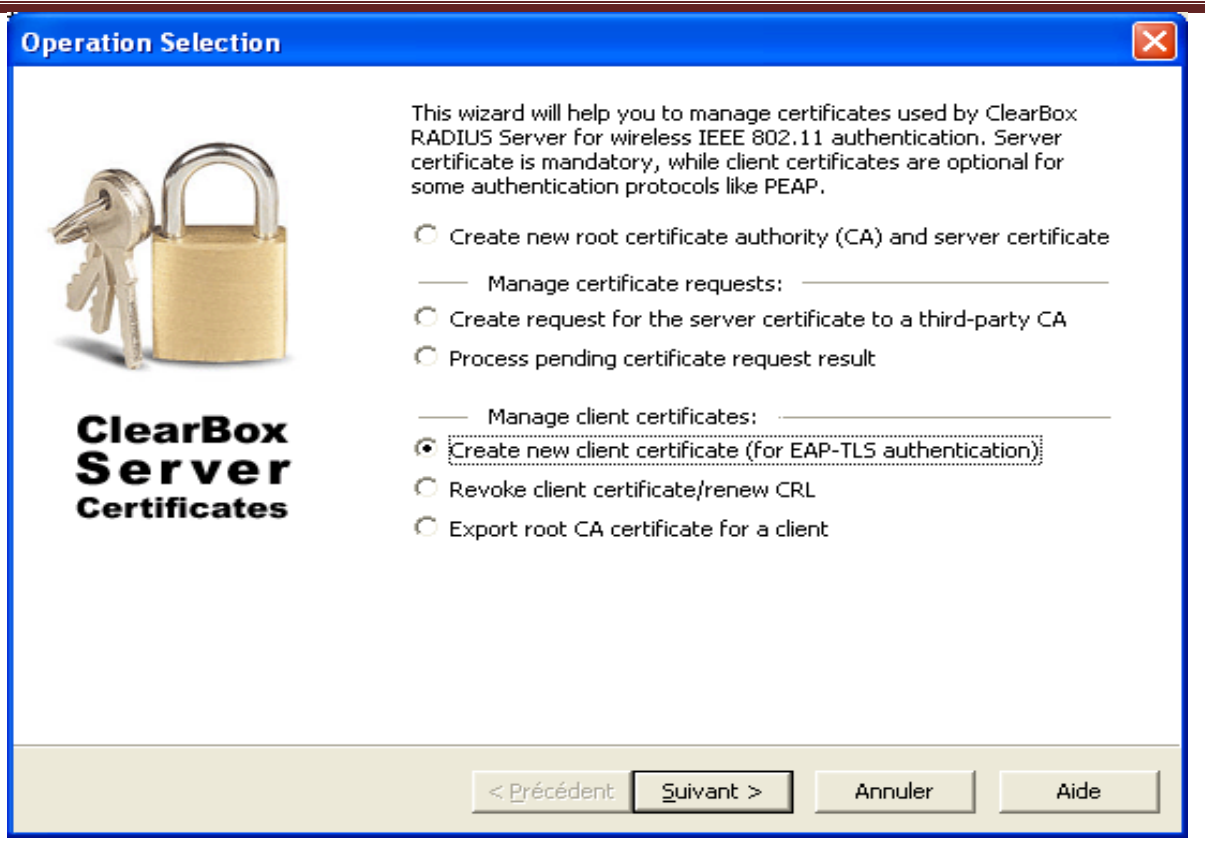

Figure 3.22 : création de certificat client

Et en spécifiant le mot de passe du certificat d'authentification racine, nous allons commencer à introduire les informations personnelles du client, son mot de passe, son adresse mail, un mot de passe et un délai de validité du certificat attribué : ça peut être 3ans (durée d'études à Sup'Com), un an seulement, si nous voulons renouveler les certificats par année universitaire, ou une durée de droit d'accès temporaire pour le visiteur (variant entre 1 et 30 jours).

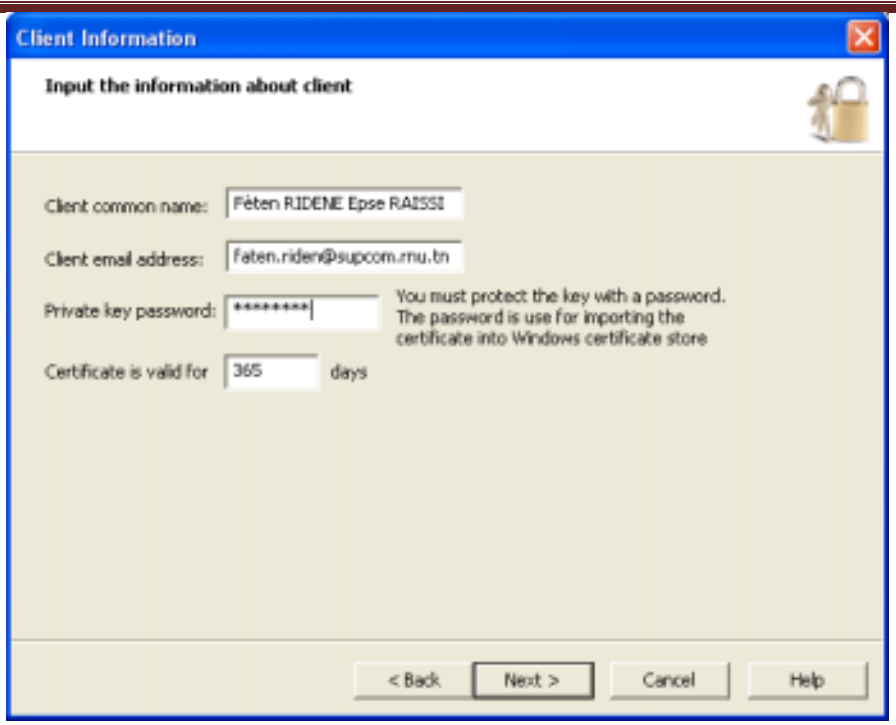

Figure 3.23 : insertion des informations du client

Puis nous indiquons le chemin où ce certificat sera enregistré

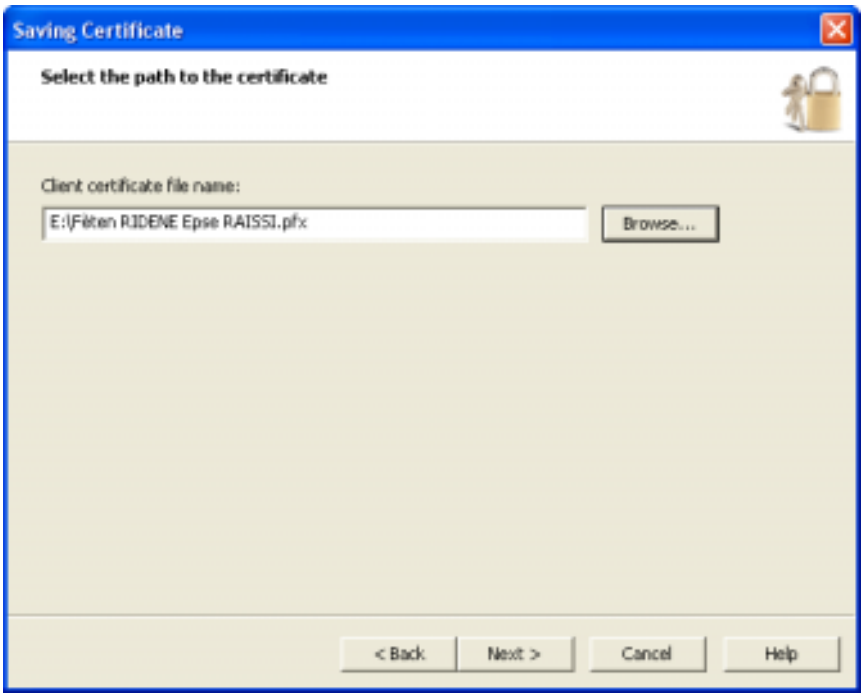

Figure 3.24 : enregistrement du certificat client

Nous portons par la suite cette clé sur un périphérique de stockage, et l'installons sur le poste du client, ce serait effectué pour chaque client, après l'avoir créé dans la base de données clients, et ce en suivant ces étapes :

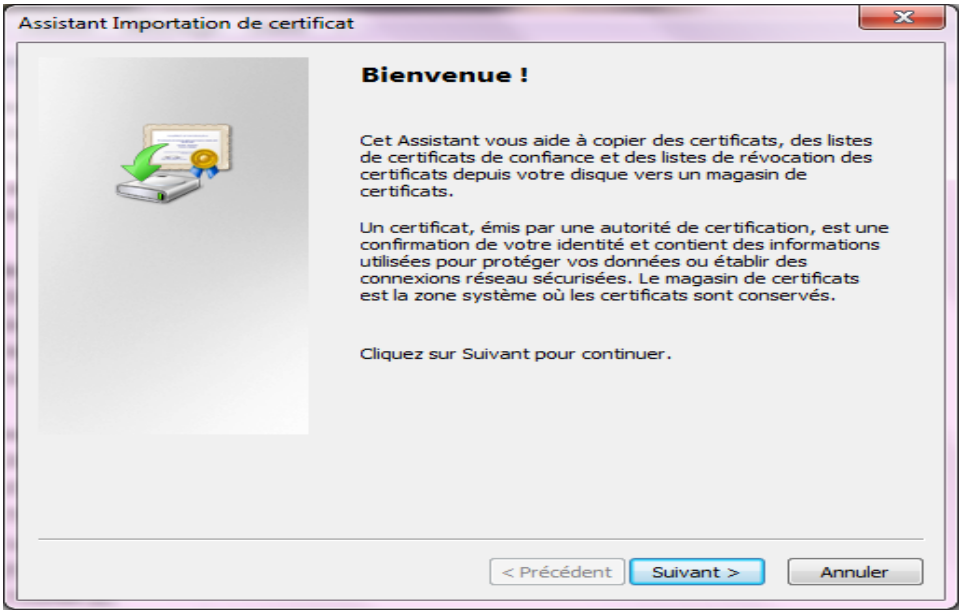

Figure 3.25.1 : Etapes d'importation du certificat sur chaque poste client

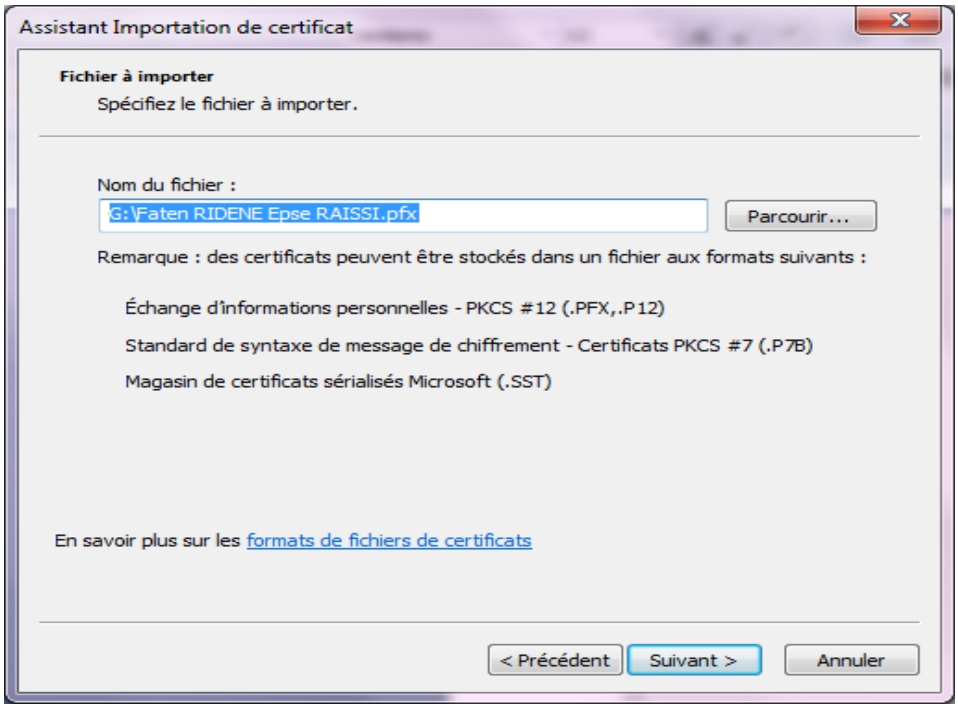

Figure 3.25.2 : Etapes d'importation du certificat sur chaque poste client

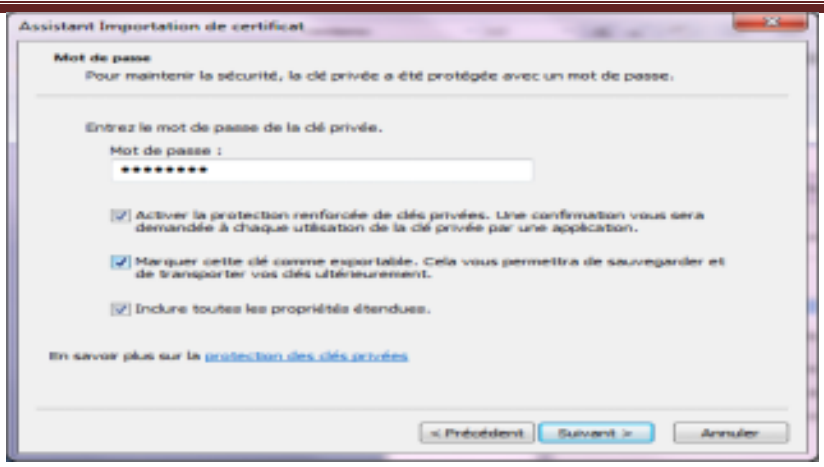

Figure 3.25.3 : Etapes d'importation du certificat sur chaque poste client

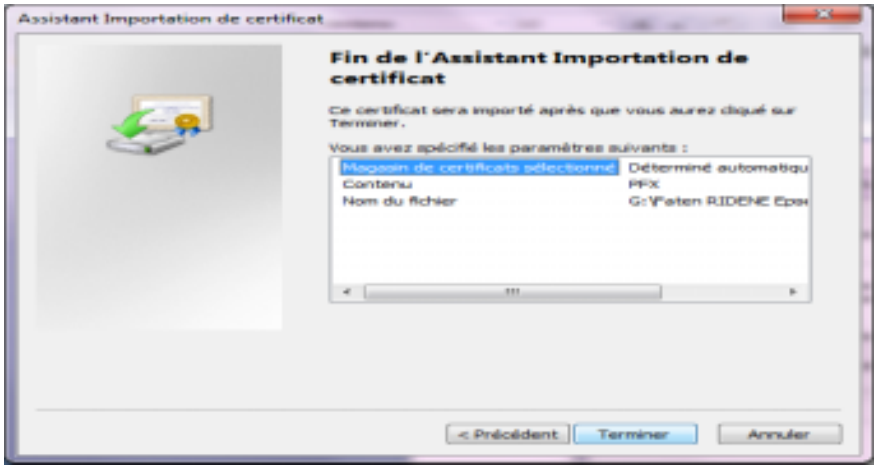

Figure 3.25.4 : Etapes d'importation du certificat sur chaque poste client

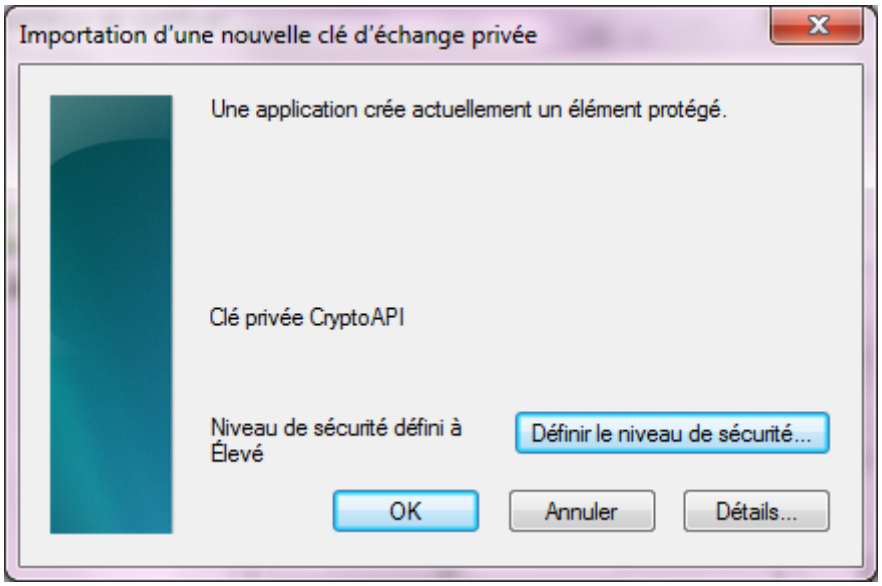

Figure 3.25.5 : Etapes d'importation du certificat sur chaque poste client

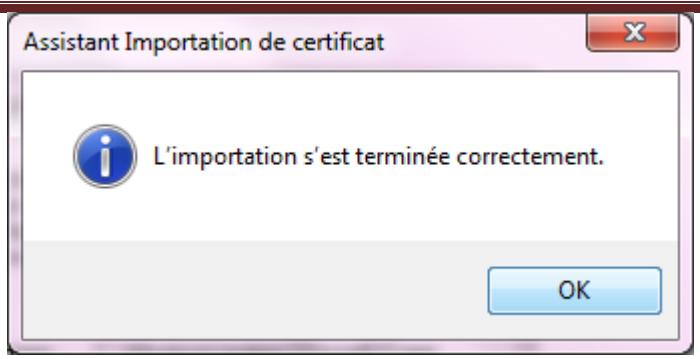

Figure 3.25.6 : Etapes d'importation du certificat sur chaque poste client

Une fois l'importation de la clé est terminée, nous allons tester que la connexion s'effectue bien en authentifiant un client.Nous lançons alors la détection des connexions WiFi disponibles, notre point d'accès est bien détecté, nous l'avons configuré au début en lui attribuant comme nom : PFE-AUTHENTIFIC, pointant par cette abréviation sur le sujet de notre projet de fin d'études.

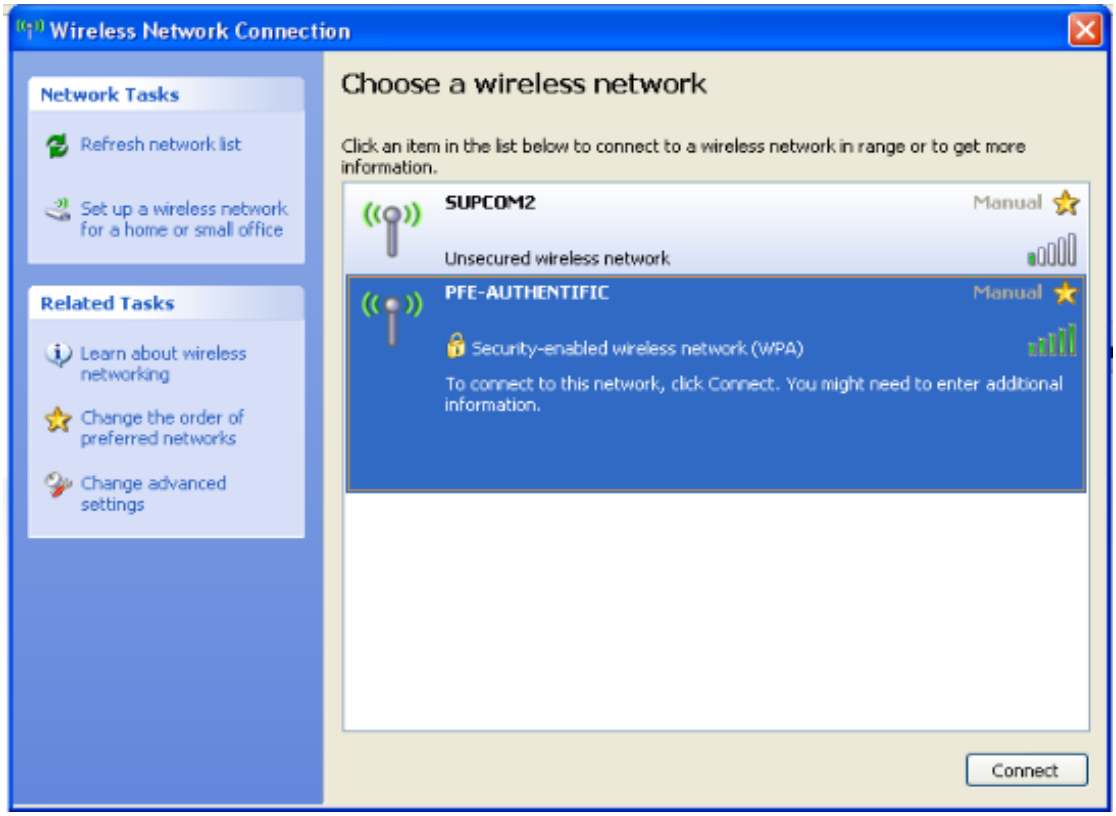

Figure 3.26 : détection de notre point d'accès

Après avoir choisi le point d'accès, on voit apparaître une notification qui confirme qu'il s'agit d'un réseau WiFi parfaitement sécurisé.

Figure 3.27 : notification pour authentification à notre point d'accès

Et en cliquant dessus, une fenêtre dans laquelle nous allons saisir le nom d'utilisateur et le mot de passe du client sans fils apparaitra

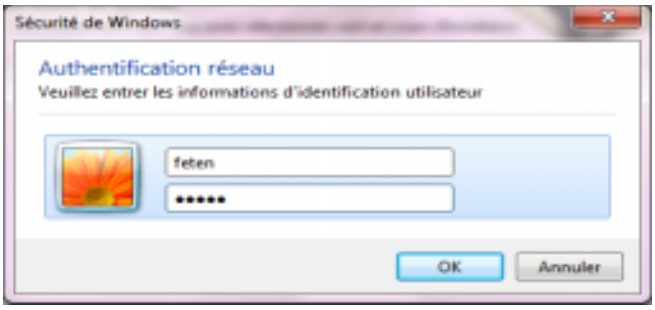

Figure 3.28 : authentification d'un utilisateur

Une fois authentifié après la vérification du serveur, nous sommes bien connectés en sécurité et nous pouvons naviguer sur internet.

Conclusion

Pour proposer un bon mécanisme de sécurité d'un WiFi, comme solution contre les points faibles dont souffre un réseau académique, il nous a fallu penser à une issue qui s'adapte avec l'architecture du réseau existant, tout en tenant compte de la durabilité, l'évolution et la fiabilité de cette solution, assez bien en termes techniques que économiques. Pour cela, nous avons pensé à mettre en place un serveur Radius, pour sécuriser notre petit réseau de test, avant de passer à le mettre en œuvre sur le grand réseau de notre société d'accueil Sup'Com.

Pour entamer ce travail, il nous a fallu faire des recherches, demander l'aide et bien sûr faire des tentatives pour bien comprendre ce mécanisme de sécurité.

Les solutions qui présentent le résultat de nos recherches, exigeaient toujours d'utiliser le protocole Radius sur un système d'exploitation serveur comme le 2003 ou le 2008 server.

Pour prouver notre aptitude, nous avons perpétuellement considéré, le fait d'accomplir des sujets déjà réalisés, comme une application et non pas un projet. Il nous a donc fallu penser à une certaine innovation : il s'agit d'installer un Serveur Radius sur un système d'exploitation client comme Windows XP, en ayant uniquement besoin d'ajouter l'empreinte serveur à travers ClearBox : c'est une application 32-bit écrite en C + +, qui offre la fiabilité et d'excellentes performances sur les plateformes Windows.

Nous avons rencontré plusieurs difficultés pour maîtriser cette application, mais y avoir recherché et travaillé pendant quatre mois, nous a donné l'occasion de bien évoluer nos connaissances et capacités dans le domaine des sécurités réseau, et principalement une forte sécurité sur les réseaux sans fils académiques.

C'est une solution très fiable à nos jours mais ce n'est pas le cas pour toujours, vu la progression très rapide de l'invention des méthodes d'attaque et d'autres méthodes de défonce en informatique : rechercher une solution « transitoire », nous a donc appris que nous devons être à jour avec les progrès du domaine TIC, et c'est ce que nous ferons pour nos prochaines études et recherches.

GLOSSAIRE

A.	
AAA	AUTHENTICATION, AUTHORIZATION, ACCOUNTING
ADSL	ASSYMETRIC DIGITAL SUBSCRIBER LINE
ARAP	APPLE TALK REMOTE ACCESS PROTOCOL
ARP	ADDRESS RESOLUTION PROTOCOL
AS	AUTHENTICATION SERVER
B.	
C.	
CA	CERTIFICATE AUTHORITY
CHAP	CHALLENGE HANDSHAKE AUTHENTICATION PROTOCOL
CSMA/CA	CARRIER SENSE MULTIPLE ACCESS WITH COLLISION AVOIDANCE
D.	
DES	DATA ENCRYPTION STANDARD
DHCP	DYNAMIC HOST CONFIGURATION PROTOCOL
E.	
EAP	EXTENSIBLE AUTHENTICATION PROTOCOL
EAP-AKA	EXTENSIBLE AUTHENTICATION PROTOCOL-AUTHENTICATION AND KEY AGREEMENT
EAP-TLS	EXTENSIBLE AUTHENTICATION PROTOCOL-TRANSPORT LAYER SECURITY
EAP-TTLS	EXTENSIBLE AUTHENTICATION PROTOCOL-TUNNELLED TRANSPORT LAYER SECURITY
F.	
FTP	FILE TRANSFER ¨PROTOCOL
G.	
GPRS	GENERAL PACKET RADIO SERVICE
GPS	GLOBAL POSITIONNING SYSTEM
GSM	GLOBAL SYSTEM MOBILE
H.	
HTTP	HYPERTEXT TRANSFER PROTOCOL
I.	
IAS	INTERNET AUTHENTICATION SERVICE
IEEE	INTERNATIONAL ENGINEERING OF ELECTRONICS AND ELECTRICS
IETF	INTERNET ENGINEERING TASK FORCE
IP	INTERNET PROTOCOL
ISO	INTERNATIONAL ORGANIZATION OF STANDARDISATION
J.	
K.	
KDC	KEY DISTRIBUTION CENTER
L.	
LDAP	LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL
LEAP	LIGHTWEIGHT EXTENSIBLE AUTHENTICATION PROTOCOL
LLS	LINK LAYER SOCKETS

M.	
MAC (adresse)	Media Access Control address
MD5	Message Digest 5
MITM	Man In The Middle
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
N.	
NAS	Network Access Server
NPS	Network Policy Server
O.	
OSI	Open System Interconnection
P.	
PAP	Password Authentication Protocol
PCMCIA	Personal Computer Memory Card International Association
PIN	Personal Identification Number
POP3	Post Office Protocol
PPP	Point to Point Protocol
PPPoE	Point to Point Protocol over Ethernet
Q.	
R.	
RADIUS	Remote Authentification Dial-In User Service
RJ45	Registred Jack (une prise Jack enregistrée)
RTC	Réseau Téléphonique Commité
S.	
SSH	Secure Shell
SSID	Service Set Identifier
T.	
TACACS	Terminal Access Controller Access-Control System
TGS	Ticket Granting Service
U.	
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
V.	
VPN	Virtual Private Network
W.	
WAP	Wireless Access Point
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	WiFi Protected Access
X.	
Y.	
Z.	

WEBOGRAPHIE

http://www.google.tn

http://www.supcom.mincom.tn/

http://fr.wikipedia.org

- http://fr.wikipedia.org/w/index.php?title=Sp%C3%A9cial:Recherche&search=Clear+Enterprise+Server%E2%84%A2+5.6&ns0=1&redirs=0
- http://fr.wikipedia.org/wiki/Remote_Authentication_Dial-In_User_Service
- http://fr.wikipedia.org/wiki/Arp
- http://fr.wikipedia.org/wiki/Man-in-the-middle
- http://fr.wikipedia.org/wiki/RADIUS_(informatique)

http://www.commentcamarche.net

http://www.faqword.com

http://www.google.com/language_tools?hl=fr

http://www.gaudry.be/kerberos.html

http://forum.pcastuces.com

http://raisin.u-bordeaux.fr/IMG/pdf/radius.pdf

http://wareseeker.com/Security-Privacy/clearbox-enterprise-radius-server-5.6.zip/7f2b5c856

http://www.01net.com

http://www.clubic.com/forum/reseaux-WiFi-lan/serveur-radius-sur-windows-7-id777036-page1.html

http://www.cnam.nat.tn/e-cnam/pages/

http://www.commentcamarche.net/contents/authentification/radius.php3

http://www.infos-du-net.com/forum/285970-8-attaque-WiFi

http://www.supcom.mincom.tn/

http://www.xperiencetech.com/radius_manual/realmlogger.html

http://ettercap.sourceforge.net/

http://forums.cnetfrance.fr/topic/166226-probleme-radius-WiFi/

http://freeradius.org/

Depuis ses origines, l'homme a eu besoin de communiquer, et surtout de sécuriser sa communication ; pour cela, il mit au point des codes, des alphabets, des langages… Paroles, gestes de la main, ombres, signaux de fumée, TAM-TAM, documents manuscrits, imprimés et maintenant sous format numérique… en garantissant toujours la sécurité de cette information par différents moyens, en utilisant des symboles, en protégeant le message durant son passage par le canal de transmission : (retour du pigeant avec une réponse, un recommandé avec accusé de réception en poste, et maintenant, nous parlons de cryptage des messages..)

La manière de véhiculer un message et d'assurer sa sécurité en confirmant que cette information n'a pas été attaquée par un tiers, outre l'expéditeur et le destinataire, progresse de jour en jour. Le souci de l'homme n'est donc plus comment véhiculer un message, mais comment le maintenir en sécurité lors de son transfert, le protégeant ainsi contre tout accès illégal et tout risque d'attaque et de modification… Ce souci est d'autant plus important dans les réseaux sans fils où l'accès est universel. Dans les zones piétonnes, les aéroports et les gares, mais aussi à la maison, dans une université… Les points d'accès Wifi sont de plus en plus nombreux et les réseaux sans fil font désormais partie de notre quotidien. Ils permettent un accès aisé, mais non sécurisé.

Dans ce projet, nous nous sommes intéressés à étudier l'authentification dans les réseaux sans fil, et plus particulièrement le réseau WiFi de Sup'Com. Nous avons donc identifié les solutions potentielles, permettant de subvenir à ce besoin, ayant retenu l'installation d'une plateforme RADIUS comme solution.

Nous avons aussi mis en évidence, la vulnérabilité des réseaux sans fils, en réalisant une attaque d'usurpation d'identité.

Finalement, nous avons mis en place une solution qui protège le réseau WiFi de Sup'Com, contre cette attaque.

Alors attachez vos ceintures, et bonne lecture…