**MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE**
**UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU**

**FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE**

**DEPARTEMENT D'ELECTRONIQUE**

# Mémoire de fin d'études

**En vue de l'obtention du**

**Diplôme de Master en Electronique**

Option : Réseaux et Télécommunications

# *Thème* :

## *Sécuriser un réseau Wifi en implémentant le protocole d'authentification 802.1x sur le serveur RADIUS.*

**Proposé et dirigé par :**

**Mr. ZIANI Rezki**

**Co-Promoteur :**

**Mr. MAMOU Amar**

**Présenté par :**

**Mlle. BOUAZIZ Sihem.**

**Mlle. FAREZ Nouara.**

**Promotion : 2012/2013**

# RÉSUMÉ

Se connecter à Internet sans le moindre câble, à domicile, au bureau, voir même dans les points d'accès publics et le besoin de plus en plus important de mobilité, ainsi que la diversification des réseaux a poussé les organismes à normaliser une nouvelle technologie nommée Wifi (*Wireless fidélité*) pour assurer une compatibilité entre les différents fabricants. Les utilisateurs équipés d'ordinateurs portables compatible Wifi peuvent rester connectés à tout moment grâce à la qualité de service offerte par le wifi.

L'application d'une stratégie de sécurité efficace est l'étape la plus importante qu'une entreprise doit franchir pour protéger son réseau. Pour cela nous avons donné les différentes attaques contre le Wifi et quelques solutions pour y remédier. Faisant partie de cette stratégie de sécurisation, le contrôle de l'accès physique au réseau s'avère une opération efficace pour limiter les possibilités d'accès des entités non désirées. Nous avons opté pour l'utilisation de l'authentification 802.1x qui permet d'authentifier les équipements connectés sur un port avant d'accéder au réseau local grâce à un serveur d'authentification sous Windows server 2008.

Nous avons suivi notre stage pratique d'une durée de troi mois au sein de l'entreprise 2INT (Institut Internationnale des Nouvelles Technologies) dont le but principale est de réaliser une implémentation du protocole d'authentification 802.1x sur un serveur RADIUS sous Windows server 2008.

Dans ce projet, nous avons mis en œuvre une technique de sécurisation d'accès aux réseaux informatiques des entreprises, afin de mieux garantir certains besoins de la sécurité : l'authentification, l'intégrité et la confidentialité des données échangées entre différents utilisateurs et d'éviter toute sorte de piratage informatique. Cette technique permet de contrôler l'accès physique aux équipements d'infrastructures réseaux en s'appuyant sur le protocole EAP pour le transport des informations d'identification en mode client/serveur, et un serveur d'identification RADIUS qui utilise une base de données Active Directory.

Après avoir installé et configuré Windows serveur 2008 (serveur DHCP, DNS, serveur NPS), nous avons pu configurer le protocole 802.1x. Ensuite nous avons appliqué l'authentification au niveau d'un point d'accès et d'un Switch Cisco Catalyst 2960.

Lors de la configuration du protocole 802.1x au niveau de l'authentificateur nous avons acquis beaucoup de connaissances sur le fonctionnement et la configuration du matériels Cisco.

Notre travail a été ainsi réalisé dans une bonne harmonie par tous les éléments de l'équipe technique, qui étaient tous à notre écoute le long de notre stage.

# REMERCIEMENTS

**E**n premier lieu, nous remercions notre **DIEU** le tous puissant de nous avoir donné la foi, la santé et nous a permit de bien mener ce travail.

**A**vant d'entreprendre la rédaction de notre mémoire, nous souhaitons vivement remercier et exprimer notre gratitude :

**A** notre promoteur **M$^{r}$ ZIANI.R**, à qui nous somme très reconnaissant pour ses remarques et ses conseils.

**A** notre Co-promoteur **M$^{r}$ MAMOU.A** et le responsable de l'entreprise 2Intpartners **M$^{r}$ KIBOUH.M** et **M$^{r}$ IMOULA.S** pour leurs orientations et leurs soutien qui nous ont beaucoup aidés au cours de notre projet.

**A**ux fonctionnaires d'**A**lgérie **T**elecom et spécialement **Mr. HADOUS.A** pour leur disponibilité et leur précieuse aide.

**N**ous tenons aussi à exprimer notre sincère gratitude à tous les enseignants de bonne foi qui nous ont accompagnés durant notre formation.

**S**ans oublier nos camarades étudiants et nos amis de MASTER I et MASTER II (réseau et télécommunication) qui nous ont soutenus tout au long de ce modeste travail.

**NOUARA, SIHEM**

*Je dédie ce modeste travail à :*

*Mes très chers parents qui m'ont soutenu tout au long de mes études et qui ont contribué à ma réussite, que dieu les garde et leur donne une longue vie.*

*Mon très cher frère Yacine et ma petite sœur adoré Ferroudja auxquels je souhaite une bonne réussite dans leurs études et leurs vies.*

*Toute ma famille et tous mes amis.*

*Mes camarades du département ELN.*

*Tous ceux qui m'ont aidé.*

*Tous ceux qui m'aime et que j'aime que je n'ai pas cité, mais que je n'ai pas oublié.*

*Ma chère amie et binôme NOUARA et sa famille.*

SAHEM

# *DEDICACES*

***Je Dédie ce modeste travail à :***

***Mes très chers parents, qui m'ont soutenu tout au long de mes études et qui ont contribué à ma réussite, que dieu les garde et leur donne une longue vie.***

***Mes frères : Brahim, Karim et leurs femmes Karima, Noura.***

***Mes sœurs : Fazia, Nadia et leurs maris Tarik et Brahim, et ma petite sœur que j'aime Rachida pour laquel je souhaite une bonne réussite dans ses études et sa vie.***

***Mes anges : Le Prince Zaki, Meyssa, Sid-Ali, Anaïs, et AmelNorElferah.***

***Toute ma famille et tous mes amis.***

***Mes camarades du département ELN.***

***Tous ceux qui m'ont aidé.***

***Tous mes amis, ceux et celles que j'aime, que je n'ai pas mentionné mais que je n'ai pas oublié.***

***A ma chère amie et binôme Sihem à qui je souhaite une bonne réussite.***

*NOUARA*

Introduction générale

## Chapitre I : Les réseaux sans fils



## Chapitre II : Sécurité d'un réseau Wifi et authentification 802.1x

## Chapitre III : Etude des éléments d'authentification

## Chapitre IV : Implémentation du protocole 802.1x sur le serveur RADIUS

## Liste des figures

### **Chapitre I :** Les réseaux sans fils



### **Chapitre II :** Sécurité d'un réseau Wifi et authentification 802.1x



### **Chapitre III :** Etude des éléments d'authentification



### **CHAPITRE IV :** Implémentation du protocole 802.1x sur le serveur RADIUS

## Liste des tableaux

### Chapitre I : Les réseaux sans fils



### Chapitre II: Sécurité d'un réseau Wifi et authentification 802.1x



### Chapitre III: Etude des éléments d'authentification

## INTRODUCTION GENERALE

Se connecter à Internet sans le moindre câble, à domicile, au bureau, voir même dans les points d'accès publics et le besoin de plus en plus important de mobilité, ainsi que la diversification des réseaux a poussé les organismes à normaliser une nouvelle technologie nommée Wifi (*Wireless fidélité*) pour assurer une compatibilité entre les différents fabricants. Les utilisateurs équipés d'ordinateurs portables compatible Wifi peuvent rester connectés à tout moment grâce à la qualité de service offerte par le wifi.

L'application d'une stratégie de sécurité efficace est l'étape la plus importante qu'une entreprise doit franchir pour protéger son réseau. Pour cela nous allons donner les différentes attaques contre le Wifi et quelques solutions pour y remédier. Faisant partie de cette stratégie de sécurisation, le contrôle de l'accès physique au réseau s'avère une opération efficace pour limiter les possibilités d'accès des entités non désirées. Nous avons opté pour l'utilisation de l'authentification 802.1x qui permet d'authentifier les équipements connectés sur un port avant d'accéder au réseau local grâce à un serveur d'authentification sous Windows server 2008. Cette technique repose sur le protocole EAP (*Extensible Authentification Protocol*).

Ce travail à été réalisé au sein d'une entreprise 2Intpartners (Institut International des Nouvelles Technologies) de Tizi-Ouzou dans le but de sécuriser un réseau Wifi composé de cinquante ordinateurs et trois Point d'Accès.

Notre projet est composé de quatre chapitres planifiés comme suite : Le premier consiste à définir les généralités sur les réseaux sans fils.

Le deuxième a pour but d'aborder les notions importantes sur la sécurité des réseaux wifi et l'authentification 802.1x.

Le troisième chapitre consiste à étudier le protocole RADIUS qui se base principalement sur un serveur relié à une base d'identification (base de données, Annuaire LDAP, Active Directory).

Dans le dernier chapitre, nous allons implémenter le protocole 802.1X sur le serveur RADIUS en configurant les différentes entités le constituant.

Nous terminerons par une conclusion générale en présentant la synthèse de notre travail.

## I.1 INTRODUCTION

Un réseau informatique est un ensemble d'équipements informatiques reliés entre eux dans le but de partager des ressources matérielles et logiciels de manière optimale. Les équipements du réseau sont interconnectés par le biais de supports de transmission.

L'évolution des technologies de l'information et de la communication et le besoin croissant de mobilité ont donné naissance aux réseaux sans fils qui utilisent comme support de transmission les ondes hertziennes suivant la technologie cellulaire.

Un réseau sans fils (*en anglais Wireless network*) est un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire. Grace aux réseaux sans fils, un utilisateur a 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''. Ce sont des réseaux faciles et rapides à déployer et qui permettent, en plus de la transmission de données, d'autres applications telles que la voix, la vidéo et l'Internet.

Les réseaux sans fils sont classés en quatre catégories selon leur étendue géographique et normalisés par un certain nombre d'organismes parmi lesquels nous citerons l'ISO (*International Standardization Organization*), l'IEEE (*Institute of Electrical and Electronics Engineers) et l'ETSI (European Telecommunications Standards Institute*).

## I.2 DEFINITION D'UN RESEAU SANS FILS

Un réseau sans fils est un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire en utilisant des ondes radioélectriques. Il est constitué d'une station de base (BTS) avec une couverture de type Point à Point ou Point-Multipoint dit cellulaire. Ce dernier type utilisé dans la plupart des réseaux locaux permet de desservir un ensemble d'abonnés d'une zone prédéfinie. Une cellule appelée BSS est composée d'un ensemble de stations reliées à un point d'accès qui constitue la station de base. Les BSS sont reliés à travers un backbone appelé système de distribution (DS : *Distribution System*).

Du coté des débits, le Wifi permet d'assurer une bande passante allant jusqu'à 54 Mbits théorique pour la norme 802.11g et 802.11a.

Les réseaux sans fils sont très prisés car ils sont plus faciles à déployer et offrent la mobilité aux utilisateurs. Ces réseaux ont été normalisés par l'IEEE 802.11 qui est un standard International et qui décrit les caractéristiques d'un réseau local sans fils (WLAN).

Le nom Wifi est une contraction de *Wireless Fidelity* qui était initialement, le nom donné à la certification délivrée par la WECA (*Wireless Ethernet Compatibility Alliance*) aux USA, qui est l'organisme chargé de maintenir l'interopérabilité entre les différents équipements répondant à la norme IEEE 802.11.

On distingue deux modes de fonctionnement ; le mode **infrastructure** et le mode **ad-Hoc** qu'on définira par la suite.

## I.3 FONCTIONNEMENT D'UN RESEAU SANS FILS

Un réseau sans fils utilise des radiofréquences (ondes électromagnétiques) comme porteuse d'un signal. Chaque point d'une liaison est constitué d'une antenne utilisée en émission et réception, et d'un module de traitement (modulation-démodulation) du signal.

Une onde électromagnétique est caractérisée par sa fréquence ou sa longueur d'onde, les deux étant liées par :

$$\lambda \times f = C \approx 3 \times 10^8 \text{ m/s (célérité).}$$

$$\lambda = C / f.$$

| Fréquence f(GHz) | longueur d'onde λ (cm) |
|---|---|
| 2.4 | 12.5 |
| 5.5 | 5.5 |

La longueur d'onde est une caractéristique à connaître car elle indique à quelle taille de structure elle va être sensible, c'est-à-dire absorbée ou bien transmise. Pratiquement l'électronique qui gère le codage de l'information et la modulation sur une porteuse (ainsi que la fonction inverse) est intégrée dans une carte de format PCMCIA ou bien PCI. Ces cartes sont appelées selon les constructeurs Air Port (selon Apple en 1999), Wifi ou 802.11b.

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

## I.4 CLASSIFICATION DES RESEAUX SANS FILS

De manière générale, les réseaux sans fils sont classés, selon leur étendue géographique en quatre catégories.

### I.4.1 Les réseaux WPAN

Ce sont des réseaux personnels sans fils regroupant les technologies suivantes :

| **Technologie** | **Norme** | **Débit théorique** | **Portée (m)** | **Bande de fréquence (GHz)** | **Observation** |
|---|---|---|---|---|---|
| Bluetooth | IEEE 802.15.1 | 1 Mbits/s | Une trentaine | 2,4- 2,4835 | - Bas prix<br>- L'émission de puissance dépend de la réglementation |
| HomeRF | Consortium (Intel, HP, Siemens, Motorola et Compaq) | 10 Mbits/s | 50 à 100 | 2,4 2,4835 | -Permet de relier des PC portables, fixes et d'autres terminaux. |
| ZigBee | IEEE 802.15.4 | 20 – 250 Kbits/s | 100 | 2,4 - 2,4835 | - Très bas prix,<br>- Très faible consommation d'énergie. |

## I.4.2 Les réseaux WLAN

Ce sont des réseaux permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Ils permettent de relier entre eux des terminaux présents dans la zone de couverture. Afin de permettre l'interopérabilité, les réseaux locaux (filaires et sans fils) sont normalisés par les organismes : IEEE et l'ETSI.

| **Technologie** | **Norme** | **Débit (Mbits/s)** | **Portée (mètres)** | **Bande de fréquence (GHz)** | **Observation** |
|---|---|---|---|---|---|
| WiFi | IEEE 802.11 | 2 - 54 | 35 -50 (indoor) des centaines (outdoor) | 2,4 – 2,4835 | -Elle comporte plusieurs déclinaisons IEEE 802.11 a/b/g |
| HiperLAN 1 | ETSI | 19 - 20 | Max 150 | 2,4 | - La vitesse de déplacement de l'utilisateur ne peut excéder 10 m/s<br>-Permet d'accéder aux réseaux ATM |
| HiperLAN 2 | | 54 | Max 150 | 5,4–5,7 | |
| HiperLink | | 155 | 150 - 200 | 17,2 – 17,3 | - Permet des liaisons fixes entre 2 points |
| DECT | | 2 | 300 | 1880 – 1900 MHz | -Technique d'accès TDMA |

## I.4.3 Les réseaux WMAN

Ce sont des réseaux qui couvrent partiellement ou totalement la superficie d'une ville.

| **Technologie** | **Norme** | **Débit (Mbits/s)** | **Portée (km)** | **Bande de fréquence (GHz)** | **Observation** |
|---|---|---|---|---|---|
| WiMax | IEEE 802.16 | 70 | 50 | 1– 66 | - Permet le raccordement des hots spots Wifi pour l'accès à Internet<br>-Techniques d'accès TDMA<br>Comporte plusieurs déclinaisons |

| | | | | | |
|---|---|---|---|---|---|
| HiperAccess | ETSI | supérieur à 100 | Très courte portée | 11–66 | - Permet d'accéder aux réseaux ATM |

### I.4.4 Les réseaux WWAN

Ils sont plus connus sous le nom de réseaux cellulaires mobiles.

| **Technologie** | **Norme** | **Débit** | **Portée (km)** | **Bande de fréquence** | **Observation** |
|---|---|---|---|---|---|
| GSM | Européenne | 9.6 Kbits/s | Jusqu'à 30km | 0.9 et 1.8 GHz | -Utilise une commutation de circuits<br>-permet le transfert de la voix ou de données numériques de faible volume |
| GPRS | Européenne | 114 Kbits/s (réel) et 171.2 Kbits/s (théorique) | 0.3 - 30 | 0.9 et 1.8 GHz | -Utilise une commutation de paquets<br>-Prise en charge des applications de données à moyens débits |
| UMTS | Européenne (ETSI) | 2G (théorique) | 0.3 - 30 | 2 GHz | -Offre un accès à Internet et à ses serveurs web<br>-Supporte des applications audio et vidéo basse définition<br>-Fonctionne en mode paquet et mode circuit |
| CDMA 2000 | Américaine (TIA) | $\leq$ 2 Mbits/s | | 2 GHz | -Utilise la technique d'étalement de bande |
| EDGE | Européenne | 384 Kbits/s (station fixe) et 144 Kbits/s (station mobile) | 0.3 - 30 | 2GHz | -Utilise la commutation de circuit |

Notre étude portera essentiellement sur les réseaux locaux sans fils de type IEEE 802.11.

## I.5 ARCHITECTURE DU RESEAU WIFI

L'architecture d'un réseau Wifi est basée sur un système cellulaire. Il existe deux modes de fonctionnement :

### I.5.1 Le mode infrastructure

Le mode infrastructure se base sur une station spéciale appelée point d'accès (PA), ce mode permet à des stations d'un réseau Wifi de communiquer avec des stations d'un réseau filaire existant (généralement Ethernet) via leur point d'accès commun.

L'ensemble des stations à portée radio du PA forme un BSS (Basic Service Set/Ensemble de services de base). Chaque BSS est identifié par un BSSID qui est généralement l'adresse MAC du point d'accès. Un ensemble de BSS forme un ESS (Extended Service Set). L'ESS est identifié par un ESSID communément appelé SSID et qui constitue le nom du réseau. Le SSID est un premier niveau de sécurité, vu que la station doit connaître ce SSID pour pouvoir se connecter au réseau.

Il est possible de relier plusieurs BSS (plus précisément leurs points d'accès) par une liaison appelée système de distribution DS (Distribution System) afin de constituer un ensemble de services étendus (ESS). Le système de distribution ou backbone est implémenté indépendamment de la partie sans fil, c'est généralement un réseau filaire (Ethernet), ou un câble entre deux point d'accès, mais il peut aussi être un réseau Token Ring, FDDI ou un autre réseau local sans fil. Cette architecture permet aussi d'offrir aux usagers mobiles l'accès à d'autres ressources (serveurs de fichiers, imprimante, etc.) ou d'autres réseaux (Internet). La zone ainsi couverte est appelée BSA (Base Set Area).

### I.5.2 Le mode Ad-Hoc

En mode ad hoc, il n'y a aucune administration centralisée. L'un des postes sera configuré comme point d'accès, les stations terminales communiquent alors directement entre elles afin de constituer un réseau « point à point » (*Peer to Peer* en anglais) ou « point multi point » c'est-à-dire un réseau dans lequel chaque machine joue en même temps le rôle de client et le rôle de point d'accès. Ces différentes stations forment une cellule appelée ensemble de services de base indépendants *IBSS* (Independant Basic Service Set), qui est un réseau sans fils constitué au minimum de deux stations et n'utilisant pas de point d'accès.

## I.6 DIFFERENTES EXTENSIONS WIFI

Le Wifi est un standard décrivant le réseau local sans fils (WLAN). Avec le Wifi, il est possible de mettre en place des réseaux locaux sans fils à haut débit sous réserve d'être à proximité d'un point d'accès. La norme 802.11 définit les couches basses du modèle **OSI** pour une liaison sans fil utilisant des ondes électromagnétiques. Ce standard possède différentes extensions selon le mode d'utilisation, la distance de diffusion du signal et le débit voulu.

### I.6.1 Les normes Wifi

| Nom de la norme | Nom | Description |
|---|---|---|
| 802.11a | Wifi | La norme 802.11a (baptisé Wifi 5) permet d'obtenir un débit théorique de 54 Mbps et un débit réel de 30Mbps. Elle spécifie 8 canaux radio dans la bande de fréquence des 5 GHz. |
| 802.11b | | Cette norme est la plus répandue actuellement. Elle propose un débit théorique de 11 Mbps (6Mbps réel) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. |

| | | |
|---|---|---|
| | Wifi | La plage de fréquence utilisée est la bande des 2.4 GHz, avec 13 canaux radio disponibles, dont 4au maximum non superposés (1, 5, 9, 13) |
| 802.11c | Pontage 802.11 vers 802.11d | Cette norme n'a pas d'intérêt pour le grand public. Il s'agit uniquement d'une modification de la norme 802.11 (niveau liaison de données). |
| 802.11d | Internationalisation | Cette norme est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11. elle consiste à permettre aux différents équipements d'échanger des informations sur les plages de fréquence et les puissances autorisées dans le pays d'origine du matériel. |
| 802.11e | Amélioration de la qualité de service | Cette norme vise à donner des possibilités en matière de qualité de service au niveau de la couche liaison de données. Ainsi cette norme a pour but de définir les différents paquets en termes de bande passante et le délai de transmission de telle manière à permettre notamment une meilleure transmission de la voix et de la vidéo. |
| 802.11f | Itinérance (roaming) | Cette norme est une recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole Inter-accès Point Roaming Protocol permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau. Cette possibilité est appelée itinérance (ou roaming en anglais). |
| 802.11g | Wifi 2 | Elle offre un haut débit (54Mbps théorique, 30Mbps réel) sur la bande de fréquence de 2.4 GHz. Cette norme a une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b. |
| 802.11h | | Elle vise à approcher la norme 802.11 du standard européen (Hiper LAN 2 d'où le 'h' de 802.11h) et être en conformité avec la réglementation européenne en matière de fréquences et d'économie d'énergie. |
| 802.11i | | Elle a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'AES (Advanced Encryption Standard) et propose un chiffrement des communications utilisant les technologies 802.11a, 802.11b et 802.11g. |
| 802.11r | | Cette norme a été élaborée de telle manière à utiliser des signaux infrarouges. Elle est désormais dépassée techniquement. |
| 802.11j | | La 802.11j est à la réglementation japonaise ce que le 802.11h est à la réglementation européenne. |
| 802.11n | | La norme IEEE 802.11n, ratifiée en septembre 2009, permet d'atteindre un débit théorique allant jusqu'à 450 Mbits/s sur chacune des bandes de fréquences utilisable (2,4 GHz et 5 GHz). Elle améliore les standards précédents : IEEE 802.11a pour la |

| | | |
|---|---|---|
| | | bande de fréquences des 5 GHz, IEEE 802.11b et IEEE 802.11g pour la bande de fréquences des 2,4 GHz. |
| 802.11s | Réseau maillé | A été crée en 2004, le débit théorique atteint est de 10 à 20 Mbits/s. Elle vise à mettre en œuvre la mobilité sur les réseaux du type ad-Hoc. |

## I.6.2 Débits et portées

Les normes 802.11a, 802.11b et 802.11g appelées « normes physiques » correspondent à des révisions du standard 802.11 et proposent des modes de fonctionnement, permettant d'obtenir différents débits en fonction de la portée.

| **Standard** | **Bande de fréquence (GHz)** | **Débit (Mbit /s)** | **Portée (m)** |
|---|---|---|---|
| 802.11a | 5 | 54 | 10 |
| 802.11b | 2.4 | 11 | 100 |
| 802.11g | 2.4 | 54 | 100 |

- **802.11a**

La norme **802.11a** permet d'obtenir un débit théorique de **54 Mbps**, soit cinq fois plus que le 802.11b, pour une portée d'environ une trentaine de mètres seulement. La norme 802.11a s'appuie sur un codage du type (Orthogonal Frequency Division Multiplexing ; **OFDM**) sur la bande de fréquence de **5 GHz** et utilisent **8 canaux** qui ne se recouvrent pas.

| **Débit théorique (en intérieur)** | **Portée (mètre)** |
|---|---|
| 54 Mbits/s | 10 m |
| 48 Mbits/s | 17 m |
| 36 Mbits/s | 25 m |
| 24 Mbits/s | 30 m |
| 12 Mbits/s | 50 m |
| 6 Mbits/s | 70 m |

- **802.11b**

La norme **802.11b** permet d'obtenir un débit théorique de **11 Mbits/s**, pour une portée d'environ une **cinquantaine de mètres** en **intérieur** et jusqu'à **200 mètres** en **extérieur** (et même au-delà avec des antennes directionnelles).

| **Débit théorique (Mbits/s)** | **Portée intérieur** | **Portée extérieure** |
|---|---|---|
| 11 | 50 m | 200 m |
| 5,5 | 75 m | 300 m |
| 2 | 100 m | 400 m |
| 1 | 150 m | 500 m |

**Remarque :** les équipements **802.11a** ne sont donc pas compatibles avec les équipements **802.11b**. Il existe toutefois des matériels intégrant des puces 802.11a et 802.11b, on parle alors de matériels **« dual band ».**

- **802.11g**

La norme **802.11g** permet d'obtenir un débit théorique de **54 Mbits/s** pour des portées équivalentes à celles de la norme **802.11b**. D'autre part, dans la mesure où la norme 802.11g utilise la bande de fréquence **2,4 GHz** avec un **codage OFDM**, cette norme est compatible avec les matériels 802.11b, à l'exception de certains anciens matériels.

| **Débit théorique (Mbits/s)** | **Portée intérieur** | **Portée extérieure** |
|---|---|---|
| 54 | 27 m | 75 m |
| 48 | 29 m | 100 m |
| 36 | 30 m | 120 m |
| 24 | 42 m | 140 m |
| 18 | 55 m | 180 m |
| 12 | 64 m | 250 m |
| 9 | 75 m | 350 m |
| 6 | 90 | 400 |

- **802.11h**

**IEEE 802.11h** est un amendement à la norme IEEE 802.11 permettant **d'harmoniser le** standard **IEEE 802.11a** avec les contraintes règlementaires de la Communauté européenne relatives aux transmissions hertziennes dans la bande de fréquences des **5 GHz** et aux économies d'énergie. Cet amendement a été ratifié le 14 septembre 2003 et publié le 14 octobre de la même année.

## I.7 DESCRIPTION DES COUCHES WIFI

La norme IEEE 802.11 repose sur une architecture en couche définie par le standard IEEE et couvre les deux premières couches du modèle **OSI**, c'est à dire la couche physique et la couche liaison de données.

| |
|---|
| LLC (Logical Link Control) |
| MAC (Media Access Control) |
| PLCP (Physical Layer Convergence Protocol) |
| PMD (Physical Medium Dependent) |

### I.7.1 La couche liaison de données

Elle est aussi composée de deux sous couches.

#### I.7.1.1 *La sous couche LLC (Logical Link Control)*

La sous couche LLC de la norme IEEE 802.11 utilise les mêmes propriétés que la sous couche LLC de la norme IEEE 802.3 (Ethernet), ce qui correspond à un mode avec connexion et avec acquittement des données. Cette couche est définie par le standard **IEEE 802.2**, elle permet d'assurer le lien entre la couche MAC et la couche réseau (OSI 3).

#### I.7.1.2 *La sous couche MAC (Media Access Control)*

La sous couche MAC 802.11 intègre les mêmes fonctionnalités que la sous couche MAC 802.3, à savoir :

- Préparer la transmission du signal au niveau de la couche physique (matériel).
- Assurer l'adressage de couche liaison de données et marque le début et la fin de la trame.

- Le contrôle d'erreurs CRC (*Contrôle de Redondance Cyclique*).

Dans la norme 802.11, la sous couche MAC réalise également la fragmentation et le réassemblage des trames.

## I.7.2 La couche physique

Cette couche assure la transmission des données sur le support, elle est constituée de deux sous couches : PMD et PLCP

### I.7.2.1 *La sous couche PMD (Physical Medium Dependent)*

Elle spécifie le type de support de transmission, le type d'émetteur-récepteur, le type de connecteur et la technique de modulation et de démodulation.

### I.7.2.2 *La sous couche PLCP (Physical Layer Convergence Protocol)*

Elle s'occupe de la détection du support et fournit un signal appelé CCA (Clear Channel Assessment) à la sous couche MAC pour lui indiquer si le support est occupé ou non.

L'IEEE a défini des couches différentes caractérisées chacune par une technique de modulation précise. Il s'agit des techniques suivantes :

- *FHSS (Frequency Hopping Spread Spectrum):* C'est une modulation avec étalement du spectre par saut de fréquence. Elle fonctionne sur la bande ISM des 2,4 GHz.
- *DSSS (Direct Sequence Spread Spectrum) :* C'est une modulation avec étalement du spectre par séquence directe. Elle fonctionne sur la bande ISM des 2,4 GHz.
- *OFDM (Orthogonal Frequency Division Multiplexing) :* Son principe est d'effectuer un multiplexage fréquentiel de sous-porteuses orthogonales.
- *Infrarouge :* Elle permet la transmission des données grâce aux ondes lumineuses par réflexion multiple ou en visibilité directe.

# I.8 LE FORMAT DE LA TRAME WIFI

**a.** ***Le préambule*** est dépendant de la couche physique et contient deux champs : un champ de synchronisation Synch et un champ SFD *(Start Frame Delimiter)*. Le champ Synch est utilisé par le circuit physique pour sélectionner l'antenne à laquelle se raccorder. Quant au champ SFD, il est utilisé pour délimiter le début de la trame.

La longueur du champ préambule varie selon la technique de modulation utilisée au niveau de la couche physique.

Pour la technique de modulation FHSS, le champ Synch s'étend sur 80 bits et le champ SFD sur 16 bits. Dans la technique DSSS, il existe deux formats possibles du champ Préambule : un format par défaut avec un champ Synch long de 128 bits, et un format avec un champ Synch court de 56 bits. Le deuxième format est utilisé pour améliorer les performances du réseau dans les cas de données critiques telles que la voix, la VoIP (Voice over IP). Le préambule court est également intéressant lorsque les trames doivent être fragmentées (on transmet moins de bits non utiles).

**b.** ***L'en-tête PLCP*** contient les informations logiques utilisées par la couche physique pour décoder la trame. Dans la modulation FHSS l'en-tête PLCP se présente comme suit :

- Le champ *PLW* (PLCP-PDU *Length Word*) indique le nombre d'octets que contient le paquet, ce qui est utile à la couche physique pour détecter correctement la fin du paquet.
- Le champ *fanion de signalisation PSF* (PLCP Signaling Field) indique le débit de transmission des données MAC.
- Le champ *HEC* (*Header Error Check)* utilise un CRC sur 16 bits pour la vérification

de l'intégrité de l'en-tête PLCP.

Dans la modulation DSSS, l'en-tête PLCP se présente sous une autre forme.

Elle est composée de quatre champs :

- Le champ *Signal* indique la modulation à utiliser pour l'émission et la réception des données.
- Le champ *Service* est réservé pour une utilisation future.
- Le champ *Length* indique le nombre de microsecondes nécessaires pour transmettre les données.
- Le champ de *contrôle d'erreurs* CRC sur 16 bits.

**c.** ***le champ de données MAC*** c'est la trame encapsulée au niveau de la sous couche MAC, son format est le suivant :

Elle est composée de cinq champs :

- Le champ de *contrôle* **:** Il est sur 2 octets.
- Le champ de *Durée* / ***ID :*** Il est sur 2octets

- Les champs *adresse 1, 2, 3 et 4* : Ces champs correspondent à des adresses MAC de stations sources, de stations de destination ou de BSSID (Base services Set Identifier).
- Le champ *contrôle de séquence* **:** C'est un champ sur 12 bits utilisé pour attribuer à chaque trame un numéro de séquence entre 0 et 4095. Le numéro de séquence est incrémenté de 1 à chaque fois qu'une trame est envoyée. Au cours de la transmission d'une trame, quatre bits sont utilisés pour coder le numéro du fragment dans l'ordre d'envoi des fragments.
- Le champ *CRC* **:** Il s'étend sur 32 bits, il sert au contrôle d'erreur.

**d. Le champ de *contrôle d'erreur CRC*** sur 16 bits qui permet de vérifier l'intégrité des données.

## I.9 LES EQUIPEMENTS DE TRANSMISSION

Il existe différents types d'équipements pour la mise en place d'un réseau sans fil Wifi :

- **Les adaptateurs sans fils ou Cartes d'Accès :**

En anglais (Wireless Adapters)**;** il s'agit d'une carte réseau adaptée à la norme 802.11 permettant à une machine de se connecter à un réseau sans fils. Les adaptateurs Wifi sont disponibles dans de nombreux format (carte **PCI**, carte **PCMCIA**, adaptateur **USB**, carte **compactflash**,…). On appelle **station** tout équipement possédant une telle carte.

- **La carte réseau sans fils PCI :**

- **La carte PCMCIA :**

- **La carte sans fils connectée à un port USB :**
-

- **Les points d'accès**

Un point d'accès Wifi est un équipement réseau qui permet à votre ordinateur de se connecter sur le réseau sans fil. Il possède une antenne radio supportant les normes 802.11b et 802.11g, il joue le rôle de passerelle entre le réseau sans fil et le réseau filaire.

## I.10 AVANTAGES ET INCONVENIENTS

### I.10.1 *Avantages* :

Si les caractéristiques actuelles d'un réseau sans fils permettent de rivaliser avec celles d'un réseau filaire, les réseaux sans fils ne visent toutefois pas à remplacer les réseaux locaux

mais plutôt à leur apporter de nombreux avantages découlant d'un nouveau service : la mobilité de l'utilisateur.

Les principaux avantages résident dans la réduction du coût de câblage et la souplesse dans le déploiement du réseau.

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

### I.10.2 *Inconvénient :*

Un certain nombre de problèmes se posent. On peut citer en particulier :

- **L'énergie :** les applications relatives aux réseaux sans fils ont un caractère nomade. Emettre ou recevoir des données consomme de l'énergie et on cherche à l'économiser en optimisant les protocoles de gestion du réseau.
- **Qualité et continuité du signal : C**es notions ne sont pas garanties du fait des problèmes pouvant venir des interférences, du matériel et de l'environnement.
- **Une faible sécurité :** il est facile d'espionner un canal radio de manière passive et est donc difficile de le protéger de manière physique (car on ne peut empêcher quelqu'un de placer discrètement une antenne réceptrice très sensible dans le voisinage), donc la protection se fait de manière logique avec de la cryptographie ou éventuellement des antennes très directionnelles.

De plus les ondes hertziennes sont difficiles à confiner dans une surface géographique restreinte, il est donc facile pour un pirate d'écouter le réseau si les informations circulent en clair. Il est donc nécessaire de mettre en place les dispositions nécessaires de telle manière à assurer une confidentialité des données circulant sur les réseaux sans fils.

## I.11 CONCLUSION

Les réseaux sans fils en général, et le Wifi en particulier sont des technologies intéressantes et très utilisées dans divers domaines comme l'industrie, la santé et le domaine militaire. Cette diversification d'utilisation revient aux différents avantages qu'apportent ces technologies, comme la mobilité, la simplicité d'installation, la disponibilité.

## II.1 INTRODUCTION

Installer un réseau sans fils sans le sécuriser permet à des personnes non autorisées d'écouter, de modifier et d'accéder à ce réseau, il est donc indispensable de le sécuriser dès son installation de façon plus ou moins forte selon les objectifs de sécurité et les ressources que l'on y accorde. La sécurité est réalisée à différents niveaux : configuration des équipements et choix des protocoles.

## II.2 LES ATTAQUES CONTRE LES RESEAUX WIFI

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

### II.2.1 Interception des données

L'interception des données se traduit par un accès illicite au contenu d'un message. Il s'agit d'une attaque contre l'intégrité.

En l'absence de chiffrement, il est facile de récupérer le contenu des données circulant sur le réseau, c'est-à-dire que le réseau 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. Pour un particulier, la menace est faible car les données sont rarement confidentielles, si ce n'est les données à caractère personnel. Pour une entreprise en revanche l'enjeu stratégique peut être très important.

Les ondes radioélectriques ont une grande capacité à se propager dans toutes les directions avec une grande portée; elles sont donc difficiles à contrôler même s'il existe des revêtements permettant de bloquer les ondes.

### II.2.2 Intrusion dans le réseau

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 fil non sécurisé représente de cette façon un point d'entrée royal pour le pirate au réseau interne d'une entreprise ou 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 fil peut également représenter une occasion pour ce dernier pour mener des attaques sur Internet.

Etant donné qu'il n'y a aucun moyen d'identifier le pirate sur le réseau, l'entreprise ayant installé le réseau sans fil risque d'être tenu pour responsable de l'attaque.

### II.2.3 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 de données. Il est possible d'envoyer des paquets requérant la dissociation de cette station afin de perturber le fonctionnement du réseau sans fil.

Un autre point faible est que la connexion à des réseaux sans fil est consommatrice d'énergie. Un envoi conséquent de données peut surcharger une machine. Tous les périphériques portables possèdent une autonomie limitée, un pirate peut donc vouloir provoquer une surconsommation d'énergie afin de rendre l'appareil temporairement inutilisable, c'est ce que l'on appelle un déni de service sur batterie.

### II.2.4 Le sniffing (écoute de réseau)

Un sniffer est un dispositif matériel ou logiciel qui permet d'écouter le trafic qui transite dans un réseau à travers un adaptateur (carte réseau sans fils), et peut être placé n'importe où. Il représente une menace pour les raisons suivantes :

- ✓ Capter les mots de passe.
- ✓ Intercepter les informations confidentielles ou propriétaires.
- ✓ Etre utilisés pour ouvrir une faille dans le système de sécurité d'un réseau voisin.

Un attaquant se place sur des points stratégiques comme la proximité d'une machine ou d'un réseau recevant de nombreux mots de passe. Si le réseau est ouvert sur Internet, l'attaquant intercepte les procédures d'authentification entre deux réseaux. Cela pourra accroître les champs d'activité de l'attaquant. Le résultat de ces attaques est la désorganisation des informations, la violation de la confidentialité et de l'intégrité des objets ou leur modification.

### II.2.5 Le spooffing (ou L'usurpation d'adresse IP)

C'est une technique utilisée en informatique qui consiste à envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribuée à l'ordinateur qui les émet. Il permet de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper l'identité d'un autre équipement du réseau pour bénéficier des services auxquels il a accès. Pour éviter ce genre d'attaques, il est recommandé de ne pas utiliser de service se basant sur l'adresse IP pour identifier les clients.

### II.2.6 Le brouillage radio

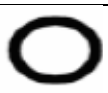
Les ondes radio sont très sensibles aux interférences, c'est la raison pour laquelle un signal peut facilement être brouillé par une émission radio ayant une fréquence proche de celle utilisée par le réseau sans fil.

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.

### II.2.7 Le war driving

C'est une pratique qui consiste à circuler dans la ville avec un ordinateur portable équipé d'une carte réseau sans fils pour la recherche de réseaux sans fils.

Des cartographies sont alors établies et permettent de mettre en évidence les réseaux sans fils déployés non sécurisés. De nombreux sites regroupant ces informations ont vu le jour sur Internet. Des étudiants londoniens ont eu l'idée d'inventer un *langage des signes* dont le but est de rendre visible 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* ».

| Deux demi-cercles opposés désignent un réseau ouvert offrant un accès à Internet | Un rond signale désigne la présence d'un réseau sans fil ouvert sans accès à un réseau filaire | Un W encerclé met en évidence la présence d'un réseau sans fil correctement sécurisé |
|---|---|---|
|  |  |  |

### II.2.8 L'homme du milieu "man in the middle"

C'est un scénario d'attaque dans lequel un pirate écoute et peut modifier une communication entre deux interlocuteurs. Elle consiste à mettre en place un point d'accès étranger, qui pourra collecter les clés fournies par une station qui aura tenté de s'y connecter, livrant ainsi les clés du processus de connexion.

## II.3 LES SOLUTIONS POUR SECURISER UN RESEAU WIFI

La sécurité d'un réseau Wifi doit être renforcée selon le degré de confidentialité des données.

### II.3.1 La sécurité élémentaire

Elle permet uniquement de résoudre le problème du contrôle d'accès. Il s'agit de techniques qui peuvent être utilisées de façon complémentaire :

#### II.3.1.1 L'identificateur de réseau

Il s'agit de l'ESSID (*Extended Service Set Identifier*), souvent appelé SSID que l'utilisateur doit connaître pour se connecter au réseau. Cette protection est en fait très sommaire, vu que les points d'accès envoient périodiquement et en clair le SSID dans les trames balise. Il suffit d'une simple écoute du réseau pour obtenir le SSID.

#### II.3.1.2 Le mot de passe

Pour se connecter au réseau, l'utilisateur utilise un mot de passe. Cette protection est également très simpliste. Il est facile pour un intrus de capturer le mot de passe et de l'utiliser par la suite pour se connecter au réseau.

#### II.3.1.3 La protection par adresse MAC

Chaque adaptateur réseau possède une adresse physique unique appelée adresse MAC, représentée par douze chiffres hexadécimaux.

Les points d'accès permettent généralement dans leur interface de configuration, de gérer une liste de droits d'accès basée sur les adresses MAC des équipements autorisés à se connecter au réseau. Le filtrage MAC peut aussi être contourné. Une écoute passive du réseau permet de récupérer les adresses MAC reconnues par le réseau.

Aussi, de nombreux adaptateurs radio permettent de modifier par logiciel leurs propres adresses MAC.

#### II.3.1.4 La protection par adresse IP

Les risques d'intrusions externes sont bien moindres en attribuant des adresses IP fixes aux stations bénéficiant d'une connexion sans fil. Il faut, donc désactiver la fonction DHCP au niveau du serveur auquel est connectée la borne Wifi.

#### II.3.1.5 Sécurité des points d'accès

Changer la configuration par défaut des points d'accès est une première étape essentielle dans la sécurisation du réseau sans fil. Pour cela il est nécessaire de :

- changer les mots de passe par défaut (notamment administrateur) par des mots de passe blindés.
- modifier la configuration par défaut (adressage privé utilisé avec DHCP ou adresse de l'interface par exemple).
- désactiver les services disponibles non utilisés (SNMP, Telnet...).
- régler la puissance d'émission du point d'accès au minimum nécessaire.

Il est également important de mettre à jour le Firmware du point d'accès dès que le constructeur propose une mise à jour (résolution d'un problème de sécurité sur un des services disponibles par exemple). Cette mise à jour suppose des tests préalables poussés afin de vérifier la compatibilité avec l'existant une fois la mise à jour effectuée.

Changer le SSID par défaut est une bonne pratique, largement recommandée dans la plupart des cas. Il est judicieux de ne pas choisir un SSID attractif. La plupart des points d'accès donnent la possibilité de désactiver la diffusion du SSID. Il ne s'agit nullement d'une mesure de sécurité car une personne informée pourra obtenir le SSID très facilement : le SSID est une donnée qui est visible lors de l'association d'un client.

Ensuite, il s'agit de configurer le point d'accès en activant les options de sécurité répondant aux objectifs choisis en matière de sécurité.

Enfin, au-delà de la sécurité logique, il est nécessaire de prendre en compte la sécurité physique des points d'accès. Le vol d'un point d'accès a pour but d'analyser sa configuration et récupérer des informations importantes telles que l'adressage IP, le mot de passe, la clé de

chiffrement. Pour éviter les conséquences d'un tel vol, on utilise un Switch WLAN pour qu'aucune information importante ne soit stockée physiquement sur le point d'accès.

## II.3.2 Sécurité renforcée

Les méthodes suivantes permettent de mieux sécuriser le réseau :

### II.3.2.1 Mise en place d'un VPN

Un réseau VPN repose sur un protocole appelé « protocole de tunneling » qui permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise. Il peut offrir des connections routées et des connections d'accès distant à des réseaux privés par l'intermédiaire d'internet. Il est dit virtuel car il relie deux réseaux « physiques » (réseaux locaux) par une liaison non filaire (internet), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent accéder aux données.

### II.3.2.2 Mise en place d'un pare-feu

Un firewall est un ensemble de différents composants matériels et logiciels qui contrôlent le trafic intérieur / extérieur, il permet de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers comme internet et de filtrer les paquets de données échangés avec le réseau.

On peut installer un firewall comme si le point d'accès était une connexion internet. Ce firewall peut être le serveur **IPsec** (VPN) des clients sans fils.

Un réseau Wifi "sécurisé" peut se schématiser comme sur la figure II.1. On considère ici que tout le réseau Wifi est étranger au réseau local et Internet. L'utilisation d'un Pare-feu pour la connexion Internet, permet de filtrer les adresses MAC associées à des adresses IP fixes.

Certains points d'accès proposent de "petits" firewall permettant de faire un filtrage de plus sur les clients du réseau.

#### II.3.2.3 Améliorer l'authentification

Afin de gérer plus efficacement les authentifications, les autorisations et la gestion des comptes utilisateurs ; il est possible de recourir à un **serveur RADIUS** (*Remote Authentication Dial-In User Service*) qui est un système client/serveur permettant de gérer les comptes des utilisateurs et les droits d'accès associés.

### II.3.3 Cryptage des données

Afin de sauvegarder la confidentialité et l'intégrité des données circulant sur le lien sans fils, il est indispensable de chiffrer le trafic de telle sorte qu'il ne soit intelligible que par les destinataires légitimes.

#### II.3.3.1 Définition

La cryptographie est une méthode permettant de rendre secrètes (illisibles) des informations afin de garantir l'accès à un seul destinataire authentifié. Elle est essentiellement basée sur l'arithmétique : il s'agit de transformer les lettres qui composent le message en succession de chiffres, puis faire des calculs sur ces chiffres pour :

- Les modifier de telle façon à les rendre incompréhensible.
- Faire en sorte que le destinataire saura les décrypter.

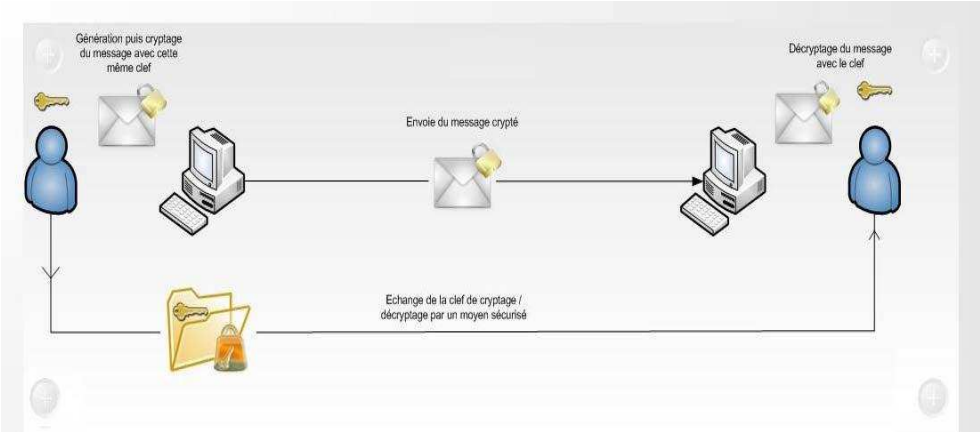
Le fait de coder un message de façon à le rendre secret s'appelle le cryptage. La méthode inverse est appelée décryptage, elle nécessite une clé de décryptage.

On distingue deux types de cryptages : symétrique et asymétrique.

**A) Cryptage symétrique**

Le cryptage symétrique appelé également cryptage à clé secrète ou chiffrement conventionnel, utilise une même clé pour crypter et décrypter le message. Les algorithmes de chiffrement les plus connus sont: le DES (*Data Encryption Standard*), le Triple DES et l'AES.

Le principe de cette technique est la distribution des clés dans un réseau étendu car elle nécessite le partage d'une seule clé avec chacun des correspondants.




**B) Cryptage asymétrique**

Ce système de cryptage utilise deux clés différentes pour chaque utilisateur : une est privée et n'est connue que par son propriétaire; l'autre est publique et donc accessible par tout le monde.

Les clés publiques et privées sont mathématiquement liées par l'algorithme de cryptage de telle manière qu'un message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante car ces deux clés sont générées en même temps. Une clé est donc utilisée pour le cryptage et l'autre pour le décryptage.

Le principal avantage du cryptage à clé publique est de résoudre le problème de l'envoi de clé privée sur un réseau non sécurisé. Il est plus lent que la plupart des cryptages à clé privée mais il reste préférable pour 3 raisons :

- Plus évolutif pour les systèmes possédant des millions d'utilisateurs.
- Permet de signer le message donc garantir l'authentification et le non répudiation.
- Supporte les signatures numériques.

### II.3.3.2 Le chiffrement WEP *(Wired Equivalent Privacy)*

Le WEP est un protocole chargé du chiffrement des trames 802.11 utilisant l'algorithme RC4 avec des clés symétriques, secrètes et statiques d'une longueur de 64 ou 128 bits. Le principe du WEP consiste à définir dans un premier temps une clé secrète de 40 ou 128 bits. Cette clé secrète 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 le nombre pseudo-aléatoire et la trame.

La clé de session partagée par toutes les stations est statique, c'est-à-dire que pour déployer un grand nombre de stations Wifi il est nécessaire de les configurer en utilisant la même clé de session, la connaissance de la clé est suffisante pour déchiffrer les communications.

| | Vecteur d'initialisation(VI) | Clef partagée | Clef RC4 K=VI ,K |
|---|---|---|---|
| WEP | 24 bits | 40 bits | 64 bits |
| WEP2 | 24 bits | 104 bits | 128 bits |

Dans le cas de la clé de 40 bits, une attaque par force brute (c'est-à-dire en essayant toutes les possibilités de clés) peut très vite amener le pirate à trouver la clé de session, et l'utilisation des clés WEP a révélé deux faiblesses importantes:

- L'utilisation d'algorithmes cryptographiques peu développés comme le RC4 car il suffit de quelques heures à un éventuel pirate pour casser les clés utilisées.
- L'impossibilité d'authentifier un ordinateur ou un utilisateur qui se connecteront au réseau.

### II.3.3.3 Le chiffrement WPA (*Wifi Protected Access*)

Le WPA est une version « allégée » du protocole 802.11i, et une solution de sécurisation de réseau wifi proposé par la Wifi Alliance, afin de combler les lacunes du WEP. Il Permet d'utiliser une clé par station connecté au réseau sans fil, alors que le WEP, utilise la

même clé pour tout le réseau. Les clés sont en effet générées et distribuées de façon automatique par le point d'accès sans fil si celui-ci est compatible à WPA.

Le WPA repose sur des protocoles d'authentification et un algorithme de cryptage, TKIP (*Temporary Key Protocol*), qui permet la génération aléatoire des clés, et offre la possibilité de modifier la clé de chiffrement plusieurs fois par seconde, pour plus de sécurité. Les intérêts de TKIP par rapport aux clés WEP sont les suivants :

- Vecteur d'initialisation de 48bits au lieu de 24 bits pour le WEP.
- Génération et distribution des clés : le WPA génère et distribue les clés de cryptage de façon périodique à chaque client, et chaque trame utilise une nouvelle clé, évitant ainsi d'utiliser une même clé WEP pendant des semaines voire des mois.
- Code d'intégrité du message appelé MIC (*Message Integrity Code*) permet de vérifier l'intégrité ICV (Int*egrity Check Value*), il est sur 4 Octets pour le WEP et sur 8 octets pour WPA.

### Architecture WPA

Le WPA peut fonctionner selon deux modes :

- **WPA Entreprise :** ce mode impose l'utilisation d'une infrastructure d'authentification 802.1x basée sur l'utilisation d'un serveur d'authentification généralement un serveur RADIUS (*Remote Authentication Dial In User Service*) qui permet d'identifier les utilisateurs sur le réseau et de définir leurs droits d'accès, et d'un contrôleur réseau (le point d'accès).
- **WPA Personal :** ce mode permet de mettre en œuvre une infrastructure sécurisée basée sur un WPA restreint ou WPA-PSK (*Pre-Shared Key*) sans serveur d'authentification. Il repose sur l'utilisation d'une clé partagée, appelée PSK, en déployant une même clé de chiffrement dans l'ensemble des équipements. Contrairement au WEP, il n'est pas nécessaire de saisir une clé de longueur prédéfinie, en effet, le WPA permet de saisir une *passphrase* (phrase secrète), traduite en PSK par un algorithme de hachage.

Cette première version du WPA ne prend en charge que les réseaux en mode infrastructure, ce qui signifie qu'il ne permet pas de sécuriser des réseaux sans fils en mode Ad-Hoc.

Ce protocole possède quelques faiblesses, dont sa sensibilité aux attaques de type déni de service. En effet, si quelqu'un envoie au moins deux paquets chaque seconde utilisant une clé de cryptage incorrecte, le point d'accès sans fils tuera toutes les connexions utilisateurs pendant une minute. C'est un mécanisme de défense pour éviter les accès non autorisés à un réseau protégé, mais il est capable de bloquer tout un réseau sans fils.

Outre ce problème, il manque au WPA pour fournir une meilleure sécurité :

- Un SSID (*Service Set IDentifier*) sécurisé, c'est-à-dire une chaine de caractères alphanumériques sécurisée permettant d'identifier un réseau sans fils.
- Une déconnection rapide et sécurisée.

### II.3.3.4 La norme 802.11i ou WPA2

**La norme 802.11i** a été ratifiée le 24 juin 2004, afin de fournir une solution de sécurisation poussée des réseaux Wifi. Elle s'appuie sur l'algorithme de chiffrement TKIP, comme le WEP, mais prend également en charge l'AES (*Advenced Encryption Standard*), beaucoup plus sûr que RC4 pour les données. La Wifi Alliance a ainsi créé une nouvelle certification, baptisée WPA-2, pour les matériels prenant en charge le standard 802.11i (ordinateur portable, PDA, carte réseau…).

Le **WPA-2** offre de nouvelles fonctionnalités de sécurité telle que le *Key caching* et la **pré-authentification** et contrairement au WPA, il permet de sécuriser également les réseaux en mode Ad Hoc.

Pour résumer, le WPA-2 offre par rapport au WPA :

- Une sécurité et une mobilité plus efficaces grâce à l'authentification du client indépendamment du lieu où il se trouve.
- Une intégrité et une confidentialité fortes garanties par un mécanisme de distribution dynamique de clés.
- Une souplesse accrue grâce à une réauthentification rapide et sécurisée.

Toutefois, pour profiter du WPA-2, les entreprises doivent disposer d'un équipement spécifique tel qu'une puce cryptographique dédiée pour les calculs exigés par l'AES.

## II.4 AUTHENTIFICATION IEEE 802.1X

### II.4.1 Définition

Le standard 802.1x est une solution de sécurisation, mise au point par l'IEEE en juin 2001. Elle permet d'authentifier les équipements connectés sur un port avant d'accéder à un réseau (sans fils ou filaire) grâce à un serveur d'authentification. Elle repose sur le protocole EAP (Extensible Authentification Protocol.

**Le 802.1X se base sur trois éléments :**

- **Supplicant** : le client demande à s'authentifier avant de pouvoir accéder aux ressources du réseau.
- **Authenticator**: l'authentificateur est l'équipement réseau (commutateur, point d'accès…) auquel le client se connecte. Suivant la réponse du serveur d'authentification, le commutateur laissera passer ou non le trafic du client.
- **Authentication server** : le serveur d'authentification vérifie sur demande du commutateur si le demandeur peut ou non accéder aux ressources réseau LAN.

### II.4.2 Les méthodes d'authentification de 802.1x

Le protocole 802.1x implique une communication indirecte entre le poste de travail et le serveur Radius. La communication entre le poste de travail et le NAS s'appuie sur le protocole EAP.

### II.4.2.1 Le protocole EAP

#### II.4.2.1.a) Définition

La communication entre l'équipement réseau (*authenticator*) et le serveur d'authentification est assurée par le protocole EAP (*Extensible Authentication Protocol*) qui assure le transport des informations d'authentification et permet d'utiliser différentes méthodes d'authentification d'où le terme '' Extensible''. Le domaine d'application de ce protocole correspond donc à tous les modes de connexion pouvant être considérés comme des connexions dites point à point telles que : connexion réseau sans fil entre un poste utilisateur et une borne d'accès Wifi.

On distingue deux types de trafic EAP :

- EAP over LAN (EAPOL) : entre le système à authentifier et le point d'accès.
- EAP over Radius : entre le point d'accès et le serveur d'authentification.

#### II.4.2.1.b) Les méthodes associées à EAP

Le protocole EAP ne propose pas qu'une seule méthode d'authentification c'est-à-dire qu'il utilise ces différents éléments pour identifier un client:

- ✓ Le login / mot de passe
- ✓ Le certificat électronique
- ✓ La biométrie
- ✓ Une puce (SIM)

Certaines méthodes combinent plusieurs critères (certificat et login/mot de passe …). En plus de l'authentification, EAP gère la distribution dynamique des clés de chiffrement. Parmi les méthodes de l'authentification les plus communes sur EAP on distingue :

- **EAP- TLS (*EAP Transport Layer Security*)**

EAP- TLS est implémenté chez de nombreux fabricants de matériel sans fils, il utilise deux certificats numériques, le serveur et le client s'authentifient mutuellement tout en cryptant les données échangées dans cette phase d'authentification. L'utilisation de clés publiques et privées des deux cotés permet de créer un tunnel sécurisé entre les deux parties, ce qui garantit l'intégrité des données. Avec ce principe le client ne fournit pas de mot de passe puisque le certificat permet l'authentification.

L'utilisation de certificat possède des avantages et des inconvénients. Ils sont souvent considérés comme plus sûrs que les mots de passe, cependant la distribution des certificats aux clients est une contrainte qu'il ne faut pas négliger.

- **EAP-TTLS (*EAP Tunneled Transport Layer Security*) et EAP-PEAP (Pro*tected EAP*)**

Ces deux méthodes sont assez similaires, elles s'appuient sur la confidentialité proposée par l'encapsulation dans un tunnel pour réaliser une authentification via login/mot de passe. On distingue deux phases d'authentification :

- ✓ Première phase : identification du serveur par le client en utilisant un certificat validé par une autorité de certification.
- ✓ Deuxième phase : identification du client par le serveur par login/password.

À l'issue de la première phase, le tunnel TLS chiffré s'établit, garantissant une grande confidentialité des échanges pour la deuxième phase où le client transmet ses éléments d'authentification (*login/password*) via le CHAP, PAP, MS-CHAP ou MS-CHAPv2 pour EAP-TTLS et MS-CHAPv2, token-card ou certificat (similaire à EAP-TLS) pour EAP-PEAP.

La différence entre EAP-PEAP et EAP-TTLS vient de la manière d'encapsuler les échanges lors de la deuxième phase. Pour EAP-PEAP, les données échangées entre le client et le serveur au travers du tunnel TLS sont encapsulées dans des paquets EAP. EAP-TTLS utilise des AVP (*Attribute-Values Pairs*) encapsulées dans des paquets EAP-TTLS.

L'avantage présenté par ces deux méthodes est que le client peut être authentifié par mot de passe, on supprime donc la complexité de gestion liée aux certificats caractéristique d'EAP-TLS, tout en proposant une authentification mutuelle.

- **EAP-MD5 (*EAP Message Digest 5-Challenge*)**

Cette méthode ne propose pas une authentification mutuelle, le client s'authentifie simplement en fournissant un couple login/mot de passe. Grace au mécanisme de challenge/ réponse, le serveur envoie un challenge au client, celui-ci renvoie son mot de passe associé au challenge, le serveur compare le résultat avec le mot de passe qu'il détient dans sa base de données, si le résultat est identique alors l'accès est autorisé, sinon il est refusé.

Le problème majeur de cette méthode réside dans le fait que les échanges ne sont pas chiffrés, en outre EAP-MD5 ne gère pas la distribution dynamique des clés WEP.

Le seul avantage de cette méthode est la simplicité : il est relativement facile de mettre en place une structure d'authentification basée sur cette méthode, celle-ci est d'ailleurs beaucoup utilisée pour des réseaux filaires ou la contrainte lié au chiffrage des échanges est moins forte que pour les réseaux wifi.

- **LEAP (*Light weight EAP*)**

C'est une implémentation assurant une authentification simple par mot de passe via une encapsulation sécurisée. Ce protocole est vulnérable aux attaques (cryptage MD5) sauf si l'utilisateur utilise des mots de passe complexes.

## II.5 LES PROTOCOLES DE TRANSPORT SECURISES

Un protocole de transport sécurisé permet de porter l'information d'un lieu à un autre suivant des règles prédéfinies sans que l'objet transporté ne soit en danger.

Étant donné que la majorité des réseaux utilisés à travers le monde sont de type TCP/IP et que le choix des entreprises se porte souvent vers ce type de réseau, nous présentons les protocoles sécurisées suivants :

### II.5.1 Le protocole ppp

Le 802.1x est une pyramide de protocoles dont la base est l'EAP. Pour bien comprendre l'EAP, il faut revenir à son origine : quand on lance une connexion à Internet via un modem téléphonique classique, l'ordinateur commence par établir une connexion avec une central téléphonique composé d'une batterie de modems eux-mêmes reliés à Internet. Ce central, mis en œuvre par un Fournisseur d'Accès à Internet (FAI) s'appelle un point de présence (*Point of Presence*, PoP). La connexion entre notre modem et l'un des modems du PoP repose sur un protocole très répandu : le Protocole de Point à Point PPP (*Point-to- Point Protocol*).

Le PPP définit notamment comment un client doit s'identifier : un mot de passe est attribué par le FAI, et ce client doit prouver qu'il le connaît. Si c'est le cas, le PoP lui autorise l'accès vers Internet, sinon, la connexion est interrompue.

### II.5.2 Le protocole PAP

Le Protocol PAP (*Password Authentication 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 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 à l'utilisateur et valide ou rejette la connexion.

PAP est le plus simple des protocoles d'authentification car il est très facile à implémenter. Mais étant donné que le mot de passe circule en clair sur le réseau, c'est aussi le moins sécurisé et il est donc fortement déconseillé car il ne procure aucune sécurité. 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.

### II.5.3 Le protocole CHAP

Le protocole CHAP (*Challenge Handshake Authentication Protocol*) est défini dans la RFC 1994. Le serveur commence par envoyer un « *défi* » au client (16 octets aléatoires) ainsi qu'un compteur qu'il incrémente à chaque fois qu'il lance un défi. Le client doit passer le compteur, son mot de passe et le défi au travers de l'algorithme de hachage MD5. Le résultat est une séquence de bits pseudo-aléatoires appelé le « *hash* » de 16 octets. Ce hash est envoyé au serveur, qui peut effectuer le même calcul et vérifier si son résultat concorde avec celui du client.

Cet algorithme permet d'éviter que le mot de passe soit transféré, et qu'un pirate ne répète une authentification réussie qu'il aurait enregistrée auparavant. Puisque le défi change à chaque authentification il ne permet pas au client de s'assurer de l'identité du serveur.

### II.5.4 Le protocole MS-CHAP

Ce protocole, souvent appelé MS-CHAP-v1, a été défini par Microsoft dans la RFC 2433. Il s'agit d'une variante de CHAP destinée à améliorer la sécurité. L'un des problèmes de CHAP est qu'il faut stocker le mot de passe en clair sur le serveur : sinon, il impossible de calculer le hash et de vérifier l'identité du client. Toute personne ayant accès à la base de données des utilisateurs peut donc voir les mots de passe de tout le monde. Pour éviter cela, MS-CHAP spécifie que le serveur doit stocker non pas le mot de passe, mais le résultat d'un hash sur ce mot de passe (selon un algorithme propriétaire de Microsoft).

Lorsque l'utilisateur saisit son mot de passe, celui-ci doit d'abord passer au travers du même algorithme de hash avant de suivre la procédure habituelle de CHAP. Malheureusement, MS-CHAP comporte des failles de sécurité dues au hash propriétaire de Microsoft, qui l'ont rendu rapidement obsolète : seuls quelques vieux systèmes Windows 95/98 l'utilisent encore.

### II.5.5 Le protocole MS-CHAP-v2

Suite à la découverte des failles de sécurité dans MS-CHAP, Microsoft a réagi en concevant cette version 2, définie dans la RFC 2759. Plus robuste, ce protocole fournit notamment un mécanisme d'authentification mutuelle : le serveur s'assure de l'identité du client, et vice versa, ce qui n'est pas le cas avec les méthodes d'authentification précédentes. Le MS-CHAP-v2 est largement utilisé dans les réseaux, Windows depuis la version Windows 2000.

## II.6 SECURITE APRES LA MISE EN PLACE DU RESEAU WIFI

Afin de conserver un niveau de sécurité satisfaisant du réseau sans fils, il est nécessaire d'appliquer les mêmes procédures que pour les réseaux filaires, à savoir :

- informer les utilisateurs : la sécurité d'un réseau passe avant tout par la prévention, la sensibilisation et la formation des utilisateurs.
- gérer et surveiller son réseau : la gestion et la surveillance d'un réseau sans fils peuvent s'effectuer à deux niveaux. La surveillance au niveau IP avec un système de détection d'intrusions classique (prelude, snort, ...) et la surveillance au niveau physique (sans fils) avec des outils dédiés (Kismet, ...).
- auditer son réseau : l'audit d'un réseau sans fils s'effectue en deux parties :
  - ✓ Un audit physique pour s'assurer que le réseau ne diffuse pas d'informations dans des zones non désirées et qu'il n'existe pas de réseau sans fils non désiré dans le périmètre à sécuriser.
  - ✓ Un audit informatique pour mesurer l'écart entre le niveau de sécurité obtenu et celui désiré.

La sécurité d'un réseau sans fils comprend aussi sa gestion. Gérer un réseau sans fil nécessite de s'appuyer sur une équipe ayant une bonne connaissance des réseaux et de la sécurité des systèmes d'information.

## II.7 CONCLUSION

Un réseau sans fils peu être installé dans une entreprise à l'insu du service informatique, pour cela il suffit à un employé de brancher un point d'accès sur une prise réseau pour que toutes les communications du réseau soient rendues « publiques » dans le rayon de couverture du point d'accès.

Il est donc essentiel de protéger le réseau sans fil, même si on considère que les données qui y circulent n'ont rien de confidentiel. En effet un réseau sans fils non protégé et sans aucun effort de configuration, peut permettre à n'importe quel utilisateur du voisinage d'utiliser la connexion Internet et éventuellement lancer un certain nombre d'attaques.

## III.1 INTRODUCTION

Le but de ce chapitre est de présenter le serveur d'authentification RADIUS qui permet aux opérateurs d'authentifier des utilisateurs, de leur autoriser certains services et d'assurer la sécurité. En suite nous allons introduire les annuaires utilisés par ce serveur et nous donnerons un aperçu sur Windows Server 2008.

## III.2 LE PROTOCOLE AAA

AAA (*Authentication, Authorization, Accounting*) signifie : authentification, autorisation et compte.

- **Authentication**

Processus permettant de garantir que la personne qui tente d'accéder au réseau dispose d'un compte valide. Le mot de passe de l'utilisateur est comparé avec les entrées figurant dans une base de données centrale.

- **Authorization**

Permet à l'exploitant du réseau de définir les services réseau dont les utilisateurs finaux peuvent bénéficier .Un utilisateur peut par exemple demander à avoir une certaine bande passante, le serveur AAA lui autorisera ou non cette demande.

- **Accounting**

Le serveur AAA a la possibilité de collecter des informations sur l'utilisation des ressources, ceci permet à un opérateur de facturer un utilisateur suivant sa consommation. Ces utilisateurs clients sont hébergés sur des routeurs ou sur des serveurs d'accès au réseau.

L'*accounting* se base sur deux types de paquets principaux : *Accounting Start* et *Accounting Stop*, une session est définie comme l'intervalle entre un Start et un Stop. Le paquet *Accounting Start* émis par le client Radius après connexion effective de l'utilisateur suite à une phase d'identification réussie contient des données de base : nom d'utilisateur, adresse IP affectée, date et heur de connexion, type de connexion, et type de service.

Quand l'utilisateur se déconnecte du service, un paquet *Accounting Stop* est envoyé avec le même identificateur de session, le serveur Radius peut alors clore la session et journaliser la déconnection, souvent avec un grand nombre de paramètres dans le paquet Stop : temps de connexion, type d'utilisation, nombre de paquets et d'octets échangés selon les divers protocoles, et éventuellement des informations plus confidentielles sur les sites visités ou contenues échangés.

La figure III.1 représente l'architecture AAA :

## III.3 LE PROTOCOLE RADIUS

### III.3.1 Définition

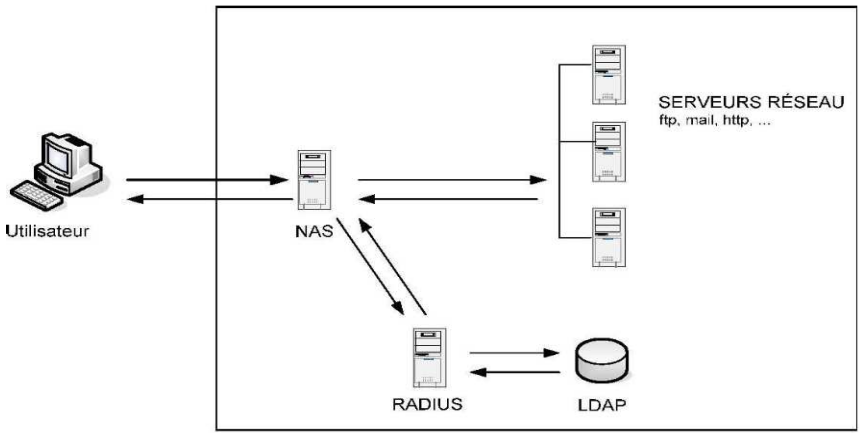
Le protocole RADIUS (*Remonte Authentication Dial-In User Service*), est actuellement utilisé pour faire de l'AAA avec des utilisateurs qui se connectent via des modems téléphoniques à Internet. Il envoie des informations au serveur d'accès (NAS) qui permet de les authentifier (*login/password*). Si l'utilisateur est correctement authentifié, le serveur lui permet l'accès au réseau, sinon la connexion est rejetée.

RADIUS a été conçu pour supporter un nombre ilimité d'équipements et d'utilisateurs. Actuellement, les opérateurs doivent pouvoir rendre des services et authentifier des milliers d'utilisateurs utilisant des technologies différentes. Ils doivent aussi être capables de rendre des services à des utilisateurs venant d'opérateurs différents, de préférence de façon sécurisée.

### III.3.2 Principe

Le principe de fonctionnement de ce protocole réside dans l'utilisation d'un secret qui permet d'authentifier les transactions et d'effectuer le cryptage du mot de passe, ceci à travers de nombreux mécanismes, les plus courants étant PAP, CHAP, MS-CHAP… . Contrairement au protocole TACACS +, il n'est possible de chiffrer que le mot de passe au sein de la trame.

Le protocole repose sur la transmission d'attribut Clef ou Valeur. Ces attributs permettent d'échanger un nombre illimité d'informations entre le client et le serveur (Password, Adresse MAC, …), et permettent donc aux principaux équipementiers de développer leurs propres attributs. La mise en place de RADIUS repose principalement sur l'utilisation d'un annuaire ou base de données, d'un serveur maître et d'un serveur client. La Figure III.2 montre un exemple courant de l'implémentation de serveur.




## III. 3.3 Les différents types de paquets

Lorsque le poste utilisateur transmet les informations nécessaires pour l'authentification (login, mot de passe, adresse MAC,…) au client RADIUS via une liaison PPP, l'authentification RADIUS se déroule suivant un dialogue entre le NAS et le serveur, qui met en jeu six types d'échanges; chacun est véhiculé au moyen d'un paquet spécifique en utilisant le protocole UDP comme l'illustre la figure III.3:

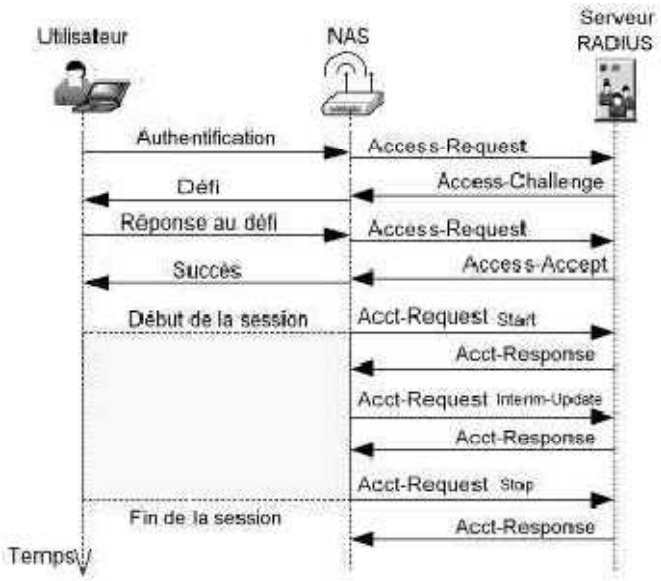



**Figure III.3**: Un scénario de communication RADIUS

- **Access-Request**

Est envoyé par le NAS vers le serveur lorsqu'un client doit être authentifié pour accéder au réseau. Il contient l'ensemble des attributs et informations de l'utilisateur (ID du client, mot

de passe, numéro du port,…). Si un mot de passe est présent, il sera haché en utilisant le mécanisme MD5.

- **Access-Challenge**

Après réception d'un paquet *Access-Request*, le serveur peut renvoyer un paquet *Access-Challenge* qui a pour but de demander d'autres informations et de provoquer l'émission d'un nouveau paquet *Access-Request* par le NAS. *Access-Challenge* sera toujours utilisé avec EAP puisqu'il permettra au serveur de demander un certificat ou un mot de passe au poste de travail.

- **Access-Accept**

Est envoyé au NAS si l'utilisateur est authentifié et donc a accès au réseau.

- **Access-Reject**

Est envoyé au NAS si l'utilisateur n'est pas autorisé à accéder au réseau. Ce paquet peut également transporter divers attributs comme : un message d'erreur à présenter à l'utilisateur.

- **Accounting-Request**

Est envoyé par le NAS pour indiquer au serveur le début (type Start) ou la fin (type Stop) d'une session. Il contient toutes sortes d'attributs donnant des informations au sujet de la session : le volume total de données téléchargées pendant la session en nombre d'octets (*Acct-Input-Octets*) ou en nombre de paquets (*Acct-Input Packets*), la durée totale de la session en secondes (*Acct-Session-Time), User-Name*, etc. Ce paquet peut éventuellement être envoyé régulièrement au cours de la session.

- **Accounting-Response**

Est renvoyé par le serveur pour indiquer qu'il a bien reçu le paquet *Accounting-Request*.

### III.3.4 Format d'un paquet radius

Les paquets RADIUS se présentent sous le format suivant :

| Code (Octets) | Identifiant (Octets) | Longueur (Octets) | Authentificateur (Octets) | Attributs et valeurs (Octets) |
|---|---|---|---|---|
| 1 | 1 | 2 | 16 | N |

**Signification des différents champs**

- **Code :** indique le type du paquet RADIUS : *Access-Request, Access-Challenge, Access-Accept, Access-Reject, Accounting-Request ou Accounting-Response.*
- **Identifiant (ID) :** est inclus dans chaque requête, il s'agit d'un simple compteur qui identifie le paquet. Ceci permet de savoir à quelle requête correspond une réponse RADIUS (car avec le protocole UDP, l'ordre des paquets peut changer entre l'émetteur et le récepteur).
- **Longueur :** Longueur du paquet en octets en comptant l'en-tête RADIUS et les attributs.
- **Authentificateur (*Authenticator*) :** Ce champ est très important du point de vue de la sécurité, il permet :
  - ✓ Au client d'authentifier la réponse du serveur.
  - ✓ De contrôler l'intégrité du paquet, pour s'assurer que ce dernier n'a pas été modifié par un pirate entre l'émetteur et le récepteur.
  - ✓ De masquer le mot de passe en créant l'attribut User-Password.
- **Les attributs**

Les attributs constituent le principe le plus important du protocole Radius. La bonne compréhension de leur signification et de leur rôle est indispensable pour tirer le meilleur parti de RADIUS. Chaque attribut possède un numéro auquel est associé un nom, et leur valeur peut correspondre à l'un des types suivants :

- ✓ adresse IP (4 octets).
- ✓ date (4 octets).
- ✓ chaîne de caractères (jusqu'à 255 octets).
- ✓ entier (4 octets).
- ✓ valeur binaire (1 bit).
- ✓ valeur parmi une liste de valeurs (4 octets).

Dans la terminologie Radius, ces attributs et leur valeur sont appelés ***Attributes Value-Pair*** (AVP).

Le format de chaque attribut est très simple. Chaque attribut précise son type, sa longueur et sa valeur :

| Type | Longueur | Valeur |
|---|---|---|
| 1 octet | 1 octet | 0 à 253 octets |

### III.3.5 Les limites du protocole radius

Le protocole RADIUS possède plusieurs failles se trouvant à l'origine de problèmes de sécurité:

- ✓ La technique de protection "*UserPassword*" ne devrait pas utiliser la fonction MD5 comme primitive de chiffrement. Car MD5 utilise l'authentification à sens unique, le point d'accès authentifie le client, mais le client n'authentifie pas le point d'accès (pas d'authentification mutuelle).
- ✓ Le paquet "*Access-Request*" n'est pas authentifié.
- ✓ Beaucoup d'administrateurs choisissent des secrets partagés identiques pour différents clients. De nombreuses implémentations clientes limitent le nombre de caractères possibles du secret partagé.

## III.4 DIAMETER

Le nom du protocole DIAMETER signifie diamètre qui est le double du rayon (RADIUS en anglais), ce protocole est un successeur de RADIUS. Il permet aux opérateurs d'authentifier des utilisateurs, de leur autoriser certains services et de collecter des informations sur l'utilisation des ressources. Il est mis en place pour satisfaire les nouveaux besoins suscités par la mobilité. Il permet aux opérateurs d'authentifier un utilisateur ayant souscrit un abonnement auprès d'un autre opérateur.

Il est constitué d'un protocole de base qui définit le format des messages, la manière dont ils sont transportés, les messages d'erreurs ainsi que les services de sécurité que toutes les implémentations doivent supporter. À ce protocole de base s'ajoutent les applications : Mobile IP, NAS et CMS.

- L'application Diameter Mobile IPv4 permet de faire de l'AAA avec un utilisateur utilisant Mobile IPv4.

- L'application Diameter NAS permet l'accès au réseau.
- L'application Diameter CMS permet de protéger les échanges Diameter au niveau applicatif entre serveurs ou entre un serveur et son client.

## III.5 SERVEUR DHCP

### III.5.1 Définition

Le serveur DHCP (*Dynamic Host Configuration Protocol*) permet la gestion et la distribution des adresses IP dynamiquement à un ordinateur qui se connecte sur un réseau, son but principal étant la simplification de l'administration d'un réseau.

### III.5.2 Fonctionnement du protocole DHCP

Il faut dans un premier temps un serveur DHCP qui distribue des adresses IP, cette machine va servir de base pour toutes les requêtes DHCP et doit avoir une adresse IP fixe. Quand une machine démarre, elle n'a aucune information sur sa configuration réseau et l'utilisateur ne doit rien faire de particulier pour trouver une adresse IP. Pour se faire, la technique utilisée est le broadcast : pour trouver et dialoguer avec un serveur DHCP, la machine va émettre un paquet de broadcast sur 255.255.255.255 avec d'autres informations comme le type de requête et les ports de connexion sur le réseau local.

Lorsque le serveur DHCP reçoit le paquet de broadcast, il renverra un autre paquet de broadcast contenant toutes les informations requises pour le client.

Il existe plusieurs types de paquets DHCP susceptibles d'être émis soit par le client pour le serveur, soit par le serveur vers un client :

- **DHCPDISCOVER:** pour localiser les serveurs DHCP disponibles.
- **DHCPOFFER :** réponse du serveur à un paquet DHCPDISCOVER, qui contient les premiers paramètres.
- **DHCPREQUEST** : requête diverse du client pour par exemple prolonger son bail.
- **DHCPACK** : réponse du serveur qui contient des paramètres et l'adresse IP du client.
- **DHCPNAK** : réponse du serveur pour signaler au client que son bail a expiré ou si le client annonce une mauvaise configuration réseau.
- **DHCPDECLINE** : le client annonce au serveur que l'adresse est déjà utilisée.
- **DHCPRELEASE** : le client libère son adresse IP.

- **DHCPINFORM** : le client demande des paramètres locaux, il a déjà son adresse IP.

## III.6 LE SERVEUR DNS

Le service DNS (*Domaine Name System*) permet de faciliter et de standardiser le processus d'identification des ressources connectées aux réseaux informatiques, et il associe un nom à une adresse IP à chaque machine connectée au réseau.

Pour déployer un serveur DNS dans un réseau, il faut définir l'adresse du réseau. Pour des organisations désirant donner un accès public à leur domaine, il faut acheter un nom de domaine chez un prestataire de services tout en assurant son unicité sur internet. Dans un réseau subdivisé en plusieurs sous réseaux, il doit y avoir un serveur DNS primaire par zone (sous réseau) et plusieurs serveurs secondaires sur lesquels on effectue des copies régulières des informations primaires pour des mesures de sécurité. Dans ce cas, une configuration des sous-domaines s'impose.

## III.7 IMPLEMENTATION DU SERVEUR RADIUS

### III.7.1 NPS (*Network Policy Server*)

NPS est le service d'authentification internet sur Windows 2008 (sous le nom de serveur IAS avec Windows 2000 et 2003) .C'est une implémentation Microsoft du serveur RADIUS : Le service NPS 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 fil, accès par commutateur d'authentification, accès par connexion à distance et VPN). En tant que proxy RADIUS, le service NPS peut envoyer les messages d'authentification et de gestion de comptes à d'autres serveurs RADIUS.

### III.7.2 NAP *(Network Access Protection)*

NAP est une nouvelle protection de l'accès réseau dans Windows server .Il permet de créer des stratégies d'intégrité de la sécurité basées sur des déclarations d'intégrité (comme des mises à jour antivirus, pare feu): par exemple il peut demander que les entités du réseau possèdent les dernières mises à jour du système d'exploitation et les dernières fiches de signatures antivirus. En fonction de cela, les entités auront plus ou moins de droits sur le réseau. Ces entités sont appelés clients NAP

## III.8 ANNUAIRES

Un annuaire est une bibliothèque mise à jour régulièrement qui regroupe des informations (nom, adresse, coordonnées) sur les membres d'une association, d'une entreprise ou d'un organisme professionnel, ou sur les abonnés à un service.

### III.8.1 LDAP *(Lightweight Directory Access Protocol)*

LDAP est normalisé par l'IETF, il s'agit d'un protocole d'interrogation d'annuaire qui est allégé par rapport à la norme X500, mais sa mise en œuvre est très lourde. LDAP regroupe les données d'une entité au même endroit, c'est un annuaire fédérateur sur lequel la plupart des applications récentes s'appuient: les outils de messageries, les actifs du réseau (proxy, firewall…), les progiciels de gestion et les intranets.

La majorité des logiciels utilisent LDAP pour l'authentification car il propose des mécanismes pour gérer l'authentification. Plusieurs méthodes sont possibles en fonction du niveau de sécurité désiré :

- ✓ La connexion anonyme est généralement limitée à la consultation de parties restreintes de l'annuaire.
- ✓ L'authentification par login /mot de passe.
- ✓ L'authentification par login/mot de passe avec hachage de ce dernier.
- ✓ L'authentification par login /mot de passe sur TLS avec un tunnel TLS entre le client et l'application et un tunnel TLS entre l'application et l'annuaire.
- ✓ L'authentification par certificat X509.

### III.8.2 Active Directory

#### III.8.2 .1 Présentation du service Active Directory

Active Directory (AD) est un annuaire système hiérarchique qui :

- ✓ Permet de localiser, rechercher et gérer des ressources représentées par des objets de l'annuaire.
- ✓ Offre des mécanismes de sécurité pour protéger ces informations.
- ✓ permet de gérer des ressources liées à la gestion du réseau (domaines, comptes utilisateurs, stratégies de sécurité… etc.).

L'active Directory est capable d'interagir avec des clients et des serveurs LDAP d'autres origines.

Certains produits Microsoft sont installés par défaut (ou fortement conseillés lors de l'installation) : DNS, serveur Web. D'autres bénéficient d'une forte intégration avec AD (serveur de courrier Exchange, ISA Server). Active Directory centralise l'authentification et le contrôle d'accès peut être défini sur chaque objet de l'annuaire.

Le service Active Directory (AD) permet une gestion centralisée. Cela permet d'ajouter, de retirer et de localiser les ressources facilement.

Ainsi, nous avons :

- **Une administration simplifiée :** Active Directory offre une administration de toutes les ressources du réseau d'un point unique. Un administrateur peut se connecter sur n'importe quel ordinateur pour gérer ses ressources.
- **Une mise à l'échelle :** Active Directory permet de gérer des millions d'objets répartis sur plusieurs sites si cela est nécessaire.
- **Un support standard ouvert :** Active Directory utilise DNS pour nommer et localiser des ressources, ainsi les noms de domaine Windows 2008 sont aussi des noms de domaine DNS.

### III.8.2.2 Structure d'Active Directory

La structure d'Active Directory est hiérarchique, elle se décompose comme suit :

#### III.8.2.2.a Structure logique

❖ **Les Domaines**

Le domaine est l'unité de base chargée de regrouper les objets qui partagent un même espace de nom. Un domaine doit reposer sur un système DNS, supportant les mises à jour dynamiques.

❖ **Unité organisationnelle (OU)**

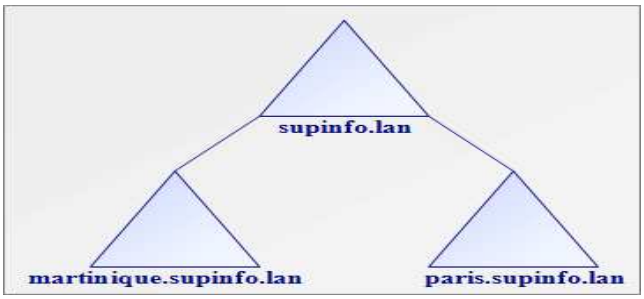
Une unité d'organisation est un objet conteneur utilisé pour organiser les objets au sein d'un domaine. Il peut contenir des comptes d'utilisateurs, des groupes, des ordinateurs, des imprimantes ainsi que d'autres unités d'organisation. L'unité d'organisation permet de faciliter la délégation de pouvoir selon l'organisation des objets.

❖ **Les Arborescences**

Une **arborescence** est un ensemble de domaines partageant un nom commun, le premier domaine installé est le domaine racine de la forêt. Au fur et à mesure que des domaines lui

sont ajoutés, cela forme la structure de l'arborescence ou la structure de la forêt.

Par exemple, supinfo.lan est le domaine parent du domaine paris.supinfo.lan et du domaine martinique.supinfo.lan.




❖ **Forêt**

C'est un groupement d'un ou plusieurs arbres qui ont des noms disjoints (par exemple: laboratoire-microsoft.org et supinfo.com). Tous les arbres d'une forêt partagent le même schéma commun et le même catalogue, mais ont des structures de noms différentes. Les domaines d'une forêt fonctionnent indépendamment les uns des autres, mais les forêts permettent la communication d'un domaine à l'autre.

❖ **Objet**

Représente une ressource du réseau qui peut-être par exemple un ordinateur ou un compte utilisateur.

❖ **Classe**

Description structurelle d'objets tels les comptes d'utilisateurs, ordinateurs, domaines, ou unités organisationnelles.

### III.8.2.2.b Structure Physique

❖ **Contrôleur de domaine**

Un contrôleur de domaine est un ordinateur chargé de stocker l'ensemble des données et de gérer les interactions entre les utilisateurs et le domaine. Il assure la propagation des modifications faites sur l'annuaire et aussi l'authentification et l'ouverture des sessions des utilisateurs, ainsi que les recherches dans l'annuaire. Un domaine peut posséder un ou plusieurs contrôleurs de domaine. Dans le cas d'une société constituée de plusieurs entités dispersées géographiquement, on aura besoin d'un contrôleur de domaine dans chacune de ses entités.

❖ **Sites**

Un site est une combinaison d'un ou plusieurs sous réseaux connectés entre eux par une liaison à haut débit fiable (liaison LAN). Définir des sites permet à Active Directory d'optimiser la duplication et l'authentification afin d'exploiter au mieux les liaisons les plus rapides.

## III.9 SERVEUR 2008

### III.9.1 Définition

Microsoft Windows Server 2008 est un système d'exploitation de Microsoft orienté serveur, il est le successeur de Windows Server 2003 et le prédécesseur de Windows Server 2008 R2. Il a été pensé par Microsoft pour offrir une plateforme souple et complète afin de répondre aux besoins des entreprises.

### III.9.2 Les différentes éditions de Windows server 2008

Microsoft Windows Server 2008 est disponible sous différentes éditions. Il existe neuf versions différentes de ce système d'exploitation :

- ✓ Windows Server 2008 Edition Standard (x86 et x64) avec ou sans HyperV.
- ✓ Windows Server 2008 Edition Enterprise (x86 et x64) avec ou sans HyperV.
- ✓ Windows Server 2008 Edition Datacenter (x86 et x64) avec ou sans HyperV.
- ✓ Windows HPC Server 2008.
- ✓ Windows Web Server 2008 (x86 et x64).
- ✓ Windows Storage Server 2008 (x86 et x64).
- ✓ Windows Small Business Server 2008 (x64) pour les PE.
- ✓ Windows Essential Business Server 2008 (x64) pour les PME.
- ✓ Windows Server 2008 pour Systèmes Itaniumbased.

Elles sont toutes disponibles en version X86 (32 bits et 64 bits) sauf la version Itanium qui est compatible avec les processeurs IA64 dont l'architecture est optimisée pour le traitement des bases de données et des applications *Line of Business* (LOB). La version R2 de Windows Server 2008 ne peut être installée que sur une version 64 bits.

### III.9.3 Présentation des rôles

Un rôle regroupe un ou plusieurs composants permettant de réaliser une tâche spécifique sur le réseau, il permet de simplifier la logique d'administration.

Dans Windows Server 2008, Microsoft a défini 17 rôles par défaut. Disposant d'une architecture extensible, de nouveaux rôles apparaissent avec le temps. Un service de rôle est un sous-ensemble d'un rôle donné.

Dés qu'un rôle se compose de plusieurs services pouvant fonctionner de manière autonome, on doit décider quel service de rôle installer. Ces derniers simplifient l'administration et réduisent la surface d'attaque du serveur.

Par défaut, aucun rôle n'est installé. Pour ce faire, on procède soit de manière manuelle par l'intermédiaire de l'administrateur ou bien automatiquement lors de l'installation d'un autre rôle ou d'une fonctionnalité.

## III.10 CONCLUSION

Dans ce chapitre nous avons présenté une méthode de sécurité qui utilise l'authentification. Le fonctionnement de cette méthode réside dans l'utilisation d'un secret partagé qui permet d'authentifier les transactions et d'effectuer le cryptage du mot de passe. Dans le chapitre suivant nous allons implémenter le protocole 802.1x sur Windows serveur 2008.

# IV.1 INTRODUCTION

Une grande partie des attaques et des problèmes de sécurité rencontrés dans un réseau informatique a une source intérieure au réseau. Donc il est nécessaire de contrôler l'accès physique au LAN en implémentant une méthode de sécurisation tel qu'une authentification **802.1x** sur un serveur **RADIUS**. Lorsque le client veut accéder au point d'accès ou au Switch qu'on aura configuré comme un client RADIUS, il doit utiliser **la norme 802.1x**.

# IV.2 INFRASTRUCTURE

## IV.2.1 Organisme d'accueil

Notre travail a été réalisé au sein d'une entreprise 2intparteners de Tizi-Ouzou, qui est organisé suivant ces organigrammes.

## IV.2.2 Organigramme de l'entreprise

### IV.2.3 Organigramme du service technique

Notre travail est rattaché au service sécurité qui utilise l'authentification 802.1x comme mécanisme de sécurité.

Les entités principales intervenant dans le mécanisme d'authentification **802.1x** sont :

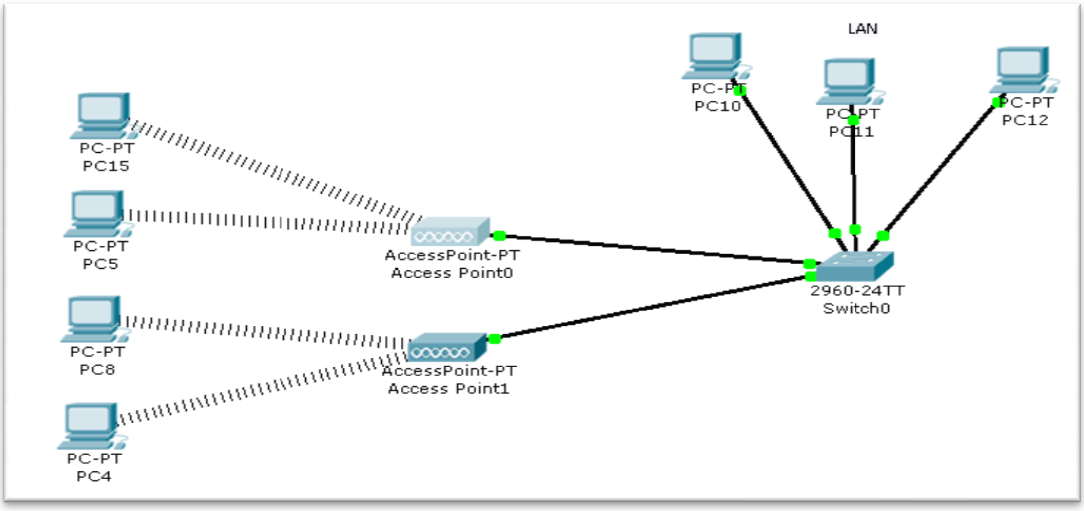
- **Des clients : 50 PC** (dans notre cas les machines clients fonctionnent sous Windows 7) avec une liaison Wifi avec adressage ipv4 automatique.

- **Un authentificateur : 03 Point d'Access** qui seront les clients RADIUS « NAS »**.**
  Adresses IP : 192.168.1.1, 192.168.1.2, 192.168.1.3
  Masque de sous réseau : 255.255.255.0
  Passerelle par défaut : 192.168.1.200
  Serveur DNS : 192.168.1.200

- **Un serveur d'authentification (**Le serveur Radius NPS sous Windows server 2008).
  Adresse IP : 192.168.1.200
  Masque de sous réseau : 255.255.255.0
  Passerelle par défaut : 192.168.1.4 (adresse du Switch)
  Serveur DNS : 192.168.1.200

### IV.2.4 Infrastructure existante :

Notre entreprise compte cinquantes ordinateurs, trois points déaccès et un switch Cisco Catalyste 2960.




### IV.2.5 Infrastructure proposé :

- 

## IV.3 EXPLICATION

Le client A demande à se connecter au réseau local via le point d'Accès Wifi capable de faire l'authentification **802.1x** (Client NAS), pour cela il demande à s'authentifier en envoyant des échanges d'informations spécifiques (login, mot passe…) qui sont appelés flux EAPOL (EAP over LAN) à travers le port non contrôlé (*Uncontrolled*) du commutateur qui permet à son tour de les transmettre au serveur d'authentification RADIUS sous forme de

EAP over RADIUS. Celui-ci vérifiera si le client a le droit ou non d'accéder au réseau selon les données d'authentifications présentes dans son annuaires Active Directory. Une fois que le client a prouvé son identité, le port contrôlé (*controlled*) change d'état et devient « *ouvert* » puis laisse tous le trafic réseau passer par ce port. Si la réponse du serveur d'authentification est négative, le port reste « *bloqué* » dans son état initial. Le processus d'authentification peut être retenté plusieurs fois. Au bout d'un nombre d'essais défini, l'authentification échoue et l'accès au réseau est bloqué.

Lorsque le client A se déconnecte, il envoie un message de fin (LOGOFF) qui va permettre au commutateur de passer le port en mode contrôlé et ainsi attendre l'authentification d'un autre client.

## IV.4 CONFIGURATION DES ENTITES

### IV.4.1 Le serveur d'authentification Radius (NPS)

Comme définit dans le chapitre précédent, NPS est le Service d'authentification Internet sur Windows server 2008. Il joue le rôle d'intermédiaire entre le serveur d'accès distant et le contrôleur de domaine.
Après avoir installé Windows server 2008 avec les paramètres par défauts, quelques modifications s'imposent :

- En premier lieu il faut s'assurer que le Switch soit capable de reconnaitre le serveur RADIUS NPS, donc on doit attribuer à notre serveur une adresse IP statique et s'assurer que son nom DNS est mis à jour, en envoyant un « ping » au serveur à partir d'un autre ordinateur du réseau et activer le DHCP.
- Ensuite on installe Active Directory qui contient les données concernant les différents comptes des utilisateurs de l'entreprise.
- On installe l'autorité de certification et on génère le certificat pour le serveur d'authentification. Puis, on procède à la création d'un compte utilisateur et lui donner un droit d'accès et on l'associe à un groupe qu'on aura créé dans l'annuaire Active Directory et cela pour chaque utilisateur qu'on veut authentifier.
- Et enfin on procède à la configuration du serveur NPS.

#### IV.4.1.1 L'installation et la gestion d'Active Directory Service

Pour installer Active Directory on sui les étapes suivantes :

1. Utiliser l'utilitaire « **Gestionnaire de serveur** »

Dans le menu ***démarrer*** ; on clique sur ***Outil d'administration*** puis ***Gestionnaire de serveur.***

- On clique sur ***Rôles*** puis ***Ajouter des rôles***, puis ***Ignorer cette page par default*** et ***suivant***.
- On coche ***services de domaine Active Directory*** puis ***suivant***, ***suivant*** et ***installer***.l'installation est en cours:
-

A la fin de l'installation la fenêtre suivante s'affiche et on clique sur ***fermer***.

2. Utiliser l'assistant « **dcpromo** » :

- On clique sur ***démarrer*** puis ***exécuter.***
- Exécution de la commande ***dcpromo***, l'assistant de l'installation démarre.

- Dans l'Assistant ***installation des services de domaine Active Directory,*** on clique sur **suivant.**

- On choisi une configuration de déploiement : **« Créer un domaine dans une nouvelle forêt »** puis on clique sur **Suivant.**
- On nomme le domaine racine de la forêt.

- On définit le niveau fonctionnel de la forêt et on clique sur ***suivant***.

- Démarrage de l'installation d'Active Directory :

- On clique sur ***redémarrer à la fin de l'opération*** pour redémarrer la machine et prendre en compte les modifications effectuées par l'assistant Active Directory.

**Remarque :** quand on installe Active Directory, le serveur doit être relié au Switch ou à un matériel informatique.

### IV.4.1.1 .a) Création d'une unité d'organisation

La création d'une unité organisationnelle s'effectue par la console Utilisateurs et Ordinateurs Active Directory pour cela **:**

- On clique sur ***Démarrer*** puis ***Outils d'administration*** et ***Utilisateurs et Ordinateurs Active Directory.***

- Dans le volet de gauche, on clique avec le bouton droit de la souris sur notre Nom de domaine puis on pointe sur ***Nouveau*** et ***unité d'organisation***.

- On tape «**UMMTO**» dans la zone de Nom, puis on clique sur **OK**.

### IV.4.1.1 .b) Création d'un compte d'utilisateur Active Directory

Sur le dossier «**UMMTO**», on fait un click droit avec la souris puis ***un nouveau utilisateur.***

- On remplie les zones ***« Nom »*** - ***« Prénom »*** et on note que ceux-ci s'affichent automatiquement dans la zone « ***Nom complet*** ». On remplie ensuite la zone ***« Nom d'ouverture de session d'utilisateur ».***
- On entre le mot de passe dans les zones ***« Mot de passe »*** ainsi que les options concernant le compte, puis sur ***terminé***.

Tous les utilisateurs créés seront affichés dans le volet droit comme le montre la fenêtre suivante :

- On édite les propriétés du client (USER1 par exemple) pour autoriser l'accès distant en sélectionnant ***Autoriser l'accès*** dans la section *Autorisation d'accès distant* sous l'onglet *Appel entrant* et on valide par **OK.**

### IV.4.1.1 .c) Création d'un groupe d'utilisateurs

Nous pouvons maintenant créer un groupe d'utilisateurs qui contiendra les utilisateurs.

- Sur le dossier ***UMMTO*** on fait un click droit puis ***nouveau groupe*** que l'on appellera « ***ELN*** ».

- Dans la boite de dialogue ***Nouvel Objet-Groupe***, on entre le Nom du groupe **« ELN »** puis on clique sur ***OK***.

Dans la fenêtre apparue, le groupe crée s'affiche :

**IV.4.1.1 .d) Ajouter les utilisateurs au groupe de travaille ELN**

- On sélectionne les utilisateurs et avec un click droit de la souris on clique sur **Ajouter à un groupe.**

- On introduit le nom du groupe auquel on veut intégrer les utilisateurs et on clic sur ***OK***.

Une fois qu'on a terminé l'installation d'AD qui contient les données concernant les différents comptes des utilisateurs de l'entreprise, on procède à l'activation du **service de stratégie et d'accès réseau.**

### IV.4.1.2 l'installation du service de stratégie et d'accès réseau

Les services de stratégie et d'accès réseau offrent plusieurs méthodes pour fournir aux utilisateurs une connectivité réseau locale et à distance, pour connecter des segments réseau et pour permettre aux administrateurs réseau de gérer de façon centralisée les accès au réseau et les stratégies de contrôle d'intégrité des clients.

Avec les Services de stratégie et d'accès réseau, on peu déployer des accès sans fils protégés 802.11 et des serveurs et des proxys RADIUS.

- Sur la page Rôles de serveurs, on sélectionne **Services de stratégie et d'accès réseau** puis on clique sur **Suivant**.

- On sui les étapes pour l'installation en cliquant sur **suivant**
- On coche le **service Serveur NPS** et on clique sur **installer**.

Une fois l'installation terminée la fenêtre suivante s'affiche :

### IV.4.1.3 Installation des services de certificats Active Directory

Les services de certificats Active Directory fournissent des services personnalisables pour la création et la gestion de certificats qui sont utilisés dans les systèmes de sécurité logiciels employant des technologies de clé publique. Les organisations peuvent utiliser des services de certificats AD pour améliorer la sécurité en liant l'identité d'une personne, d'un périphérique ou d'un service à une clé privé correspondante.

Les applications prises en charge par les services de certificats AD incluent les réseaux sans fils sécurisés.

- On ouvre une session en tant que membre du groupe Administrateurs de l'entreprise.
- On clique sur **Démarrer**, sur **Outils d'administration**, puis sur **Gestionnaire de serveur**. La console Gestionnaire de serveur s'ouvre.
- Dans le volet gauche, on clique sur **Rôles** puis, dans le volet d'informations, on clique sur **Ajouter des rôles**.
- Sur la page **Sélectionnez des rôles de serveurs**, on clique sur **Services de certificats Active Directory**, puis sur **Suivant**.

- On coche **Autorité de certification**, puis **Suivant**.

- Sur la page **Spécifier le type d'installation**, on coche **Entreprise**, puis **Suivant**.

- Sur la page **Spécifier le type d'autorité de certification**, on clique sur **Autorité de certification racine**, puis sur **Suivant**.

- Sur la page **Configurer la clé privée**, on vérifie que **Créer une nouvelle clé privée** est sélectionné, puis on clique sur **Suivant**.

- Sur la page **Configurer le chiffrement pour l'autorité de certification**, on modifie les paramètres selon nos besoins. Notons que la **Longueur de la clé en caractères** par défaut est 2048. En fonction de la taille et du trafic réseau, on peut modifier la taille de la longueur de clé en caractères et on clique sur **Suivant**.

- Sur la page **Configurer le nom de l'autorité de certification**, on modifie le nom commun pour l'autorité de certification en fonction de nos besoins, puis on clique sur **Suivant**.

- Sur la page **Période de validité du certificat**, **Sélectionnez la période de validité du certificat généré par cette Autorité de certification** on tape le nombre et on sélectionne l'unité de temps (années, mois, semaines ou jours) qui déterminent la date d'expiration des certificats délivrés par l'autorité de certification. La valeur par défaut de cinq années est recommandée. On clique sur **Suivant**.

- On spécifie l'emplacement du dossier contenant ces éléments et on clique sur **Suivant**.

- Une fenêtre de confirmation s'affiche avec tous les paramètres qu'on a configurés, on clique sur **Installer** puis **Terminé.**

### IV.4.1.4 Lancement du SERVEUR NPS

Il est nécessaire que le serveur d'accès à distance soit configuré en tant que client Radius du serveur NPS considéré.

- Dans **Serveur NPS**, on clique sur **NPS (Local)** puis dans la section de **détail** on sélectionne **Serveur Radius pour les connexions câblées ou sans fil 802.1X** dans la zone **Configuration standard** et on clique sur **Configurer802.1X**.

- Sur la page suivante on sélectionne le type de connexion pour laquelle on veut créer une stratégie, ici « Connexion sans fil sécurisées ».

- On saisie le nom de notre stratégie avant de cliquer sur **Suivant** :

- Sur la page **Configurer les méthodes d'authentification** est sélectionné par défaut **carte à puce ou autre certificat**, on modifie ce choix et on sélectionne PEAP puis on clique sur **Suivant**.

- On ajoute un groupe d'utilisateurs et on clique sur **ok** :

- Dans la page **configurer un réseau local virtuel (VLAN),** on clique sur **configurer** puis **suivant,** la fenêtre suivante s'affiche **:**

Une fois la configuration terminé, on peu y accéder à tout moment, le « **Tree View** » à gauche nous permet de visualiser les stratégies, clients radius et tous autre option.

### IV.4.1.5 Configuration du serveur RADIUS NPS

#### A) Ajouter un nouveau client RADIUS

La configuration d'un nouveau client RADIUS se fait comme suite :

- Dans la fenêtre de NPS, on clique sur ***client et serveur RADIUS***, on fait un clic droit sur ***client RADIUS***, ***nouveau*** et on remplie la fiche de renseignement.

Le secret partagé est : Passw0rd, ce mot de passe est partagé entre le serveur et le client RADIUS.

Cette manipulation est à répéter pour chaque équipement réseau qui aura l'authentification **802.1x** à activer.

#### B) Installer la stratégie d'accès réseau

Sous Windows Server 2008, les stratégies ne peuvent être gérées que via la console NPS. La stratégie réseau permet d'indiquer qui peut se connecter et sous quelles conditions elle comprend:

- ✓ **Une vue d'ensemble**, soit des informations qui indiquent si la stratégie est active et si elle autorise ou bloque l'accès, et la méthode de connexion réseau.
- ✓ **Des conditions** pour préciser le cadre de déclenchement de la stratégie (horaire, groupes, utilisateurs, système d'exploitation, etc.).
- ✓ **Des contraintes** pour préciser les méthodes d'authentification, le délai d'inactivité et d'expiration, des restrictions horaires et le type de port NAS, soit le type de média d'accès (Ethernet, FDDI, VPN, etc.), l'ID de la station appelée.
- ✓ **Des paramètres** pour définir des paramètres de connexion spécifiques aux protocoles utilisés.

- On fait un click droit sur NPS **| Stratégies | Stratégies réseau | Propriété** :

- On tape le nom de la stratégie.

- On sélectionne la condition *GROUPE WINDOWS* qui spécifie que l'utilisateur ou l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.

Ici le groupe sélectionné est le groupe ELN.

- On détermine les accès du groupe rajoutés précédemment

- On configure la méthode d'authentification : pour déployer la protection d'accès réseau (NAP) avec une connexion 802.1x on doit configurer le protocole PEAP.

- On peut configurer des paramètres supplémentaires de la stratégie réseau.

Le serveur NPS rejette automatiquement la demande de connexion d'un utilisateur au bout de 10 minutes si cette demande ne repend pas à une contrainte.

-A la fin de la configuration de la nouvelle stratégie, cette fenêtre s'affiche :

La configuration de la stratégie réseau est terminée et l'authentification radius est activée.

- On sélectionne le niveau d'autorisation pour le groupe

### IV.4.1.6 Enregistrement du serveur NPS dans AD

Une fois le serveur RADIUS « NPS » est configuré il faut l'enregistrer dans le domaine Active Directory pour qu'ils puissent communiquer. Pour ce faire, aller dans ***Server NPS*** et faire clique droit sur celui-ci et ensuite on clique sur ***inscrire le serveur dans Active Directory***.

- On appuie sur **ok**, et le message suivant apparait.

## IV.4.2 Configuration du supplicant

Le poste client (*supplicant*) doit être configuré pour qu'il puisse se connecter au Switch à travers un port utilisant l'authentification **802.1x**. Il faut donc que le poste client supporte ce protocole.

- Pour se faire, il suffit d'accéder au panneau de configuration de la connexion réseau souhaité, puis sélectionner l'onglet « Authentification ».
- On active l'authentification IEEE 802.1x pour ce réseau et on sélectionne la méthode EAP protégé (PEAP).
- On clique sur propriété, on décoche la case « Valider le certificat du serveur » qui permet de configurer ce client de telle sorte qu'il ne se connecte au réseau que si le certificat de serveur est validé et on choisit la méthode d'authentification « mot de passe sécurisé (EAP-MSCHAP version2) ».
- On clique sur configurer la boite de dialogue « propriétés EAP MSCHAPv2 », si la case de celle-ci est cochée la station de travail se connecte au réseau avec les paramètres d'identification de l'utilisateur enregistré. Dans le cas contraire, quand un autre utilisateur essaie de se connecter au réseau à travers la même station, un message lui demandant de s'authentifier s'affiche.

### IV.4.3 Configuration de L'authentificateur (Switch Cisco)

**Remarque :** dans le cas où on veut faire une authentification pour un port du Switch et l'utiliser pour une authentification 802.1x câblé, on configure le Switch de la manière suivante :

Dans le cadre de notre stage, le Switch disponible au sein de l'entreprise est le Switch Cisco Catalyst 2960, 24 ports pour la connexion Client / Switch.

Notre travail est de configurer l'authentification via Active directory avec le protocole 802.1x sur le port fastethernet f0/3.

Le Switch utilisé supporte l'authentification 802.1x avec l'annuaire RADIUS et la configuration de notre Switch se déroule comme suite :

- On alimente le Switch et on le relie au serveur avec le câble Consol (Bleu).
- On configure le nom du Switch, son mot de passe, et son adresse IP :

```
>en                          //Accéder au mode privilégié.
#configur terminal           //Pour configurer le Switch.
#hostname ClientNAS          //Attribuer un nom au Switch.
#interface vlan 1
#ip add 192.168.0.2 255.255.255.0      //Adresse IP est masque sous réseau du Switch.
#no shutdown                           // Active l'interface.
#exit                                  //Sortir.

//Attribuer un mot de passe.
#line vty 0
#password ccna
#login
#exit

#conf ter
#username ccna password ccna           //Nom d'utilisateur et mot de passe
#exit
#wr                                    //Enregistrer la configuration.
```

- On relie le Switch au serveur avec un câble réseau.
- Dans le serveur, on clique sur ***démarrer***, ***exécuter*** puis ***CMD.*** L'interpréteur de commendes Windows apparait.
- On pingue le Switch pour vérifier si la connexion est bonne entre lui et le serveur.

- Dans l'invite de commendes, on accède au Switch avec le TELNET qui est déjà activé sur la machine.

- On doit entrer le nom de l'utilisateur et le mot de passe pour entrer dans le Switch :

```
telnet 192.168.0.2
username : ccna          //Entrer le nom
password: ccna           //Entrer le mot de passe
enable
password:ccna
ClientNas #
```

- On Implémente le modèle AAA. Cette configuration a pour but d'activer l'authentification AAA et 802.1x sur le port FastEthernet.

```
#configure terminal
#aaa new-model
#aaa authentication dot1x default group radius
#dot1x system-auth-control
#radius-server host 192.168.0.1 auth-port 1645 acct-port 1646
#radius-server retransmit 5
#radius-server key Passw0rd
```

**Ces différentes commandes servent à :**

- **dot1x system-auth-control :** C'est pour la configuration du 802.1x, si le client est authentifié correctement le port permettra d'accéder aux ressources de réseau demandées par le client jusqu'à ce qu'il se déconnecte.
- **Radius-server host 192.168.0.1 auth-port 1645 acct-port 1646** : permet de configurer les paramètres de serveur RADIUS sur le commutateur (indiquer le nom ou l'adresse IP de serveur RADIUS), qui utilise le port UDP 1645 pour l'authentification et le port 1646 pour l'Accounting, c'est à dire la gestion des informations récoltées pendant toute la durée de la session, après identification de l'utilisateur.
- **radius -server retransmit 5 :** spécifier le nombre de fois que le client essayer de s'authentifier au serveur avant que ce dernier lui coupe la connexion.
- **Radius server-key Passw0rd** : permet d'indiquer la clef de chiffrage utilisée entre le commutateur et le serveur RADIUS qui est Passw0rd.

- On configure le 802.1x  sur le port Fastethernet f0/3 :

```
#configure  terminal
#interface f 0/3                  //Accéder à l'interface
#duplex auto                      //Configurer le mode bidirectionnelle automatique.
#speed auto                       //Configurer la vitesse bidirectionnelle d'interface et activer la
                                    configuration de vitesse automatique.
#switchport mode access           //Pour désactiver le mode dynamique par défaut du Switch pour
                                    pouvoir configurer 802.x.
#switchport access vlan 1         // Affecter le port à un réseau local virtuel vlan1.
#end
#wr                               //Enregistrer la configuration en cours dans la configuration
                                    de démarrage du commutateur.
```

```
#inter f0/3
#Switchport mode access    // Le 802.1x ne peut pas être appliqué sur n'importe quel port. Il
                             faut donc désactiver le mode dynamique à l'aide de cette
                             commande.
#dot1x port-control auto
#end
#wr
```

- la configuration du Switch est achevée et le port f0/3 devient orange.

## IV.4.4 Configuration de L'authentificateur (Point d'accès AP)

Notre architecture est basée sur une connexion Wifi, la configuration de notre point d'accès est la suivantes :

- Alimenter le point d'accès et ouvrir un navigateur internet puis lancer la recherche avec le site suivant : http://192.168.1.1/ qui est l'adresse par défaut du Point d'Accès

- Entrer le nom et mot de passe par défaut qui est ***admin***, ***admin*** :

- Au niveau de l'interface graphique du PA on désactive le DHCP pour éviter des conflits d'adresse avec le DHCP du serveur RADIUS, le chemin à suivre est le suivant :

  Basic, ***DHCP***, ***None*** et ***Submit*** pour enregistrer les modifications.

- On configure les paramètres de notre Wlan : Nom (SSID) : 2int, Mot de passe : Passw0rd, Adresse IP du serveur : 192.168.1.200, le port d'authentification : 1812, secret partagé entre le client NAS et le serveur : Passw0rd, les adresses MAC des Clients autorisés à se connecter.

- Une fois la configuration terminée, on doit rebooter le PA.

## IV.5 SIMULATION

Après la configuration des entités (Serveur, Client, Switch, Point D'accès), on va se connecter au réseau avec notre poste client (Supplicant).

Quand la carte réseau sans fils du poste client essaye d'authentifier le réseau, la fenêtre suivante s'affiche et lui demande des informations supplémentaires (Nom, Mot de passe).

- On rentre nos coordonnées  et on clique sur ***OK***.

- Dans le cas où les coordonnées sont erronées, le message suivant s'affiche :

- après avoir entré les bonnes coordonnées, le client NAS envoie la requête d'authentification au serveur RADIUS, ce dernier vérifie ces coordonnées au niveau de sa base de données Active Directory et autorise l'accès au réseau pour le client. On remarque que le port devient vert après l'authentification
- On pingue le serveur depuis le client pour vérifier que la connexion est bonne.

Une fois que le pingue est effectué, le client peu accéder au ressources du réseau.

## IV.6 CONCLUSION

Dans notre étude, on a utilisé l'Active Directory qui est l'un des moyens les plus fiable et les plus prometteurs en terme sécurisation des connexions.

Le protocole 802.1x ne constitue pas une réponse absolue aux problématiques de connexion au réseau local mais s'avère être un outil simple et discret pour mieux contrôler l'usage du réseau.

## CONCLUSION GENERALE

Dans ce projet, nous avons mis en œuvre une technique de sécurisation d'accès aux réseaux informatiques des entreprises, afin de mieux garantir certains besoins de la sécurité : l'authentification, l'intégrité et la confidentialité des données échangées entre différents utilisateurs et d'éviter toute sorte de piratage informatique. Cette technique permet de contrôler l'accès physique aux équipements d'infrastructures réseaux en s'appuyant sur le protocole EAP pour le transport des informations d'identification en mode client/serveur, et un serveur d'identification RADIUS qui utilise une base de données Active Directory.

Après avoir installé et configuré Windows serveur 2008 (serveur DHCP, DNS, serveur NPS), nous avons pu configurer le protocole 802.1x. Ensuite nous avons appliqué l'authentification au niveau d'un point d'accès et le Switch Cisco Catalyst 2960.

L'implémentation de 802.1x dans une infrastructure réseau est facile à réaliser et ne nécessite pas l'ajout d'un nouveau matériel au réseau, ce qui constitue l'un des avantages de la méthode.

Lors de la configuration du protocole 802.1x au niveau de l'authentificateur nous avons acquis beaucoup de connaissances sur le fonctionnement et la configuration du matériels Cisco.

Nous avons également eu beaucoup de plaisir à apprendre et à nous familiariser avec le Windows server 2008 pour mieux gérer la sécurité de notre architecture réseau.

Néanmoins, cette technique d'authentification ne permet pas d'assurer la sécurisation maximale des réseaux et reste à améliorer car *la sécurité parfaite n'existe pas*. Pour une éventuelle amélioration, on peut installer des certificats pour le serveur et les clients.

# *Bibliographie*


1. F. Lemanique, tout sur les réseaux sans fil, édition Dunod, 2009.
2. G.Aurélien,Wifi professionnel la norme 802.11, le déploiement, la sécurité,édition Dunod,2009.
3. S.Borderes, Authentification réseaux avec RADIUS (802.1X,EAP Free RADIUS), édition Eyrolles,novembre 2006.
4. T.Deman, F.Elmaleh, M.Chateau, S.Neild,Windows server 2008 (Administration avancée) ,éditions Dunod, 2008
5. P.Freddi, Windows server 2008 MCTS 70-642 - Configuration d'une infrastructure réseau , éditions Dunod, 2008
6. D.Holme, N.Ruest, D.Ruest, MCTS 70-640- Configuration d'une infrastructure Active Directory avec Windows server 2008 , edition Dunod, Septembre 2008.
7. K.Hadiouche,S.Guidoum, Etude et implémentation d'un réseau wifi sécurisé au sein de l'ENPED,Mémoire de Master en Electronique, UMMTO, 2011.
8. B.Magatte-D.Niang **,**Etude des performances de la norme IEEE 802.11 pour l'implémentation d'un réseau WiFi à l'ITO ,Mémoire d'Ingénieur,Ecole de Télécommunication d'Oran,2005.
9. A.Mokrani, A.Belghit, Implémentation du protocole d'authentification 802.1x avec le serveur RADIUS dans les réseaux informatiques, Mémoire Master en Electronique,UMMTO**,**2011.
10. **N.** Boughias**,** K. Baouali, L. Boudia,Implémentation d'un réseaux WiFi sécurisé à base d'un Contrôleur C 1000 d'Algérie Telecom au niveau de la résidence universitaire I.L.E de Tizi-Ouzou , Mémoire d'Ingénieur en Electronique, UMMTO, 2012.
11. Cours réseau informatiques et sécurité, Master II Résaeu et télécom, UMMTO,2013.


***Les sites :***


1. www.cisco.com.
2. http://fr.wikipedia.org/wiki/IEEE_802.1X.
3. http://www.commentcamarche.net/contents/wifi/wifi-802.1x.php3.
4. http://www.freeradius.org.
5. http://www.youtube.com/watch?v=JNSY46EPiws&feature=related.
6. http://www.memoireonline.com/07/09/2324/m_Les-technologies-sans-fil-Le-Wi-Fi-et-la-Securite5.html

**AES** (Advanced Encryption Standard)

Est un algorithme de chiffrement symétrique, il prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits. Les 16 octets en entrée sont permutés selon une table définie au préalable. Ces octets sont ensuite placés dans une matrice de 4x4 éléments et ses lignes subissent une rotation vers la droite. L'incrément pour la rotation varie selon le numéro de la ligne. Une transformation linéaire est ensuite appliquée sur la matrice, elle consiste en la multiplication binaire de chaque élément de la matrice avec des polynômes issus d'une matrice auxiliaire, cette multiplication est soumise à des règles spéciales. La transformation linéaire garantit une meilleure diffusion (propagation des bits dans la structure) sur plusieurs tours.

Finalement, un XOR entre la matrice et une autre matrice permet d'obtenir une matrice intermédiaire. Ces différentes opérations sont répétées plusieurs fois et définissent un « tour ». Pour une clé de 128, 192 ou 256, AES nécessite respectivement 10, 12 ou 14 tours.

**ATM :** (Asynchrone Transfer Mode)
Est un protocole réseau de niveau 2 à commutation de cellules qui permet de multiplexer les différents paquets de données sur un même lien utilisant une technique de type TDM ou MRT (multiplexage à répartition dans le temps).

**ANSI** (American National Standards Institute)
Principal organisme de standardisation aux Etats-Unis. L'ANSI est un organisme non gouvernemental, soutenu par des organisations commerciales, des associations professionnelles et l'industrie. Elle constitue le membre américain de l'ISO.

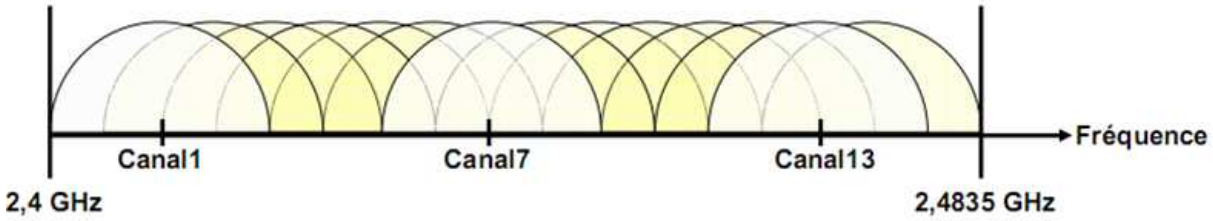
**Bande passante:** Plage de fréquence supportée d'un câble ou d'un canal, mesurée en Hz.

**CDMA :** (Code Division Multiple Access)

Utilisent une technique d'étalement de spectre permettant de diffuser un signal radio sur une grande gamme de fréquence.

**DSSS** (Direct Sequence Spread Spectrum)

C'est une technique de modulation avec étalement du spectre par séquence directe. Elle fonctionne sur la bande ISM des 2,4 GHz. La bande est divisée en 14 canaux de 20 MHz, chaque canal de 20 MHz étant constitué de quatre unités de 5 MHz. Chaque canal est espacé de 5 MHz, sauf le canal 14, espacé de 12 MHz avec le canal 13.



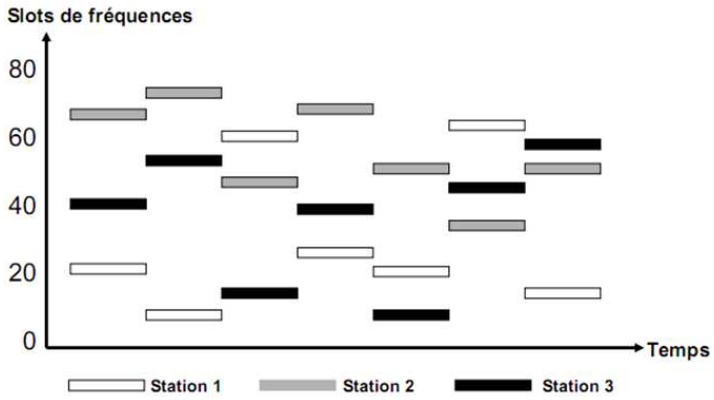
**DECT** (Digital Enhanced Cordless Telephone)

Norme de téléphonie sans fils numérique sur la bande 1,18 à 1,9GHZ, conçue pour une gamme large d'utilisations, cette norme est principalement utilisée pour des communications vocales.

**ETSI :** (L'European Telecommunications Standards Institute) est l'organisme de normalisation européen du domaine des télécommunications. Son rôle est de produire des normes de télécommunications pour le présent et le futur et est officiellement responsable de la normalisation des Technologies de l'information et de la communication (ICT) pour l'Europe en coopération avec le CEN et le CENELEC qui sont les instances Européennes représentant l'ISO et la CEI.

**FHSS** (Frequency Hopping Spread Spectrum)

C'est une technique de modulation avec étalement du spectre par saut de fréquence ; On modifie la fréquence de la porteuse par une séquence de sauts. C'est-à-dire que l'émetteur change de fréquence d'émission de façon périodique et suivant une séquence préétablie, il synchronise le récepteur grâce à des trames balises qui contiennent la séquence de saut et la durée. Dans la norme 802.11 la bande de fréquence ISM (2,400 à 2,4835 GHz) est divisée en 79 canaux de 1 MHz et le saut se fait toutes les 300 à 400 ms. L'émetteur et le récepteur s'accordent sur une séquence de saut. La norme définit trois ensembles de 26 séquences possibles (78 séquences au total).




**IR** (Infrarouge)
Elle permet la transmission des données grâce aux ondes lumineuses par réflexion multiple ou en visibilité directe.

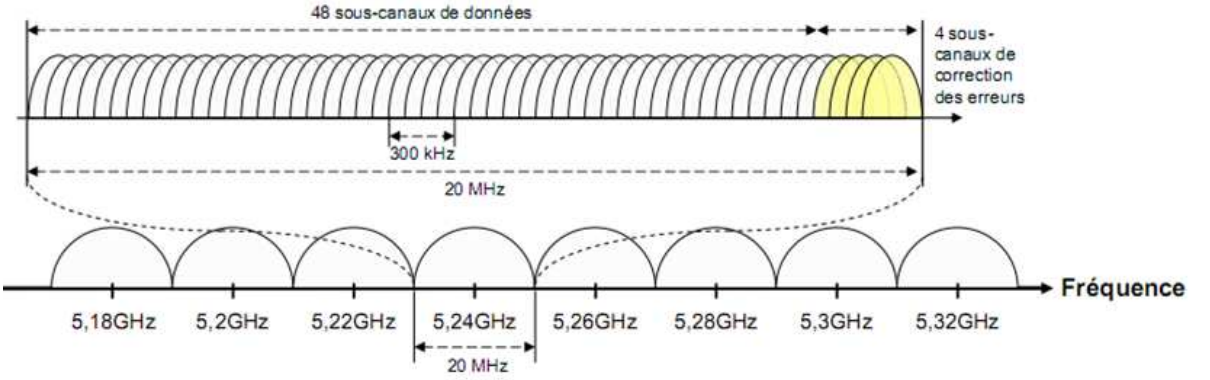
**IEEE** (Institute of Electrical and Electronic Engineers)
Organisme professionnel international qui émet ses propres standards et qui est membre de l'ANSI et de l'ISO.

**ISO (**International Standards Organization)
Organisme international qui élabore les standards comme l'OSI. La plupart des pays industrialisés ont chacun un correspondant local (ex: ANSI, IEEE...).

**MAC (address)** (Media Access Control address)
Il s'agit de l'adresse matérielle d'une carte réseau. On ne peut pas la changer.

**MD5** (Message Digest-5)
La méthode MD5 EAP fournit le niveau le plus bas de la sécurité possible et elle est la plus facile à mettre en place. Elle est basée sur le couple nom utilisateur / mot de passe. La faiblesse de ce système est qu'il utilise l'authentification à sens unique, le point d'accès authentifié le client, mais le client n'authentifié pas le point d'accès (pas d'authentification mutuelle).

**OFDM (**Orthogonal Frequency Division Multiplexing)
Son principe est d'effectuer un multiplexage fréquentiel de sous-porteuses orthogonales. Le fonctionnement est le suivant. Le canal est décomposé en cellules temps/fréquence, que l'on transmet en les modulant (chacune par une fréquence).Pour résoudre le problème d'interférence inter-symbole lié à la réception multiple d'une même information (transmission multi chemins), on insère un intervalle de garde entre chaque symbole, et l'on choisit correctement la durée d'un symbole par rapport à l'étalement de l'écho. L'OFDM utilise la bande des 5.2 GHz.




**OSI** (Open Systems Interconnection)
Il s'agit d'un modèle de référence pour les protocoles. L'OSI est définit sur 7 couches (Physique, Liaison, Réseau, Transport, Session, Présentation, Application).

**RC4**
L'algorithme RC4 a été pensé par **Ron Rivest** en 1987 et développé pour la RSA Security en 1994. Il est basé sur les permutations aléatoires, avec des opérations sur des octets.
L'algorithme a une longueur de clé variable (de 1 à 256 octets). Cependant à cause des lois d'exportation, la clé a souvent une longueur de 40 bits. La clé est utilisée pour initialiser une "table d'états" de 256 octets.

**SHA-1 :** (*Secure Hash Algorithm*) est une fonction de hachage cryptographique conçue par la *National Security Agency* des États-Unis (NSA), et publiée par le gouvernement des États-Unis comme un standard fédéral de traitement de l'information. Elle produit un résultat appelé « *hash* » ou « *condensat* » de 160 bits.

**TKIP** (Temporal Key Integrity Protocol)
Est un protocole de communication utilisé pour la protection et l'authentification des données transitant sur un réseau Wifi. Destiné à remplacer le WEP, il est spécifié dans la norme IEEE 802.11i et permet de conserver le matériel supportant WEP. TKIP emploie des solutions techniques proches de WEP (utilisation de l'algorithme de chiffrement RC4) mais sans les erreurs de conception.

TKIP utilise du « *key mixing* » pour chaque paquet, une vérification de l'intégrité des messages et un mécanisme de mise à jour de la clé, éliminant ainsi d'autres problèmes de conception qui affectent le WEP. En limitant la quantité de données chiffrées avec une même clé, il devient difficile pour un attaquant de deviner celle-ci.

Par rapport à WEP, quatre algorithmes ont été ajoutés :

- un code d'intégrité de message nommé *Michael*, le *MIC* (*message integrity code*) assure que le message n'a pas été modifié sur 8 octets.
- un compteur pour les vecteurs d'initialisation à l'instar du *numéro de séquence* des paquets dans TCP.
- une génération périodique d'une nouvelle clé temporaire, elle-même dérivée de la clé principale.
- une génération de sous-clé pour chiffrer un paquet (*key mixing*) à partir de la clé temporaire et d'un vecteur d'initialisation.

**TDMA:** (Time Division Multiple Access)

Technologie de transmission numérique permettant de transmettre plusieurs flux simultanés par répartition de temps.

**TCP/IP:** (Transport Control Protocol/Internet Protocol)

Protocoles de communication utilisée sur internet. Série d’instruction définissant la façon dont les paquets de données sont envoyés sur les réseaux. C’est le langage de communication entre tous les ordinateurs connectés à Internet. Ces protocoles incluent également une fonctionnalité qui permet de s’assurer si les paquets de données ont atteint leur destination dans le bon ordre.

**UDP:** (User Datagram Protocol) Est un protocole non orienté connexion dont le contrôle d’erreur est archaïque.

# SOMMAIRE

# Introduction Générale

# Chapitre I

# Les réseaux sans fils

# Chapitre II

# Sécurité d’un réseau Wifi et authentification 802.1x

# Chapitre III
# Etude des éléments d’authentification

# Chapitre IV
# Implémentation du protocole 802.1x sur le serveur RADIUS

# Conclusion Générale

# Glossaire

# Bibliographie

# Annexe