MINISTÉRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ ABOU-BEKR BELKAID – TLEMCEN
FACULTÉ DES SCIENCES DE L'INGÉNIEUR
DÉPARTEMENT DE TELECOMMUNICATION

Mémoire de Magistère

En

Systèmes et Réseaux de Télécommunications

THÉME

Étude et mise en œuvre de protocoles de sécurité des réseaux Wi-Fi : Application au réseau de l'université de Tlemcen

Par

BOUCHENAK Sofya

Soutenu en Juin 2007 devant le Jury, composé de :

Mr A. BESSAID.	M C	Université Abou Bekr Belkaid – Tlemcen	Président
Mr A. CHIKH	M C	Université Abou Bekr Belkaid – Tlemcen	Examinateur
Mr A. ABDELMALEK	C C	Université Abou Bekr Belkaid – Tlemcen	Examinateur
Mr M. FEHAM.	Prof	Université Abou Bekr Belkaid – Tlemcen	Directeur
Mr C. KARA TERKI	CC	Université Abou Bekr Belkaid – Tlemcen	Co-Directeur

Étude et mise en œuvre de protocoles de sécurité des réseaux Wi-Fi : Application au réseau de l'université de Tlemcen

Auteur : BOUCHENAK Sofya
Prof. Responsable : FEHAM Mohamed
Sujet proposé au sein du labo *STIC*

Á mon défunt grand père 'Khelil Zoubir'

Á mes parents.

Remerciements

Nous remercions ALLAH le Tout-puissant de nous avoir donnés le courage, la volonté et la bonne santé pour pouvoir mener à terme le présent travail.

Ce thème a été effectué au Laboratoire de recherche sur les *Systèmes et Technologies de l'information et de la Communication* (*STIC*) au Département de Télécommunications de la Faculté des Sciences de l'Ingénieur de l'Université Abou-bekr Belkaïd Tlemcen, dirigé par Monsieur **M. FEHAM**, Professeur à l'Université Abou-bekr Belkaïd de Tlemcen.

J'exprime mes sincères remerciements à **Mr FEHAM**, pour sa motivation, son soutien, sa générosité et également pour sa présence et sa disponibilité.

Mes grands respects et remerciements s'adressent à **Mr C. KARA TERKI** de m'avoir aidée à développer ce thème. Je le remercie également pour son soutien, ses conseils, son dévouement, sa disponibilité et sa remarquable sympathie.

J'exprime mes sincères remerciements aux membres du jury d'avoir accepté d'examiner mon travail :

Á Monsieur **A. BESSAID**, Maîtres de Conférences à l'Université Abou-bekr Belkaïd Tlemcen, d'avoir accepté de présider le jury.

Á Monsieur **A. Chikh**, Maîtres de Conférences au Département d'Informatique de la Faculté des Sciences de l'Ingénieur de l'Université de Tlemcen; d'avoir accepté de rapporter cette thèse, pour l'intérêt qu'il a bien voulu porter à ce travail en acceptant de faire partie du jury.

Je tiens à remercier Mr **A. Abdelmalek**, Chargé de Cours à l'Université Abou-bekr Belkaïd Tlemcen, pour ces précieux conseils et d'avoir examiné ce travail.

Enfin j'adresse mes remerciements les plus sincères aux membres du laboratoire STIC : à Mme Feham, Mr Ben Ahmed, Melle Djelti, Mr Merzougui et Mr Moussaoui.

.

Mes grands remerciements à mes deux familles KHELIL et BOUCHENAK à ma grand-mère, Mohamed, Tsouria, Fethi, Dalila, Mustapha, Souhila, Hafeda, Latefa, Zineddine, Tema, Samir et mes cousines Nafissa, Houda, Farah et Farihane de m'avoir supportée et soutenue.

Tous les mots restent faible pour exprimer ma profonde gratitude à mes parents qui sont d'un grand réconfort et d'un immense soutien, mes frères et sœurs Nawel, Mohamed, Lamia, Ghouti, Bouchera et Kheir Eddine.

Mes remerciement s'adressent à tous mes amis : Ikram de m'avoir aidée à terminer ce travail, Bouchera, Kamila, Naima, Soumia, wassila, douja, Nesma, Salima, wassila, hanane et hicham, ainsi que toute ma promotion d'ingénieurs de l'année 2004.

Enfin je remercie Abdallah pour ses conseils, son soutien et son aide.

Résumé

Les réseaux sans fil, plus particulièrement ceux de la norme IEEE802.11ou Wi-Fi connaissent un essor remarquable. La faiblesse de ces réseaux reste la sécurité des informations transmises sur le support hertzien.

Le réseau sans fil de l'université de Tlemcen est un réseau ouvert, ne disposant d'aucun mécanisme de sécurité. Pour cela une politique de sécurité doit être mise en place. Elle est déterminée à partir de l'audit de ce réseau, la classification des services et la définition des besoins de sécurité. Aussi,, cette politique ne doit pas brider l'autonomie des utilisateurs, ni encombrer le système d'information.

Notre contribution par se travail est de mettre en œuvre des protocoles d'authentification du protocole 802.1x tels que EAP-TLS et EAP-TTLS sur un réseau type de l'université. Ces protocoles sont robustes par l'utilisation de certificats électroniques et présentent une souplesse d'installation. Le mécanisme de chiffrement WEP qui est couplé à ces protocoles d'authentification est le seul mécanisme de chiffrement disponible sur les points d'accès de l'université. Nous proposons à l'avenir l'utilisation de mécanismes de chiffrement plus puissants tels que le WPA ou WPS pour plus de confidentialité.

Abstract

The Wireless Networks, especially of the IEEE802.11 standard have a remarkable success. The weakness of these networks remains the safety of the information transmitted on the hertzian support.

The wireless Network of the University of Tlemcen is an open network, any mechanism of security is applied. Therefore, we must apply a safety politic. It's established from the audit of the network, the classification of services and the definition of the security's needs. But this politic must not constrain the user's autonomy, neither load the system of Information.

Our contribution is to apply some protocols of authentication of the 802.1x protocol as EAP-TLS and EAP-TTLS on a similar network of the university. These protocols are sturdy, they use an electronics certificates. The WEP is used with these protocols of authentication; it's the only mechanism available in the university's bridges. We suggest in the future, the use of some protocols more strong as WPA or WPS for more confidentiality.

Table des Matières

Chapitre II :

Les technologies sans fil (Wi-Fi).

Aucune entrée de table des matières n'a été trouvée.

Chapitre III :

Les mécanismes de sécurité Wi-Fi.

Chapitre IV :

Une politique de sécurité pour le réseau sans fil de l'université de Tlemcen.

Liste des Tableaux

Listes des Figures

Listes des Annexes

Introduction Générale

Les réseaux sans fil constituent une catégorie très importante des réseaux de Télécom, le **Wi-Fi** est celui qui connait le plus grand succès.

Les perspectives des réseaux **Wi-Fi** sont très larges, pour les environnements domestiques, d'entreprises et d'opérateurs de Télécommunications. Dans de tels réseaux, l'utilisateur est libre de se déplacer tout en restant connecté au réseau.

Dans le cas des entreprises, le déplacement de bureaux en salles de réunion ne préoccupe pas l'utilisateur, puisqu'il reste toujours connecté. De plus, la mise en œuvre de tels réseaux est très facile, il suffit juste d'une bonne configuration et le réseau est opérationnel. De tels environnements sont appelés Internet ambiant, car la connexion peut se faire de partout, à tout moment et à haut débit. Ces avantages garantissent à **Wi-Fi** une carrière longue et prospère.

Néanmoins deux handicaps majeurs freinent ce succès, les failles de sécurité et la difficulté d'assurer une qualité de service.

Les problèmes liés à la qualité de service sont dus aux distances variées entre les points d'accès et les machines, aux interférences et aux obstacles.

Le problème de sécurité des réseaux **Wi-Fi** est lié au fait que les signaux radio qui traversent l'air entre les cartes de communications et les points d'accès peuvent être interceptés. Les données portées par ce signal sont alors sujettes aux modifications et aux vols. L'autre problème est du aux erreurs de conception des solutions qui ont été commercialisées au début de l'essor de **Wi-Fi**.

Les mécanismes de sécurité implémentés et normalisés au niveau des produits ont longtemps été faibles. Des solutions supplémentaires proposées par les constructeurs ont été mises en œuvre, mais à des prix exorbitants. Les organes de normalisation ont également réagi en proposant de nouvelles normes, plus ou moins adaptées aux besoins des particuliers et plus ou moins compatibles avec les produits déjà en vente.

Le manque de sécurité est très néfaste pour les réseaux **Wi-Fi**. La sécurité demande beaucoup de moyens humains et matériels.

L'université de Tlemcen dispose d'un réseau informatique très vaste au sein duquel existe une grande portion du réseau sans fil qui s'étend aux quatre coins de la ville de Tlemcen. Ce réseau ne dispose actuellement d'aucune mesure de sécurité.

Notre contribution, dans le cadre de ce travail, est de proposer une politique de sécurité pour le réseau sans-fil d'une université. Ce réseau a ses propres spécificités qui le différencient de celui d'un autre type de structure. Une université, de par sa raison d'être, doit rayonner et s'ouvrir sur l'extérieur. Une politique de sécurité trop stricte, risque de nuire à cette mission. Dans une université, une gestion de réseau, centralisée et trop contraignante, risque de brider l'autonomie des chercheurs dans les laboratoires. Il est rare, dans une université, qu'un ordinateur soit utilisé par un seul utilisateur. De plus, ces utilisateurs changent d'année en année. Tous ces facteurs tendent souvent à rendre toute politique de sécurité, peu efficace et pire encore ne réussit parfois qu'à alourdir l'utilisation et la gestion du réseau. Mais le besoin est là. Les universités doivent mettre en place un système d'information automatisé, opération qui peut s'avérer périlleuse dans un environnement non sécurisé. Après avoir étudié les vulnérabilités des services du système d'information en se basant sur la normalisation des protocoles de sécurisation des connexions sans-fil, nous détaillerons la mise en oeuvre des mécanismes d'authentification pour contrôler l'accès à un réseau sans fil type de l'université

Ce mémoire est s'organisé en cinq chapitres :

Le premier chapitre est consacré à un état de l'art sur la sécurité **Wi-Fi** à travers lequel, nous présentons l'état actuel de l'utilisation de la technologie **Wi-Fi** dans le monde. Des exemples sont donnés de quelques entreprises et universités qui utilisent le **Wi-Fi**, sur lesquels nous allons nous baser par la suite.

Dans le chapitre deux, une description générale de la norme **802.11** est présentée, avec des caractéristiques principales et son mode de fonctionnement. Le but de ce chapitre est de présenter les mécanismes de cette norme.

Le chapitre trois est consacré à la sécurité des réseaux **Wi-Fi**, avec entre autres les attaques et les mécanismes de sécurité.

Dans le chapitre quatre, nous nous intéresserons aux besoins de sécurité de l'université et aux vulnérabilités de son système d'informations. Nous présenterons des propositions visant à améliorer son niveau de sécurité.

La mise en œuvre et l'implémentation des méthodes de sécurité suggérées sur un réseau **Wi-Fi** utilisant l'infrastructure des réseaux de l'université de Tlemcen sont présentées dans le chapitre cinq.

1

État de l'art sur la sécurité Wi-Fi

Bien que les réseaux sans fil nous offrent des facilités de déploiement et une souplesse d'utilisation, ils nous laissent perplexes face à la sécurité qui est le point crucial d'un réseau de télécommunication. Ceci est dû au fait que les ondes radio sont un support de transmission partagé, quiconque se trouvant dans la zone de couverture peut écouter le support et s'introduire dans le réseau.

La sécurité des réseaux **Wi-Fi** de la norme **802.11** qui utilise la fréquence 2.5 GHz plus particulièrement ouvre un champ vaste aux chercheurs réseaux en tentant de trouver des solutions efficaces pour ce point néfaste; aussitôt les pirates et les hackers développent des logiciels d'écoute et d'intrusion pour pénétrer au sein des réseaux sans fil.

La plupart des points d'accès dispatchés dans le monde entier ne sont pas sécurisés ou même configurés par défaut. Certaines des entreprises qui utilisent le Wi-fi dans le monde ne se soucient pas de la sécurité de leurs points d'accès. La sécurité coute chère et cause de graves conséquences sur le système d'information des sociétés. Les universités qui disposent de points d'accès Wi-Fi, requièrent une forte sécurité pour garantir la confidentialité des informations et une bonne exploitation des ressources du réseau.

Au cours de ce chapitre, nous allons faire le point sur l'état de la sécurité des réseaux **Wi-Fi** plus particulièrement celle des universités et des entreprises.

I.1 – PRÉSENTATION

Le nom **Wi-Fi** provient de la contraction de l'expression Anglaise *Wireless* qui signifie technologie sans câble. En fait, **Wi-Fi** est le nom et le label grand public pour désigner les réseaux sans fils basés sur la norme **802.11** **[1]**.

I.1.1 – Historique

La finalisation de la norme **802.11** fut en 1998 **[2]**. Début 1999, le **Wi-Fi** a d'abord été utilisé par *Apple* sous le nom d'*Airport*. Son usage s'est généralisé en juin 2000, lorsqu'un groupe de Seattle a lancé la première communauté libre d'ordinateurs communiquant sous **Wi-Fi**.

Largement médiatisée, cette initiative a fait un grand effet aux Etats-Unis et dans le monde. En juin 2002 la bande de fréquence 2,4 Ghz est devenue accessible. Depuis, des milliers de points d'accès ont été installés dans plusieurs départements des plus grandes villes au monde **[2]**.

I.1.2 – Évolution des réseaux sans fil

Afin de bien comprendre l'évolution du **Wi-Fi**, nous proposons quelques définitions des différentes technologies des réseaux sans fil existantes.

Les groupes de travail qui se chargent de cette normalisation sont l'**IEEE 802.15**, pour les réseaux **WLAN**, l'**IEEE 802.16** pour les réseaux **WMAN** atteignant plus de dix kilomètres, et l'**IEEE 802.20**, pour les **WWAN**, c'est-à-dire les très grands réseaux.

Les figures (**FIG** I.1) et (**FIG** I.2) illustrent les différentes catégories de réseaux sans fil suivant leur étendue et les normes existantes.

Dans le groupe **IEEE 802.15**, trois sous groupes normalisent des gammes de produits en parallèle.

- **IEEE 802.15.1**, le plus connu, s'occupe de la norme Bluetooth, aujourd'hui largement commercialisée.
- **IEEE 802.15.3**, en charge de la norme **UWB**, met en œuvre une technologie très spéciale consistant à émettre à une puissance extrêmement faible, sous le bruit ambiant, mais sur pratiquement l'ensemble du spectre radio, entre 3,1 et 10,6 GHz. Les débits atteints sont de l'ordre du gigabits par seconde sur une distance de 10 mètres.
- **IEEE 802.15.4**, en charge de la norme ZigBee a pour objectif de promouvoir une puce offrant un débit relativement faible mais à un coût très bas.

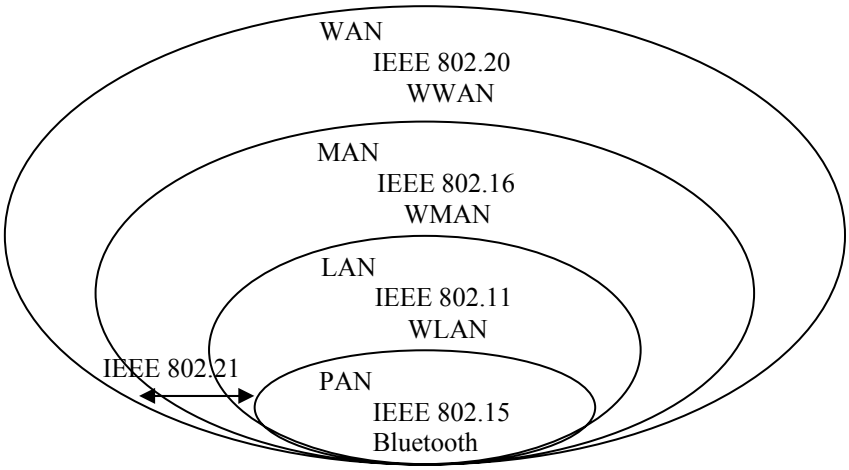


FIG I.1 – *Grandes catégories de réseaux sans fil* **[3].**

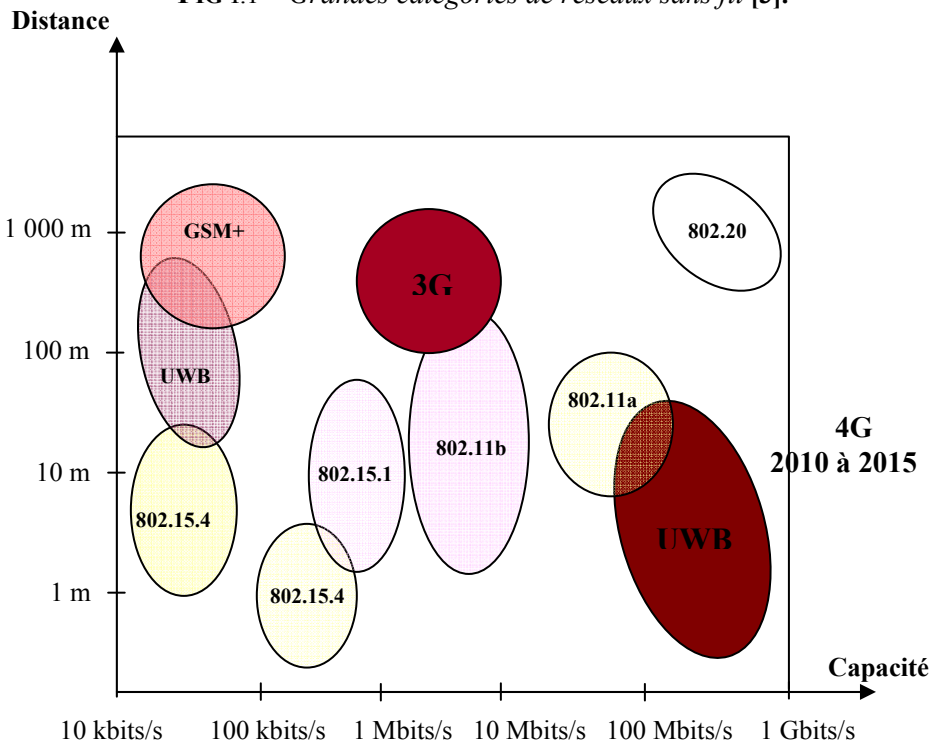


FIG I.2 – *Principales normes de réseaux sans fil* **[3].**

Du coté de la norme **IEEE 802.11**, dont les produits sont nommés **Wi-Fi**, il existe aujourd'hui trois propositions, dont les débits sont de 11Mbits/s (**802.11**b) et 54 Mbits/s (**802.11**a et g). Une quatrième proposition, **IEEE 802.11**n, devrait bientôt augmenter le débit, qui pourrait atteindre 320 Mbits/s.

HiperLAN est une technologie par l'**ETSI**. Deux versions de ce standard existent, **HiperLAN1** et **HiperLAN2** qui peuvent fonctionner ensemble. Ce standard utilise une bande de fréquence proche du 5 GHz. Le débit théorique proposé par **HiperLAN1** est proche de 20 Mbits/s et celui de l'**HiperLAN2** est de 54 Mbits/s. La zone de couverture dépend du milieu, la fréquence ayant une longueur d'onde plus petite, celle-ci est plus sensible aux obstacles, cependant dans des milieux dégagés (type point à

point) la connexion sera meilleure que pour le **Wi-Fi**.

L'objectif des réseaux **802.16** est de remplacer les modems ADSL, des réseaux téléphoniques fixes, pour offrir à l'utilisateur final des débits importants, de l'ordre de quelques centaines de kilobits par secondes jusqu'à plusieurs mégabits par seconde. Ces réseaux sont appelés **BLR** ou **WLL**.

Le consortium *Wimax* a été mis en place pour développer les applications de cette norme **IEEE 802.16**. Plusieurs normes sont proposées selon la fréquence utilisée.

Les réseaux étendus se sont principalement développés sous l'égide d'organismes internationaux, comme l'**UIT**. Les principaux standards développés à ce jour sont le **GSM**, le **GPRS**, **EDGE**, l'**UMTS** et le **cdma2000**. La norme **IEEE** équivalente est l'**IEEE 802.20**, ou **MBWA**, que l'on appelle **Wi-Mobile**. Son objectif est de concurrencer les standards des opérateurs de téléphonie mobile grâce à un coût très bas **[3].**

La norme **802.11** nous intéresse de prêt, elle est la plus développée.

I.1.3 – La norme Wi-Fi

La norme **IEEE 802.11** a donné naissance à la génération des réseaux sans fil **Wi-Fi [3].** Cette norme offre des débits de 1 ou 2 Mbits/s. Des révisions ont été apportées à la norme originale afin d'optimiser le débit (c'est le cas des normes **802.11**a, **802.11**b, **802.11**g). Le tableau I.1 résume toutes les normes existantes et quelques caractéristiques **[4]**.

Nom de la norme	Nom	Description
802.11a	Wi-fi5	La norme 802.11a (baptisé *WiFi 5*) permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). La norme 802.11a spécifie 8 canaux radio dans la bande de fréquence des 5 GHz.
802.11b	Wi-fi	La norme 802.11b est la norme la plus répandue actuellement. Elle propose un débit théorique de 11 Mbps (6 Mbps rééls) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2.4 GHz, avec 3 canaux radio disponibles.
802.11c	Pontage 802.11 vers 802.1d	La norme 802.11c n'a pas d'intérêt pour le grand public. Il s'agit uniquement d'une modification de la norme 802.1d afin de pouvoir établir un pont avec les trames 802.11 (niveau *liaison de données*).
802.11d	Internationali-Sation	La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11. Elle consiste à permettre aux différents équipements d'échanger des informations sur les plages de fréquence et les puissances autorisées dans le pays d'origine du matériel.
802.11e	Amélioration de la qualité de service	La norme 802.11e vise à donner des possibilités en matière de qualité de service au niveau de la couche *liaison de données*. Ainsi cette norme a pour but de définir les besoins des différents paquets en terme de bande passante et de délai de transmission de telle manière à permettre notamment une meilleure transmission de la voix et de la

		vidéo.
802.11f	Itinérance (roaming)	La norme 802.11f est une recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole *Inter-Access point roaming protocol* permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau. Cette possibilité est appelée *itinérance* (ou *roaming en anglais*)
802.11g		La norme 802.11g offre un haut débit (54 Mbps théoriques, 30 Mbps réels) sur la bande de fréquence des 2.4 GHz. La norme 802.11g a une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b
802.11h		La norme *802.11h* vise à rapprocher la norme 802.11 du standard Européen (HiperLAN 2, d'où le *h* de 802.11h) et être en conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie.
802.11i		La norme *802.11i* a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'*AES* (*Advanced Encryption Standard*) et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
802.11Ir		La norme *802.11r* a été élaborée de telle manière à utiliser des signaux infra-rouges. Cette norme est désormais dépassée techniquement.
802.11j		La norme *802.11j* est à la réglementation japonaise ce que le 802.11h est à la réglementation européenne.

TAB I.1 – *Les différentes normes Wi-Fi* **[4]**.

I.1.3.1 – Portées et débits

Les normes **802.11**a, **802.11**b et **802.11**g, 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 (Tableau I.2) **[5]**.

Standard	Bande de fréquence	Débit	Portée
Wi-Fi a (802.11a)	5 GHz	54 Mbit/s	10 m
Wi-Fi B (802.11b)	2.4 GHz	11 Mbit/s	100 m
Wi-Fi G (802.11b)	2.4 GHz	54 Mbit/s	100 m

TAB I.2 – *Portée et débits des normes 802.11* **[5]**.

I.1.3.2 – Les organismes de régulation

L'avantage principal de **Wi-Fi** est sa capacité à utiliser les bandes de fréquence de la norme **802.11** sans avoir besoin d'une licence **[1]**.

En effet, ces bandes sont reconnues par les organismes de réglementation internationaux. Il s'agit :

- du FCC pour les Etats-Unis ;
- de l'ETSI pour l'Europe ;
- du MKK pour le Japon ;
- de l'ARPT pour l'Algérie **[1]**.

I.2 – LES RÉSEAUX WI-FI

La norme **802.11** est devenue de nos jours une technologie prometteuse. En Algérie c'est l'ARPT qui régule les fréquences. La fréquence 5,86 Ghz est une bande avec licence pour une utilisation outdoor. Les fréquences 2,5 et 3,5 GHz ne nécessitent pas de licence pour une utilisation indoor.

Grâce au **Wi-Fi**, il est possible de créer des réseaux locaux sans fil à haut débit (figure I.3). Dans la pratique, il permet de relier des ordinateurs portables, des machines des bureaux tels que des imprimantes, des assistants personnels (PDA) ou même des périphériques à une liaison haut débit (11 Mbits/s ou 54 Mbits/s) sur un rayon de plusieurs dizaines de mètres en intérieur. En environnement ouvert, la portée peut atteindre des dizaines de kilomètres **[6].**

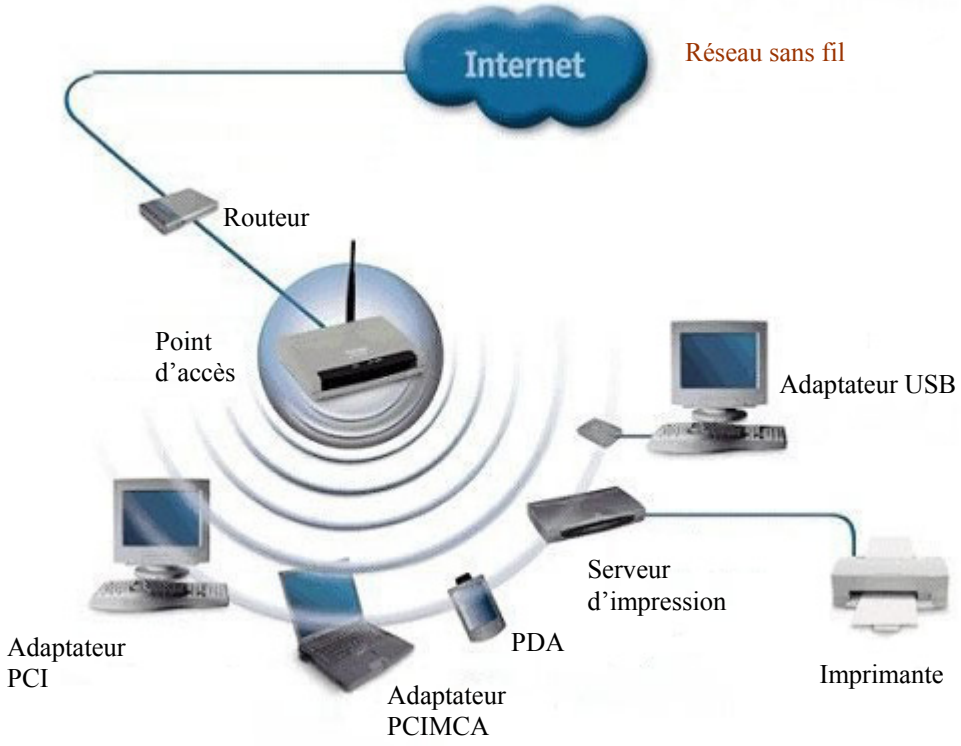


FIG I.3 – *Exemple de réseau sans fil d'entreprise.*

Ainsi des FAI irriguent des zones à forte concentration d'utilisateurs (gares, aéroport, hôtels, trains, etc.) avec des réseaux sans fil connectés à Internet. Ces zones d'accès sont appelées *« Hot Spots »*.

Grâce à **Wi-Fi**, le nomadisme s'implante rapidement et il n'est plus nécessaire de rechercher une prise de connexion et de configurer son ordinateur, pour accéder aux services. Le **Wi-Fi** est très utile, plusieurs organismes font appel à cette technologie lors de leurs expositions ou manifestations économiques.

En Algérie, Algérie Télécom en collaboration avec d'autres opérateurs étrangers, travaille pour lancer **Wi-Fi**.

I.2.1 – Déploiement de Wi-Fi

Le **Wi-Fi** est déployé généralement de deux manières :

I.2.1.1 – Liaison point à points

Les liaisons point à point sont utilisées pour relier des sites distants se trouvant dans des zones où le câble est difficile à installer. L'exemple de la figure (**FIG** I.4) est le cas d'un site, situé dans une ville urbaine, s'alimentant d'un lien terrestre relié à Internet. Il transmet la communication à l'antenne de distribution du site qui lui est en face. C'est la méthode la plus facile pour rejoindre une municipalité en périphérie **[1]**.

I.2.1.2 – Liaison point à multipoints

Les liaisons sont très fréquentes et nombreuses. Elles permettent de diffuser la connexion Internet à tous les clients se trouvant dans le périphérique de l'antenne de diffusion. Dans la figure (**FIG** I.4), l'antenne de réception du site rediffuse la connexion Internet à tous ses clients **[1]**.

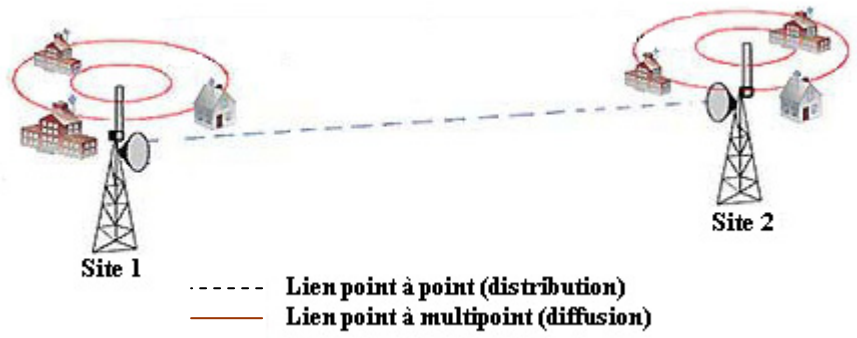


FIG I.4 – *Réseau de distribution sans fil Wi-Fi.*

I.2.2 – Avantages et inconvénients des réseaux Wi-Fi

I.2.2.1 – Avantages

L'explosion des WLAN et de leurs nombreux avantages renforce leur compétitivité par rapport aux LAN traditionnels. Les principaux avantages offerts par les réseaux locaux sans fil sont :

- **mobilité :** ceci simplifie les déplacements de l'utilisateur.
- **Simplicité d'installation :** il suffit d'avoir des stations munies d'une interface sans fil, de configurer l'AP et mettre le réseau en route.
- **Coût réduit :** les interfaces des réseaux WLAN sont un peu plus élevées que ceux des LAN, mais la connectivité n'existe pas, donc pas de câblage.
- **Inter connectivité avec les LAN :** les WLAN sont compatibles en connexion avec les LAN.
- **Fiabilité :** l'efficacité des transmissions sans fil a été prouvée dans divers domaines d'applications (militaires&civiles). Les interférences liées aux ondes radios provoquent parfois de grosses baisses de performances. Cependant, une distance limitée entre les différents équipements et une bonne organisation du WLAN permet de prémunir contre ce genre de problèmes **[7]**.

I.2.2.2 – Inconvénients

Le gros inconvénient est l'absence de sécurité liée à un support ouvert (interface radio). Les données émises sont dans toutes les directions et sans contrôle. Cela aura plusieurs impactes.

- **Des réglementations locales spécifiques :** dans le cas où les fréquences ne sont pas permises, on doit réduire les puissances.
- **Sensibilité à l'environnement :** si l'environnement utilisé est plein d'obstacles physiques, tels que des murs ou des structures métalliques, la transmission deviendra perturbée voire impossible.
- **Brouillage:** parfois, les ondes sont émises vers des endroits où cela n'est pas nécessaire. Cela causera le brouillage d'autres transmissions.
- **Entrée non contrôlée d'informations :** de la même façon qu'il sera possible de capturer l'information, il sera possible de l'injecter sur le réseau. Les conséquences pourront être catastrophiques si l'objet de l'injection est un virus par exemple.
- **La chute du débit :** c'est fréquent lors des communications nombreuses ou d'informations riches (images, vidéo, etc.). La connexion par ondes radio du **Wi-Fi** ne garantit ni la qualité des communications, ni la continuité d'un point d'accès à un autre. Le signal et le débit diminuent en fonction de la distance **[7]**.

Il est clair que les avantages amenés par les réseaux sans fil apportent avec eux de nombreux inconvénients. Cependant, il est possible de passer outre ces inconvénients.

I.3 – ÉTAT DES LIEUX DES RÉSEAUX WI-FI OUVERTS ET SÉCURISÉS

Au départ les réseaux **Wi-Fi** étaient une solution adéquate pour les administrateurs réseau et pour les lieux publics, dans les cas difficiles de déploiement de réseaux locaux filaires.

Les réseaux **Wi-Fi** sont scindés en deux types :

- Les réseaux ouverts au grand public dans les grandes capitales telles que Washington, Paris ou Londres, et les lieux publics trop fréquentés tels que les gares et les aéroports.
- Les réseaux sécurisés qui limitent l'accès uniquement pour les personnes inscrites au sein des entreprises ou des campus universitaires.

I.3.1 – Les réseaux Wi-Fi ouverts

Il existe de nos jours des réseaux **Wi-Fi** non sécurisés, alors que la sécurité est lancée partout dans le monde et dans les firmes des équipements **802.11**. Quelques points d'accès restent ouverts au public.

Des équipes expertes en sécurité recensent le nombre de points d'accès au monde qui ne sont pas sécurisés.

Une étude faite à la Nouvelle Zélande a recensé 50 sociétés utilisant un réseau **Wi-Fi** ouvert. Ces réseaux sont accessibles par tous les pirates du passage **[8]**.

Les réseaux ouverts incluent de *« grands noms de sociétés »* aussi bien que les réseaux publics d'hôtels **[9]**. Ceci est un danger économique et social. Une entreprise d'une grande importance économique peut perdre ses ressources informatiques, ses bases de données, mais aussi peut être amenée à disparaître en cas de vole de projets, causés par des intrusions réseaux **[8]**. Il est également sujet à poursuites juridiques quand le réseau de l'entreprise est utilisé pour des fins malveillantes.

Les AP (Access Point) non sécurisés font le bonheur des voyageurs et des étudiants dans les trains, les aéroports et les campus. Ces AP sont très nombreux et ne cessent de s'accroîtrent surtout dans les grandes villes à grande densité de population. Néanmoins la sécurité s'impose en mettant en œuvre des mécanismes de sécurité robuste surtout pour les grandes entreprises.

Certains préfèrent laisser leurs réseaux ouverts afin de faire profiter tout le monde de la connexion Internet et du partage de l'information, ou par insouciances à d'éventuelles attaques.

D'autres parts, il existe certains sites tels que les universités et quelques sociétés qui préfèrent sécuriser leurs réseaux pour garantir une stabilité et facilité de gestion des utilisateurs.

I.3.1.1 – Sécurité des réseaux sans fil en Europe

Depuis deux ans des études ont été faites sur les réseaux et les protocoles sans fil afin de lever le voile sur la situation et d'attirer l'attention des usagers sur les problèmes potentiels. L'objectif principal de l'étude est les points d'accès **Wi-Fi [9]**.

Ces études se sont déroulées en Chine à Pékin, en Tientsin à Hanouvre dans le cadre du salon CeBit 2006 et à Londres à l'occasion du salon InfoSecurity au printemps 2006.

Paris a fait également l'objet de l'étude sur le niveau de développement et de protection des réseaux **Wi-Fi** dans les quartiers d'affaires. L'Enquête s'est déroulée du 22 au 25 novembre 2006 à la cour de La Défense (où se tenait le salon InfoSecurity) et dans les quartiers de Paris. Des données ont été collectées sur environ 1000 points d'accès. Il s'agit du plus grand nombre d'AP jamais détecté **[9]**.

I.3.1.2 – Chiffrement du Trafic

L'indice le plus digne d'intérêt concernant les réseaux sans fil est le rapport entre AP protégés et non protégés **[9]**.

Selon une ancienne étude effectuée par les wardrivers **[9]**, « 70% des réseaux sans fil dans le monde ne déploient aucun mécanisme de sécurité. Á Pékin, ils sont 60%, à CeBit 55%, et à Londres 50% » **[9].**

D'après les données récoltées de cette Enquête, Paris reçoit la palme d'excellence officieuse de des réseaux **Wi-Fi** les mieux sécurisés, passant devant Londres (49%) **[9]**.

Cette étude qui a duré 2 ans, a noté une tendance forte à l'augmentation de pourcentage de réseaux dans lesquels sont déployés telle ou telle méthode de chiffrage (WEP ou WPA), moins de 70% à Moscou, 60% à Pékin et 30% à Paris de réseaux sans fil non cryptés. C'est une tendance mondiale qui tend à démontrer que les administrateurs ont pris au sérieux la situation du trafic *« ouvert ».*

D'après RSA Security, 74% des réseaux sans fil professionnels sont protégés par le WEP au premier trimestre 2006 (contre 65% en 2005). Pour New York, 75% (contre 62% en 2005), Paris a le plus fort taux puisque seulement 22% ne sont pas sécurisés.

RSA recense un quart des réseaux sans fil d'Entreprise n'est pas sécurisé. Un quart est utilisé avec la configuration par défaut **[10]**.

Les host pots frauduleux constituent actuellement une menace à prendre au sérieux. Ils sont faciles à installer. Les pirates sont pratiquement certains de recueillir des informations fiables dans un délai restreint estime de son coté Phil Crackenelle de Capgeminui UK Security consulting Pratic qui a fait la partie technique de l'étude **[10]**.

- En résumé, des réseaux non sécurisés existent encore et il faut sensibiliser les administrateurs réseau à déployer des mécanismes de sécurité.

I.3.2 – Les réseaux sécurisés

Contrairement aux réseaux sans fils publics qui ne font appel à aucun mécanisme de sécurité, il existe quelques grandes universités qui ont apporté des solutions pour faire de leurs réseaux sans fil, des réseaux sécurisés. Pour être plus explicites, nous allons décrire quelques réseaux universitaires où la sécurité a été établie.

Les plus grandes universités à Londres, Paris et même Alger ou Tlemcen utilisent la technologie **Wi-Fi** pour faire étendre le réseau facilement et rapidement.

Dans un tel secteur, l'accès à Internet est vital, la conception des LAN est primordiale, mais la sécurité est parfois nécessaire.

Parmi les grandes universités Française qui s'intéressent à la sécurité **Wi-Fi,** citons comme exemple : Nancy, Nantes, Limoges, Paris et Louis Pasteur **[11], [12], [13], [14]**. Á ce sujet là des travaux ont été publiés par des Ingénieurs et même des doctorants.

- Université Henri Poincaré de Paris

C'est un réseau ouvert à tous les étudiants. Il offre un accès à Internet, sous certaines conditions et un accès aux ressources informatiques de l'université **[11]**. Les étudiants ont accès à la connexion Internet mais pas aux ressources Informatiques de l'université telle que les services de scolarité.

- Université de Limoges

L'université dispose d'un réseau sans fil étendu sur tous les campus. L'accès à Internet et la consultation de la boite aux lettres universitaires s'effectue via un client de messagerie.

Un service a été mis en œuvre à partir du nouveau service 22 juin 2006 par sécurité informatique qui consiste à établir une configuration des clients de messagerie (Outlook) des utilisateurs **Wi-Fi** pour qu'ils utilisent les certificats TLS au niveau du serveur SMTP (envoi de message). Les messages et mots de passe envoyés seront ainsi chiffrés et ne passeront pas en clair sur le réseau **[12]**.

- Université de Pierre et Marie Currie

Un exemple très pratique d'une université utilisant le **Wi-Fi** est l'université Parisienne de **Pierre et Marie Currie.**

Depuis Janvier 2005, cette université déploie sur l'ensemble de ses sites, dont le CHU, un réseau informatique sans fil (nommé CanalIP).

L'infrastructure du réseau sans fil UPMC offre un mode de connexion sécurisé avec authentification et chiffrement de la totalité de la session sans fil de l'utilisateur.

Tout le trafic de l'utilisateur étant chiffré grâce à un logiciel client installé préalablement sur le pc, un vol de mot de passe ne peut avoir lieu par écoute du trafic échangé sur le réseau sans fil.

D'autre part, la clé de chiffrement n'est pas statique, elle varie au cours du temps empêchant, ainsi, des attaques réalisées avec l'un de nombreux programmes de piratages qui sont disponibles sur Internet. De cette façon, le réseau de l'université est bien géré et assure une confidentialité et intégrité des échanges de données.

D'autres universités telles que Nantes ont opté pour d'autres mécanismes d'authentification et de chiffrement **[13]**.

- Université de Louis Pasteur

Dans un article paru en 2002, des méthodes d'authentification ont été étudiées et appliquées pour contrôler l'accès aux 900 points d'accès de l'université. La définition de la politique de sécurité de l'université est en fort rapport avec les besoins de sécurité définis lors de l'installation du réseau sans fil et les équipements disponibles. En attendant que les points d'accès supportant le WPA soient sur le marché. Pour cela ils ont opté pour les méthodes d'authentification EAP-TLS, EAP-TTLS et EAP-PEAP. Il existe d'autres solutions de sécurité basées sur les réseaux VPN **[14].**

- Université de Tlemcen

L'université de Tlemcen de son côté, dispose d'un réseau sans fil qui est l'extension du réseau filaire. C'est une solution souple pour relier des sites distants en mode point à point.

Dans le cas d'une utilisation point à multipoints, le **Wi-Fi** est utilisé dans les laboratoires de recherche ou dans les salles de recherche et même dans les bibliothèques.

Le **Wi-Fi** nous épargne des câbles percés partout sur les mûrs et des prises informatiques. Il est aussi facile de changer de salle ou de déplacer des équipements sans avoir à se soucier du câblage à faire et au déplacement des prises.

La mise en marche du réseau est très rapide. Le réseau sans fil de l'université est ouvert et n'utilise aucun mécanisme de sécurité.

Quelques laboratoires de recherche utilisent le WEP comme mécanisme de sécurité. Ce mécanisme n'étant pas sûr **[15]**, ne garantit pas une sécurité au réseau et moins aux utilisateurs et leurs applications.

Cependant des travaux dans le cadre de projets de fin d'études d'ingénieurs ont eu pour thème la sécurité du réseau de l'université de Tlemcen **[16]**, **[17]**, **[18]**.

En 2005, des études ont été faites par des ingénieurs en informatique concernant le réseau **Wi-Fi** d'un laboratoire de recherche. Le premier travail consistait à prouver que la clé WEP utilisée seule n'était pas un moyen sûr pour assurer la sécurité du réseau **[16].** Le deuxième travail avait pour objectif d'utiliser le WEP, accompagné d'un mécanisme d'authentification. Quoique ce mécanisme a ses faiblesses et n'est pas très robuste face aux attaques d'intrusions **[17]**.

En 2006, d'autres travaux ont eu lieu. Cela consistait à faire un audit sur le trafic du réseau de l'université, recenser les attaques, les virus et les vers réseau. Á travers cette étude il serait possible de déterminer le niveau d'insécurité du réseau. La finalité du travail portait sur une proposition d'une architecture de réseau informatique sécurisé **[18].**

I.3.3 – Évolution des mécanismes de sécurité

Le moyen de sécurité primaire pour ces réseaux est le WEP, implémenté dans tous les équipements réseaux actuels. Face aux failles trouvées, des améliorations ont été apportées à ce mécanisme en mettant le WEP2, puis le WPA et le WPA2. Ces mécanismes sont plus robustes que le WEP classique.

Afin de sensibiliser le grand public au problème de la sécurité réseau, la **Wi-Fi** Alliance vient de mettre en place une certification optionnelle baptisée WPS. Pour l'obtenir, les fabricants devront s'arranger pour que leurs périphériques réseau puissent être paramétrés le plus simplement possible, tout en assurant un niveau de protection satisfaisant.

Le programme WPS prévoit notamment que la protection d'un réseau **Wi-Fi** puisse être activée au moyen d'un simple bouton sur l'appareil concerné, ou au moyen d'une séquence numérique de type code PIN (comme sur les téléphones portables). Un nouveau périphérique certifié WPS serait ainsi automatiquement reconnu par le réseau domestique. Il suffirait alors d'appuyer sur le bouton, ou de rentrer le code numérique, pour que les paramètres réels du réseau (nom du réseau, clé WPA) soient transmis à la machine et que cette dernière puisse s'y connecter. L'utilisation d'un bouton, et non d'un mot de passe, permettrait de sécuriser simplement des périphériques qui ne disposent pas d'écran.

Un certain nombre de composants **Wi-Fi** signés Atheros, Broadcom, Buffalo ou Marvell sont d'ores et déjà certifiés WPS, indique la **Wi-Fi** Alliance, qui espère que les premiers produits pourront faire leur entrée sur le marché d'ici la fin du premier semestre 2007. Elle envisage ensuite de porter cette certification aux puces sans contact (*Near Field Communication*) ainsi qu'à l'USB **[19]**.

I.4 – CONCLUSION

Les réseaux sans fil basés sur la norme **IEEE 802.11** constituent une solution pratique et intéressante offrant mobilité, flexibilité, faible coût de déploiement et d'utilisation. L'utilisation de ces réseaux est généralement non sécurisée. Par contre dans certains cas particuliers, la sécurité s'impose et devient un point noir pour ces réseaux. Cela engendre des répercutions sur les utilisateurs tels que les grandes entreprises ou les universités.

Dans ce chapitre, nous avons énuméré l'état actuel de la sécurité au sein des réseaux **Wi-Fi**, des lieux publics et des lieux privés en présentant des exemples des réseaux sans fil de quelques universités. En ce qui concerne l'université de Tlemcen plus précisément, des travaux ont été faits. Il reste à trouver une solution de sécurité adéquate.

2

Les réseaux sans fil (Wi-Fi)

Les réseaux sans fil connaissent une évolution considérable de par leur facilité de déploiement. Ces réseaux prennent de l'ampleur à l'échelle d'une ville, d'une entreprise et même des universités. Les communications entre équipements terminaux peuvent s'effectuer directement ou par le biais de station de base. Les communications entre points d'accès s'effectuent de façon hertzienne ou par câble. Ces réseaux atteignent des débits de plusieurs mégabits par seconde, voir de centaines de Mégabits par seconde.

Plusieurs normes ont vu le jour et ont été développées selon les besoins requis par les utilisateurs. Ceci nécessite la commercialisation de plusieurs gammes de produits, et les normalisations en cours devraient introduire de nouveaux environnements.

Le but de ce chapitre est de présenter les différentes normes des réseaux sans fil, en se basant beaucoup plus sur la norme **802.11**. Nous détaillerons son mode de fonctionnement et ses principales caractéristiques.

Plusieurs facteurs clés laissent prévoir une montée en puissance du marché des réseaux sans fil, parmi lesquels nous pouvons citer :

- Une maturité progressive des normes (spécialement celles dérivées du **802.11**, **802.11**a, **802.11**b et **802.11**g) ;
- Un investissement considérable des grands constructeurs dans la fabrication des terminaux, carte et point d'accès.
- Des propositions de solutions de sécurisation et de roaming (avec certaines limitations).
- Une baisse de coûts des équipements.
- Une bande de fréquence utilisable sans licence par conséquent, divers marchés sont ouverts (marché domestique, télétravail, éducation, santé, grand publique…) **[20]**.

Pour comprendre le fonctionnement de cette technologie **Wi-Fi**, nous proposons dans ce qui suit une étude technique de la norme de base **IEEE 802.11.**

II.1 – ÉQUIPEMENTS WI-FI

La norme **IEEE 802.11** considère deux types d'équipements : une station sans fil et un point d'accès.

II.1.1 – Point d'accès Wi-Fi (figure II.1)

Le point d'accès est le cœur d'un réseau **Wi-Fi**. Il est considéré comme pont pour relier le réseau filaire et le réseau sans fil. Ce point d'accès est constitué d'un Emetteur/Récepteur radio, d'une carte réseau filaire et d'un logiciel de pontage. C'est la station de base du réseau sans fil qui donne l'accès à de multiples stations sans fil au réseau filaire **[3]**.

DLink AP7100

Cisco Aironet350

FIG II.1 – *Les points d'accès Wi-Fi.*

Il s'agit d'un *«* Centraliseur ou Concentrateur *»* **[21]** pour le réseau **Wi-Fi**. Dans certains cas, le débit maximum peut être partagé entre les stations, donc son fonctionnement se rapproche plus de Hub que de Switch **[21]**.

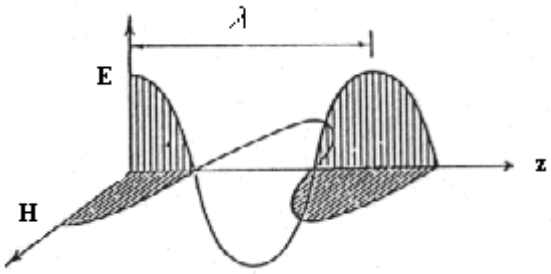
Les points d'accès peuvent être munis d'une seule antenne, ou de deux antennes que l'on peut diriger afin d'améliorer la réception. Il est possible même de changer d'antennes selon les utilisations du réseau.

II.1.2 – Les antennes Wi-Fi

II.1.2.1 – Définition

Les ondes **Wi-Fi** sont rayonnées ou captées par l'antenne **Wi-Fi**. Ce dispositif se trouve sur chaque station d'émission ou de réception **Wi-Fi**.

L'onde électromagnétique est par définition une oscillation. Elle se propage dans l'espace ou dans la matière. Le schéma suivant décrit cette variation. La technologie **Wi-Fi** est donc l'ensemble des techniques conçues pour la transmission sans fil des donnés d'un réseau utilisant Ethernet **[22]**. Le schéma de la figure II.2, le décrit :



λ : étant la longueur d'onde.

FIG II.2 – *Propagation des ondes radioélectriques* **[22]**.

II.1.2.2 – Caractéristiques de l'antenne Wi-Fi

L'antenne **Wi-Fi** est un dispositif un peu complexe, qui peut être placé dans un endroit dégagé pour que les ondes **Wi-Fi** ne soient pas dégradées par les obstacles.

L'Antenne **Wi-Fi** se définit par les caractéristiques suivantes : **[22]**

- Bande de fréquences d'utilisation de l'antenne **Wi-Fi** 2.4Ghz;
- Type d'antenne **Wi-Fi**: Puissance admissible en émission de l'antenne **Wi-Fi**;
- Directivité, gain et diagramme de rayonnement de l'antenne **Wi-Fi**;
- Dimensions et forme de l'antenne **Wi-Fi**;
- Polarisation de l'antenne **Wi-Fi**;
- Mode d'alimentation et impédance au point d'alimentation de l'antenne **Wi-Fi**;
- Résistance mécanique de l'antenne **Wi-Fi**.

II.1.2.3 – Les types d'antennes Wi-Fi [22]

- Antenne **Wi-Fi** Omnidirectionnelles :

Grâce à cette antenne de 9 dB de gain, il est possible détendre la zone de couverture du réseau sans fil **Wi-Fi**. Le signal radio est alors transporté sur de plus longues distances que l'antenne **Wi-Fi** d'origine.

Cette antenne peut être montée sur un AP ou un Routeur **Wi-Fi**.

- Antenne **Wi-Fi** Panneau ou Patch 12dB :

C'est un nouveau modèle d'antenne directionnelle 12dB. Cette antenne est utilisée sur un dispositif répondant à la norme **802.11**b ou **802.11**g. Elle permet de relier des réseaux locaux distants de plusieurs kilomètres et des bâtiments. Pour une utilisation Indoor comme Outdoor, cette antenne est très efficace pour capter le signal des équipements **Wi-Fi**.

- Antenne **Wi-Fi** Sectorielle 21dB :

Grâce à cette antenne **Wi-Fi**, l'extension du réseau **Wi-Fi** devient facile. Son gain de 21 dBi permet de couvrir un secteur de façon optimum. L'angle de cette antenne est de 120°, offrant une couverture optimale au réseau **Wi-Fi**.

- Antenne **Wi-Fi** directionnelle 12dB Grille :

Le gain de cette antenne est de 12 dB. Elle permet d'étendre la zone de couverture du réseau sans fil **Wi-Fi** à plusieurs kilomètres. Elle est conforme à la norme **802.11**b ou **802.11**g. Cette antenne peut être fixée au mur ou en extérieur et est conçue pour les points d'accès.

- Antenne **Wi-Fi** Yagi :

Cette Antenne **Wi-Fi** Yagi permet de relier deux bâtiments distants. Elle est conçue pour être utilisée en extérieur, cette antenne **Wi-Fi** est très efficace pour étendre le réseau **Wi-Fi**. Elle est très directive et remplit parfaitement la fonction pour laquelle elle a été créée.

II.1.2.4 – Mode d'alimentation

Généralement, l'antenne est placée à l'extrémité loin de l'équipement **Wi-Fi**. Une ligne bifilaire ou un câble est utilisé pour relier l'antenne au point d'accès.

Pour un fonctionnement optimal, l'impédance au point d'alimentation doit être du même ordre que l'impédance caractéristique de la ligne d'alimentation. Les impédances sont de l'ordre de 50 ou 75 ohms pour le câble et environ 300 ohms pour la ligne bifilaire **[22]**.

II.1.3 – Les Cartes d'accès 802.11

Les stations sans fil communiquent entre elles et avec le point d'accès grâce aux cartes d'accès **802.11** ou adaptateurs sans fil (Wireless adapters ou Network Interface Controller NIC) (figure II.3). Les formats des adaptateurs sont en cartes PCI, PCMCIA ou USB, etc.) **[5]**.

Carte PCI Dlink AG530

PCMCIA / PC Card

Adaptateur WL-54USB, USB, réseau **Wi-Fi** & **802.11**g

FIG II.3 – *Les adaptateurs Wi-Fi.*

II.2 – MODES DE FONCTIONNEMENT Wi-Fi

Le standard **802.11** définit deux modes: mode infrastructure et mode Ad-hoc.

II.2.1 – Mode « INFRASTRUCTURE »

Le mode infrastructure (figure II.4) permet aux stations de communiquer entre elles à travers un point d'accès.

- Une cellule est une zone constituée d'un ensemble de machines, et d'un point d'accès qui couvre cette zone. Elle est dite ensemble de services de base (BSS), elle est identifiée par un SSID. Ce dernier

est d'une longueur de 6 octets et correspond à l'adresse MAC du point d'accès dans le mode infrastructure.

- Les BSS peuvent être reliées entre elles par une liaison appelée système de distribution (notée DS) pour constituer un ensemble de services étendu ESS. Le système de distribution peut être soit un câble ou une liaison sans fil entre deux points d'accès. Sa fonction est le transfert des paquets entre les différentes cellules d'une même zone de services étendue ESS.
- Un ESS est identifié par un ESSID de 32 caractères de long (au format ASCII), c'est le nom attribué au réseau. Il est abrégé en SSID et représente le premier niveau de sécurité, puisque l'utilisateur doit le connaitre pour se connecter au réseau étendu **[23].**

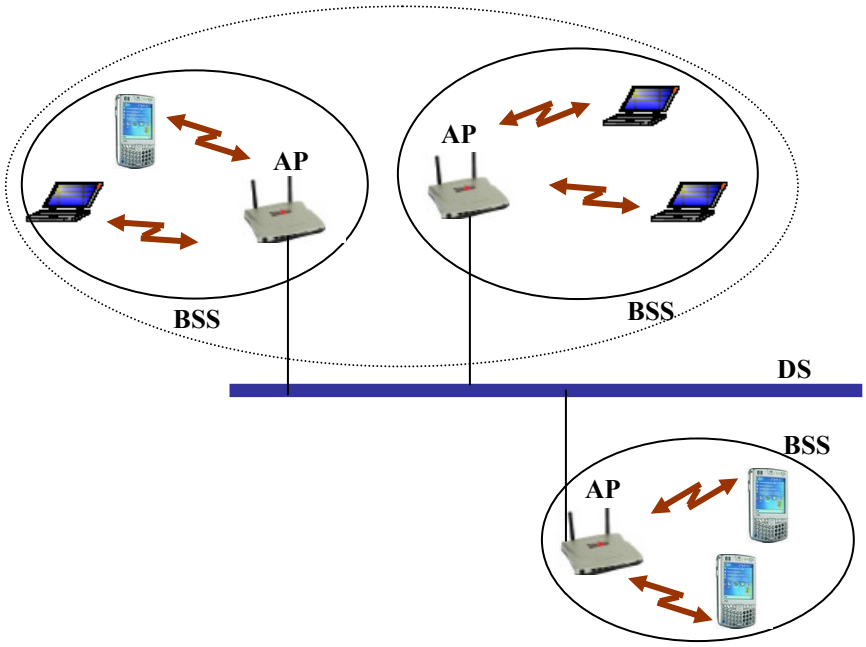


FIG II.4 – *Le mode Infrastructure.*

- Au passage d'un utilisateur nomade d'un BSS à un autre dans l'ESS, l'adaptateur sans fil change de point d'accès en fonction du signal reçu par les points d'accès se trouvant dans l'ESS. La communication entre les AP de ces déplacements se fait grâce au système de distribution. La caractéristique qui permet aux stations de « passer de façon transparente » d'un AP à un autre est appelée Itinérance (Roaming).
- Lorsqu'une station veut s'associer à un point d'accès appartenant à un ESS, elle diffuse sur chaque canal une requête de sondage (probe requeste) contenant l'ESSID pour lequel elle est configurée et le débit que peut supporter son adaptateur sans fil. Chaque point d'accès diffuse (à une raison d'un envoi toutes les 0,1 secondes environ) une trame balise (Beacon) pour donner des informations concernant son BSSID, ou éventuellement son ESSID. Généralement, l'ESSID est

diffusé par défaut, mais il est recommandé de désactiver cette option. La requête de sondage reçue, permet à l'AP de vérifier l'ESSID et la demande de débit présent dans la trame balise.

Dans le cas où l'ESSID est le même que celui de l'API, ce dernier envoi des informations concernant la charge et les données de synchronisation. D'après ces informations, la station détermine la qualité du signal émis par l'AP.

Si une station se trouve au milieu de plusieurs AP, elle pourra choisir le point d'accès offrant le meilleur compromis de débit et de charge **[23]**.

II.2.2 – Mode « Ad Hoc »

Dans le cas du mode Ad Hoc (figure II.5), les machines se connectent entre elles et forment un réseau point à point. Chaque machine joue alors le rôle de station et de point d'accès.

L'ensemble des stations forme un ensemble de services de base indépendants (IBSS).

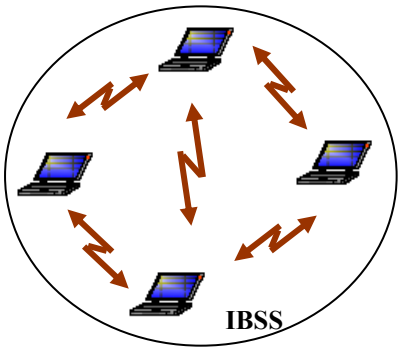


FIG II.5 – *Le mode Ad- hoc.*

Par définition, un IBSS est un réseau sans fil constitué au minimum de deux stations sans avoir besoin d'un point d'accès.

Ce type de réseau est éphémère, il est utilisé dans les salles de travail ou de réunion. Il est identifié par un SSID, équivalent à l'ESS en mode Infrastructure.

La portée de chaque station détermine la portée du BSS indépendant, le mode Ad Hoc, ne permet pas de transmettre les trames d'une station à une autre. Un IBSS est alors un réseau sans fil restreint **[23]**.

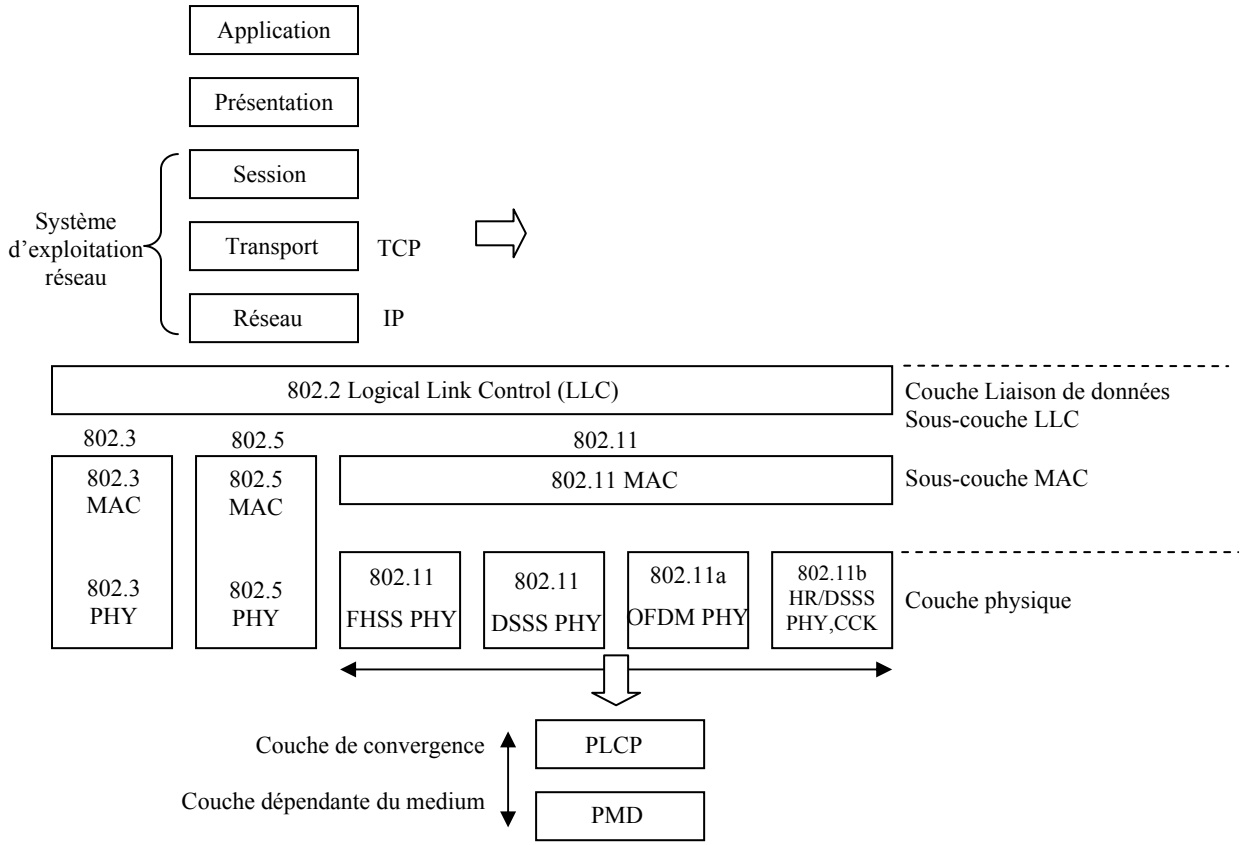
II.3 – DESCRIPTION DE LA STRUCTURE EN SOUS-COUCHE

Á l'instar des autres standards **IEEE 802**, le standard **802.11** se base sur deux couches inférieures du modèle ISO, la couche physique (PHY) et la couche de liaison de données qui contient la sous-couche MAC et la sous-couche LLC, comme le montre la figure II.6 **[20].**

La couche physique utilise plusieurs techniques de modulation et de codage binaire pour transmettre les trames MAC sur le support de communication.

Dans la norme **802.11**, les couches physiques et MAC sont détaillées. L'architecture, les fonctions et les services de base **Wi-Fi** (**802.11**b) sont définis par le standard **802.11** d'origine.

La spécification **802.11**b n'affecte que la couche physique, permettant d'offrir des débits supérieurs et une connectivité plus robuste.



(a) Pile protocolaire ISO

FIG II.6 – *IEEE 802.11 et la famille 802* **[20]**.

II.3.1 – Les différentes couches physiques

Le standard de base de la norme **802.11** définit trois couches physiques **[20]** :

- Une couche physique radio utilisant une technique d'étalement de spectre en saut de fréquence (FHSS) dans la bande 2,4 GHz.
- Une couche physique radio utilisant une technique d'étalement de spectre en séquence directe (DSSS) dans la bande 2,4 GHz.
- Une couche physique pour la transmission par infrarouge (IR). La transmission par infrarouge opère en bande de base.

Grâce aux transmissions basées sur l'étalement de spectre, il est possible d'accroître les performances de la transmission sans fil concernant les effets de la propagation par trajets multiples, les interférences et le bruit. La couche physique est structurée en deux sous couches :

- La sous-couche de convergence ;

- La sous-couche dépendante du médium de transmission.

– La couche PLCP

Cette couche s'appelle aussi sous-couche de convergence. Elle a pour rôle de s'adapter à la couche inférieure qui est dépendante du support (Infrarouge, FHSS ou DSSS). Cette couche a pour rôle d'insérer des entêtes qui permettent la synchronisation ou l'identification de la modulation utilisée sur le support **[20]**.

Les trames envoyées par la couche PLCP sont appelées PPDU. Le format des PPDU dépend de la sous-couche basse utilisée. La procédure de transmission PLCP est invoquée par la procédure CS/CCA qui est exécutée pour :

- Détecter le début d'un signal qui peut être capté (phase écoute de la porteuse CS),
- Déterminer si le canal est libre avant de transmettre un paquet (phase CCA) **[20]**.

Les formats des paquets PLCP sont exposés en **Annexe A**.

– La sous-couche basse

Elle a pour rôle de coder et de transmettre les bits envoyés pour la couche de convergence sur le médium ou PMD. En plus du plan de transport de l'information, un plan de contrôle existe. Toutes les fonctionnalités de contrôle (management) relatives à la couche physique sont implémentées dans la couche PHY management. Les informations de gestion sont stockées dans une base de données MIB, au format SNMP **[20]**.

II.3.1.1 – Couche physique radio avec étalement de spectre en saut de fréquence FHSS [24]

La technique FHSS utilise le saut de fréquence dans laquelle la bande passante disponible est divisée en 79 sous canaux. Chaque canal est de 1 MHz de largeur offrant un débit d'au moins 1 Mbits/s avec un codage binaire. Un accord est établi entre l'émetteur et le récepteur sur une séquence de sauts de fréquences porteuses afin de transmettre les données successivement sur les sous canaux existants. Le calcul de la séquence de sauts permet d'éviter que deux stations utilisent le même sous canal.

La bande de fréquence 2,4 - 2,4835 GHz utilisée dans la norme **802.11** permet de créer 79 canaux de 1 MHz. Le temps entre deux transmissions successives sur un canal puis sur un autre est de 400 ms, ce qui permet de reconnaitre facilement sur une fréquence donnée un signal transmis.

La technique FHSS (figure II.7) était conçue pour des utilisations militaires. Actuellement, cette technologie est utilisée dans les réseaux locaux, donc la séquence de fréquences utilisées est connue.

Dans ce cas, aucun mécanisme de sécurisation des échanges n'est assuré par l'étalement de spectre par saut de fréquence. Le standard **802.11** utilise le FHSS dans le but de réduire les interférences entre les transmissions des stations d'une cellule.

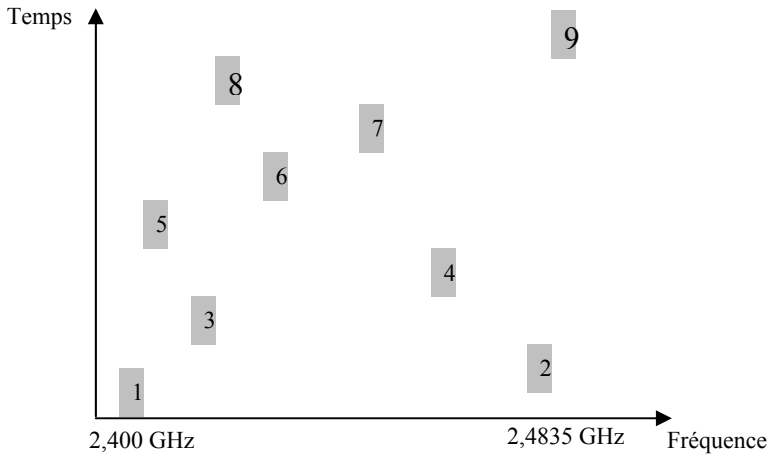


FIG II.7 – *La technique FHSS* **[20].**

La figure II.8 explique comment peut-on transmettre des données dans une plage de fréquence perturbée. Grâce au découpage des 79 canaux, seulement les sous canaux perturbés seront affectés **[20]**.

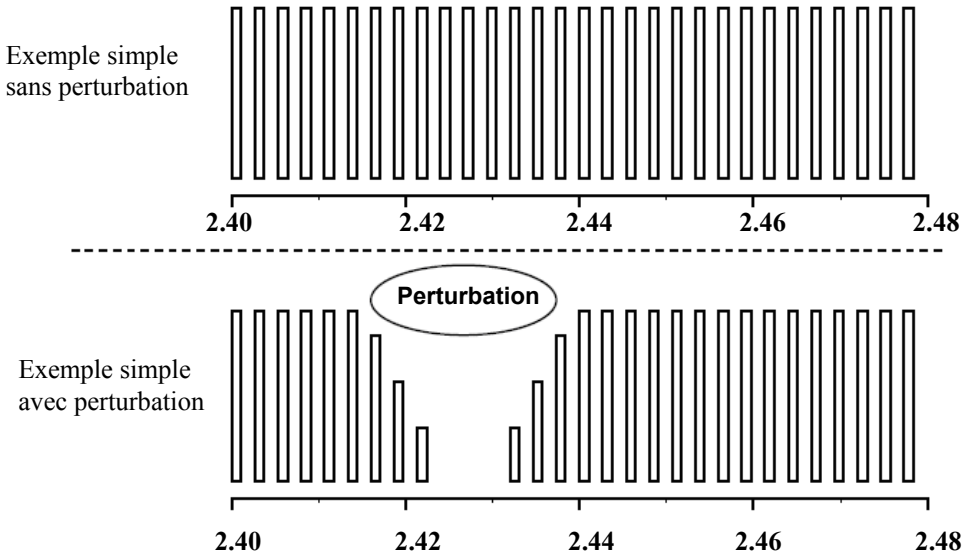


FIG II.8 – *Le Frequency-Hopping Spread Spectrum (FHSS)* **[24]**.

Une trame FHSS au niveau physique se compose de trois parties. Elle commence par un préambule, ensuite une entête et se termine par la partie données (figure II.9).

Préambule		En-tête			TRAME MAC
Synchro 80 bits	SFD 16 bits	PLW 11 bits	PSF 5 bits	CRC En-tête 16 bits	

FIG II.9 – *La structure de la trame 802.11 au niveau physique pour le FHSS* **[24]**.

Chaque champ de chaque partie possède un rôle spécifique :

A – Le préambule

– *La synchro :* est une séquence de synchronisation qui est composée d'une suite de 80 bits constitués en alternance de 0 et de 1. Elle permet à la couche physique de détecter la réception d'un signal. Elle permet accessoirement aussi, de choisir la meilleure antenne de réception si le choix existe.

– *Le SFD :* est l'identificateur de trame. Il est constitué par la suite de bits suivants: 0001100101101101.

B – L'entête

– *Le PSDU Length Word (PLW) :* est un paramètre passé par la couche MAC qui indique la longueur de la trame. C'est donc la longueur de la partie de donnée dans cette trame.

– *Le PSF :* est un champ sur 5 bits qui permet de définir la vitesse de transmission. Le premier bit (numéro 0) est toujours à 0. Les bits 1, 2 et 3 sont réservés et définis par défaut à zéro. Le 4ème et dernier bit, indique la vitesse de transmission. A 1Mb/s il est à 0 et à 2Mb/s il est à 1.

– *Le CRC de l'entête :* est le champ de contrôle d'erreur de l'entête, composé de 16bits.

C – La partie donnée

– *La Trame MAC :* contient les données relatives à la couche MAC. La partie de données est émise en utilisant une *technique de blanchiment* pour éviter d'avoir une suite de 0 ou de 1, qui risquent de poser des problèmes, tel qu'une désynchronisation du signal.

Les modulations utilisées :

Une modulation de fréquence GFSK à deux niveaux pour 1Mbits/s ;

Une modulation de fréquence à quatre niveaux pour 2 Mbits/s.

Les préambules dans tous les cas sont transmis avec une modulation de 1 Mbits/s.

II.3.1.2 – Etalement de spectre à Séquence directe (DSSS)

Le DSSS est la deuxième couche physique qui utilise une technique radio. Pour cela, la bande de fréquence est divisée en 14 sous-canaux de 22 MHz. Ces canaux fournissent des signaux bruités. Ce phénomène est du au fait que les signaux adjacents ont des bandes passantes dont le recouvrement est partiel. Ils peuvent par conséquent se perturber mutuellement (figure II.10).

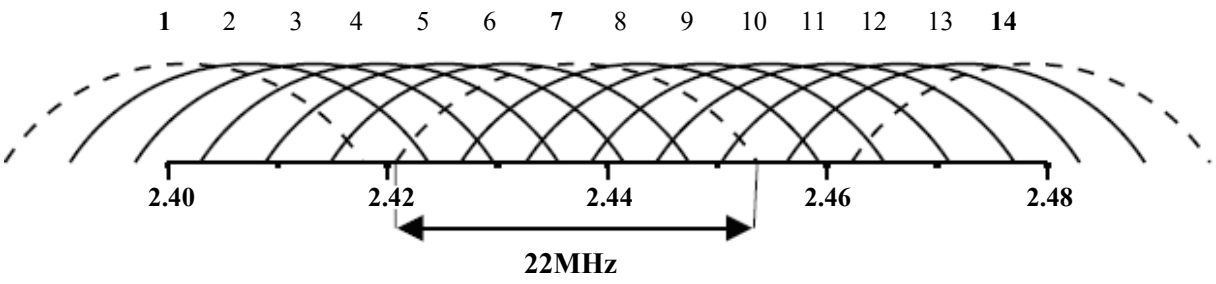


FIG II.10 – *Le Direct Sequence Spread Spectrum (DSSS)* **[25]**.

Le principe de cette technique est de transmettre pour chaque bit une séquence Barker de bit. Chaque bit de valeur ‘1’ est remplacé par une séquence de bits et chaque bit de valeur ‘0’ par son complément **[25]**.

Dans la couche physique de la norme **802.11**, le ‘1’ est représenté par une séquence de 11 bits (10110111000) et le ‘0’ par (01001000111).

Le chip code chaque bit encodé à l’aide de la séquence. Grâce au chipping (figure II.11), la transmission de l’information redondante est effectuée. Ce qui permet le contrôle d’erreurs sur les transmissions, et même la correction d’erreur.

Pour une transmission de 11 Mbps correcte et d’après le théorème de Shannon, il faut transmettre sur une bande de 22 MHz. « D’après le théorème de Shannon, la fréquence d’échantillonnage doit être au minimum égale au double du signal à numériser » **[21]**.

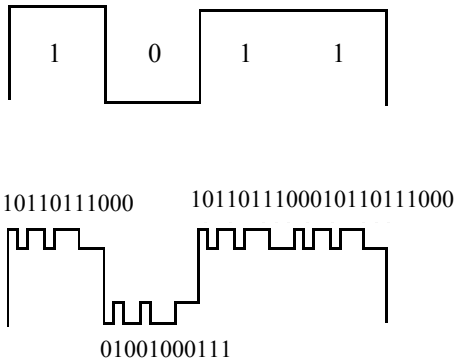


FIG II.11 – *Technique du chipping* **[25]**.

La bande de fréquence 2.400-2.4835 GHz (d'une largeur de 83.5 MHz) du standard **802.11**b a été découpée en 14 canaux séparés de 5MHz. Voici les fréquences associées aux 14 canaux (Tableau II.1) :

Canal	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Fréquence (GHz)	2.412	2.417	2.422	2.427	2.432	2.437	2.442	2.447	2.452	2.457	2.462	2.467	2.472	2.484

TAB II.1 – *Canaux des fréquences du standard 802.11b* **[25]**.

Une trame DSSS au niveau physique est composée, comme pour la technique précédente, de trois parties : un *préambule*, puis une *entête* et enfin la partie données (figure II.12).

Préambule		En-tête				TRAME MAC
Synchro 128 bits	SFD 16 bits	signal 8 bits	service 8bits	Longueur 16 bits	CRC En- tête 16 bits	

FIG II.12 – *La composition de la trame 802.11 au niveau physique pour le DSSS* **[25]**.

A – Le préambule

– ***La synchro :*** est une séquence de synchronisation pseudo-aléatoire. Elle sert à la synchronisation au niveau récepteur.

– ***SFD :*** permet au récepteur de détecter le début de la trame. Ce champ de deux octets vaut en hexadécimal F3A0.

B – L'entête

– ***Le signal :*** permet d'indiquer la vitesse de transmission sélectionnée. Si la valeur de ce champ est à 0A (en hexadécimal) la transmission se déroulera à 1Mb/s et si celle ci est à 14 (en hexadécimal), la transmission se déroulera à 2Mb/s. Il faut savoir qu'en fonction de la vitesse de transmission, une modulation différente est appliquée. Le *differential binary phase shift keying* est utilisé lors d'une transmission à 1 Mb/s et en opposition au Differential quadrature phase shift keying lors d'une transmission en 2 Mb/s.

– ***Le service :*** est réservé pour un usage futur La valeur 00 signifie que le transmetteur est conforme à la norme **IEEE 802.11**.

– ***La longueur :*** indique la valeur de la longueur de la partie de données. Sa valeur peut varier entre 4 et 2^{16}.

– ***Le* CRC *de l'entête :*** est le champ de contrôle d'erreur de l'entête.

C – La partie donnée

– ***La Trame MAC :*** contient les données de la trame physique. Elles sont transmises selon la modulation sélectionnée dans le champ *signal*.

La transmission par DSSS offre deux débits **[20]**. Les modulations utilisées sont :

- Une modulation de phase DBPSK pour 1Mbits/s ;
- Une modulation en quadrature de phase DQPSK pour 2Mbits/s.

❖ Les produits actuels existants sur le marché ont tendance vers la norme **802.11**b DSSS offrant 4 débits. Le choix du débit est défini en fonction des conditions radio **[20]**.

D'après la figure II.13, nous constatons que plus la distance entre l'AP et les équipements est courte plus le débit utilisé est élevé aussi bien pour FHSS que pour DSSS.

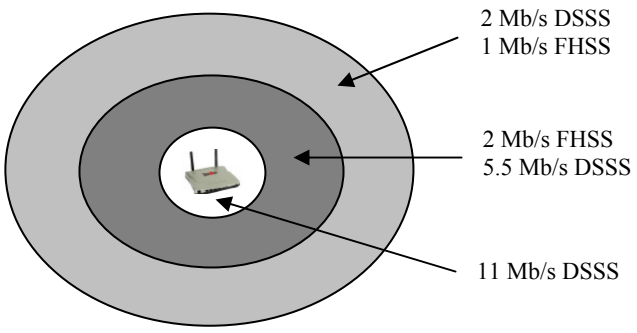


FIG II.13 – *Mécanisme de changement de débit en fonction de la distance* **[20]**.

L'étendue de la zone de couverture en mode DSSS dépend des débits utilisés avec une distinction selon le type de l'environnement intérieur (Indoor) ou extérieur (Outdoor).

Ces mesures sont en fonction de l'environnement où elles ont été prises (Tableau II.2).

Débits (Mbits/s)	Portée (mètres)
11	50
5,5	75
2	100
1	150

TAB II.2 (a) – *Environnement intérieur (indoor), technique DSSS* **[20]**.

Débits (Mbits/s)	Portée (mètres)
11	200
5,5	300
2	400
1	500

TAB II.2 (b) – *Environnement extérieur (outdoor), technique DSSS* **[20]**.

II.3.1.3 – La technique infrarouge

L'utilisation de la technique Infrarouge dans le standard **IEEE 802.11** est possible. Cette technique utilise une onde lumineuse pour la transmission de données. Les transmissions se font de façon unidirectionnelle. Le fait que la transmission soit non dissipative, un niveau de sécurité plus élevé est offert.

La technologie infrarouge permet d'obtenir des débits allant de 1 à 2 Mbit/s, en utilisant une modulation appelée PPM.

Le principe de la modulation PPM est de transmettre des impulsions à amplitude constante et à coder l'information suivant la position de l'impulsion. Le débit de 1 Mbps est obtenu avec une modulation de 16-PPM, tandis que le débit de 2 Mbps est obtenu avec une modulation 4-PPM permettant de coder deux bits de données avec 4 positions possibles (figure II.14) **[26].**

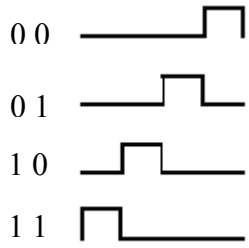


FIG II.14 – *Modulation PPM* **[26]**.

II.3.1.4 – Couche physique radio avec étalement de spectre en séquence directe HR/DSSS du standard 802.11b : [20]

La modulation CCK permet des transmissions à 5,5 et 11 Mbits/s dans le standard **IEEE 802.11**b. L'information est envoyée en utilisant des codes complémentaires spéciaux et sophistiqués. Le taux de chipping est de 11 Mchip/s avec une durée de symbole de 8 chips. Le débit de 5,5 Mbits/s est obtenu avec une transmission de 4 bits par symbole au lieu de 8 pour atteindre un débit de 11 Mbits/s.

La couche MAC supportée est toujours la même. Bien que la modulation utilisée soit différente, les canaux disponibles sont identiques à ceux autorisés pour la couche DSSS PHY à faible débit.

II.3.1.5 – Les techniques de modulation [27]

Le standard **802.11**b utilise une technique de modulation de phase appelée PSK. Cependant chaque bit produit une rotation de phase. Les débits peu élevés sont transmis par une rotation de 180° (technique appelée BPSK), tandis qu'une série de quatre rotations de 90° (technique appelée QPSK) permet d'atteindre des débits deux fois plus grands.

Le débit de la norme **802.11**b peut être optimisé par d'autres types d'encodage.

La méthode CCK permet d'encoder plusieurs bits de données en une seule puce (chip) en utilisant 8 séquences de 64 bits. Le codage simultané de 4 bits, permet d'obtenir un débit de 5.5 Mbps et celui de 8 bits permet d'obtenir un débit de 11 Mbps.

La technologie PBCC permet de réduire les effets de distorsions du signal dues aux multi trajets.

Les débits atteints sont de l'ordre de 22Mbit/s.

La norme **802.11**a opère dans la bande de fréquence des 5 GHz. Elle offre 8 canaux distincts. Pour bien profiter de ces canaux, une technique de transmission est proposée. L'OFDM permet d'obtenir des débits théoriques de 54 Mbps en envoyant les données en parallèle sur les différentes fréquences. De plus la technique OFDM fait une utilisation rationnelle du spectre (Tableau II.3).

Technologie	Codage	Type de modulation	Débit
802.11b	11 bits (Barker sequence)	PSK	1 Mbps
802.11b	11 bits (Barker sequence)	QPSK	2 Mbps
802.11b	CCK (4 bits)	QPSK	5.5 M bps
802.11b	CCK (8 bits)	QPSK	11 M bps
802.11a	CCK (8 bits)	OFDM	54 Mbps
802.11g	CCK (8 bits)	OFDM	54 Mbps

TAB II.3 – *Caractéristiques des technologies 802.11* **[27]**.

II.3.1.5.1 – La technique OFDM du standard 802.11 [20]

La norme **802.11** utilise la technique OFDM dans la bande 5 GHz. cette technique permet d'obtenir des débits de 54 Mbits/s, La largeur de bande disponible est de 455 MHz dont 200 sont alloués à l'usage en intérieur et 255 à l'usage en extérieur. Cette modulation résout les problèmes dus à la transmission multi trajets, plus particulièrement l'écho. Son principe est d'effectuer un multiplexage fréquentiel de sous porteuses orthogonales. Le canal est décomposé en cellules temps/fréquences qui seront transmises après une modulation QAM64. Le problème d'interférence inter-symbole lié à la réception multiple d'une même information (transmission multi chemins) pourrait être résolu, en insérant un intervalle de garde entre chaque symbole, et l'on choisit exactement la durée d'un symbole par rapport à l'étalement de l'écho.

La couche physique supportant la modulation OFDM est complexe, puisqu'elle fait appel à un ensemble de techniques de transmission telles que la modulation de phase, la transmission multi-porteuses OFDM, le codage convolutionnel et l'entrelacement.

II.3.1.5.2 – Principe de fonctionnement (figure II.15)

Dans la technique OFDM, la bande de fréquence est divisée en porteuses. L'utilisation de ces porteuses peut être simultanée, en y multiplexant les données. Un canal se compose de 52 porteuses de 300 KHz de largeur. Le transport de l'information utile utilise 48 porteuses et la correction d'erreur utilise 4 porteuses appelées porteuses pilotes. L'OFDM supporte une série de modulation et de codes permettant d'offrir l'ensemble des débits. Dans la bande (de 5,15 à 5,35 GHz), huit canaux de 20 MHz sont définis. Il est possible d'avoir une co-localisation de huit réseaux au sein du même espace et avoir un débit maximal de 432 Mbits/s.

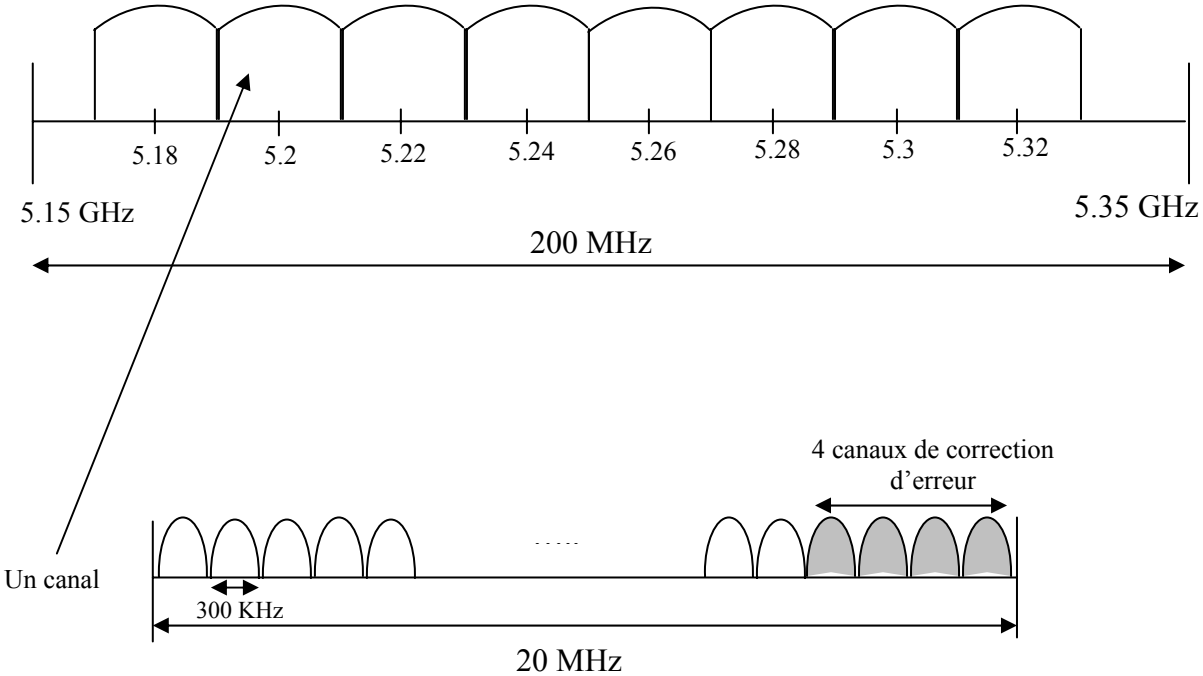


FIG II.15 – *Canaux OFDM dan la bande basse de 5 GHz* **[20]**.

La chaîne de transmission globale est résumée par le diagramme de la figure II.16.

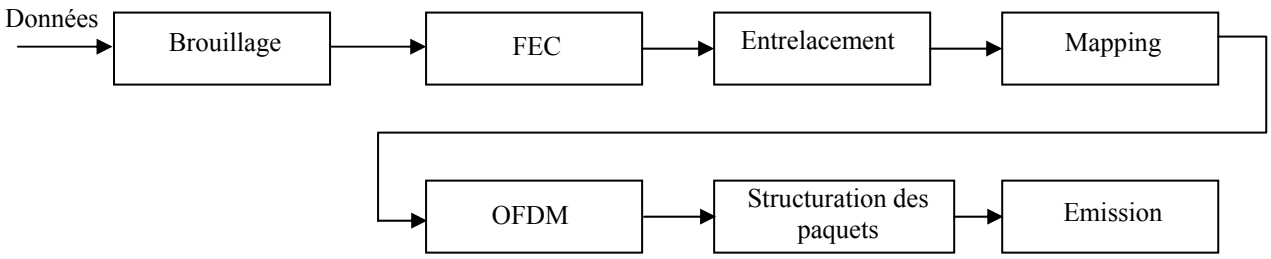


FIG II.16 – *La chaîne de transmission OFDM* **[20]**.

En premier lieu, il faut choisir le débit en fonction de l'état du lien radio, c'est une exécution d'un mécanisme automatique d'adaptation de lien.

Après la construction des trames, il faudrait réarranger les éléments de l'information (brouillage). Le codage appliqué est le FEC en ajoutant de la redondance.

En raison de renforcer la protection de l'information, on effectue un entrelacement des bits codés qui sont ensuite mappés en constellation de points (1, 2, 4 ou 6). Chaque groupe de bits représente un nombre complexe sont ensuite assemblés pour former un symbole OFDM, chacun de ces symboles lui est assigné une porteuse.

L'application de la modulation OFDM permet d'obtenir un signal en bande de base. La durée d'un symbole OFDM est de quatre microsecondes. Le paquet de la couche physique est ainsi construit en rajoutant les champs nécessaires (préambule…) à sa transmission sur les liens sans fil.

II.3.2 – Couche liaison de donnée

La couche liaison de données est la couche 2 du modèle OSI. Cette couche a pour objectif de réaliser le transport des données. La couche liaison de données de la norme **IEEE 802.11** est essentiellement composée de deux sous couches :

- LLC s'occupe de la structure de la trame.
- MAC définit le protocole d'accès au support.

La couche LLC utilise les mêmes propriétés que la couche LLC **802.2** et permet de relier un WLAN à tout autre réseau local appartenant à la famille **IEEE**. La couche MAC est spécifique à **IEEE 802.11** et définit des mécanismes nouveaux d'accès au support. Elle est indépendante des caractéristiques du support physique et des débits et supporte les deux topologies infrastructure et ad hoc **[20]**.

En plus de la transmission de données, d'autres services de base sont fournis tels que :

- Association/désassociation ;
- Confidentialité (mécanisme WEP etc.) ;

- Authentification et contrôle d'accès ;
- Fragmentation/réassemblage et séquencement ;
- Economie d'énergie.

Dans ce qui suit nous allons voir en détail les caractéristiques des deux sous couches.

II.3.2.1 – La couche de contrôle d'accès au support (Mécanisme d'accès au médium) [20]

La couche MAC définit deux méthodes d'accès différentes :

- La **DCF** qui est utilisée pour un accès distribué et aléatoire comme celui de **802.3** avec plusieurs autres algorithmes spécifiques aux WLAN. Elle est conçue pour prendre en charge le transport du trafic asynchrone. Les utilisateurs ont les mêmes droits d'accès au support. C'est donc une méthode d'accès de base avec contention.

- La **PCF** est spécifique pour un accès contrôlé. Cette technique est basée sur l'interrogation à tour de rôle des terminaux (polling), elle nécessite l'existence d'une unité de contrôle. PCF est conçue pour la transmission des données qui ont des contraintes telles que (voix, vidéo…). C'est une méthode optionnelle d'accès sans contention. CFP est la période du mode PCF et CP est la durée de contention.

Les informations relatives aux deux modes d'accès avec et sans contention sont diffuseés dans le BSS à travers les trames balises appelées Beacon frames ou Beacons (un Beacon est équivalent à la voie balise dans les réseaux GSM). On parle d'une supertrame constituée par une partie CFP à la suite de laquelle le contrôle passe en mode SCF. Le début d'une supertrame est délimité par une trame balise.

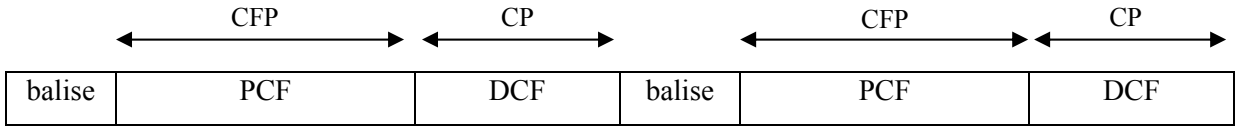


FIG II.17 – *Structure de la supertrame : Période d'accès sans contention CFP et période d'accès avec contention CP* **[20]**.

Nous allons voir en détail les deux types de mécanismes d'accès.

II.3.2.1.1 – La technique d'accès de base CSMA/CA [20]

Le mécanisme d'accès de base, appelé DCF est tout simplement le mécanisme CSMA/CA. Les protocoles CSMA sont bien connus de l'industrie, où le plus célèbre est Ethernet, qui est un protocole CSMA/CD.

Pour comprendre le principe du mécanisme CSMA/CA, nous allons examiner les problèmes radio qui ont guidé à développer un nouveau mécanisme inspiré du CSMA/CD mais adapté au contexte de la transmission sans fil. En effet, la transmission sans fil a entraîné des problèmes nouveaux inconnus dans le monde filaires tels que :

- Le problème des stations cachées ;
- Le problème des stations exposées ;
- L'effet *« proche-loin »* ou near-far **[20]**.

– Le problème de la station cachée :

Le problème du nœud caché (figure II.18) se produit lorsque deux stations séparées par une distance importante ne peuvent pas s'entendre l'une et l'autre. Mais elles ont des zones de couverture qui se recoupent.

Si les stations A et B détectent les porteuses en écoutant le canal et ne peuvent pas s'entendrent, elles vont s'autoriser à émettre en même temps. Á partir de là, si A et C veulent envoyer simultanément des paquets à une station B située dans l'intersection des zones de couverture, une collision entre les paquets sera produite, dans ce cas B ne pourra recevoir aucune des deux communications. Les stations A et C sont alors cachées l'une par rapport à l'autre **[20]**.

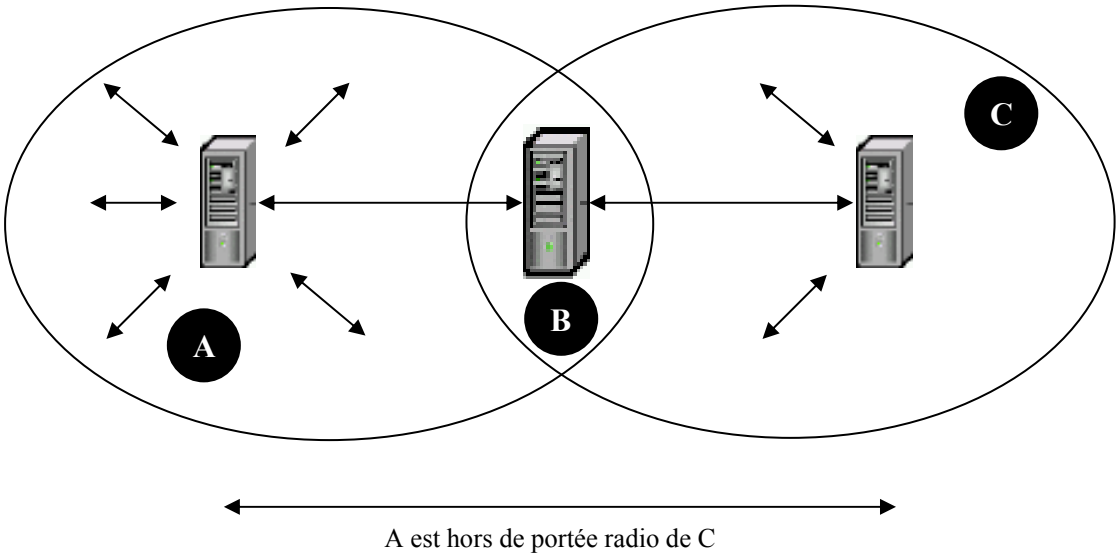


FIG II.18 – *Solutions Cachées* **[20]**.

– Le problème de la station exposée (figure II.19) :

Une station B transmet des données à A. Si C écoute le canal radio, elle écoute une communication en cours, donc elle constate qu'elle ne peut pas transmettre à D or si C transmettrait, cela créerait des collisions seulement dans les régions où les destinations D et A se situent **[20]**.

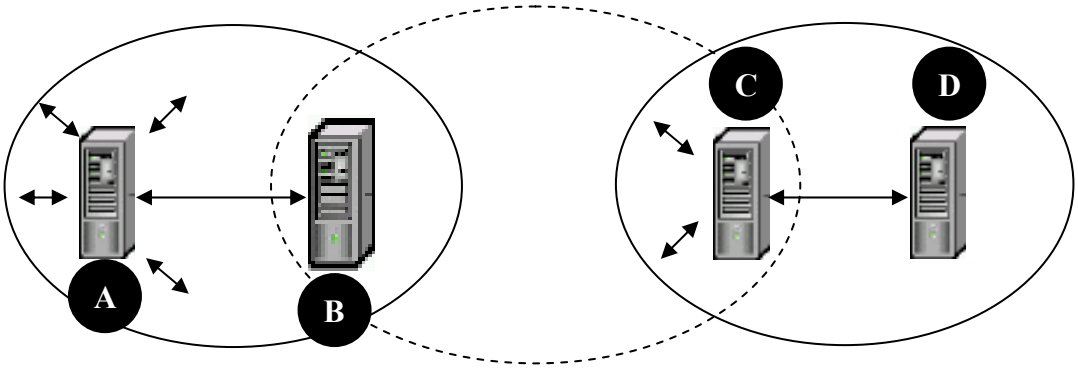


FIG II.19 – *Solutions Exposées* **[20]**.

Comme solution à ce problème, le standard **802.11** propose l'utilisation du mécanisme d'esquive de collision (Collision Avoidance) ; si une station veut émettre, elle écoute le support et s'il est occupé, la transmission est différée.

La station est autorisée à transmettre si le support est libre pour un temps spécifique (appelé DIFS, dans le cas de la transmission asynchrone). La station réceptrice va vérifier le CRC du paquet reçu et envoie un accusé de réception ACK. La réception de l'ACK indiquera à l'émetteur qu'aucune collision n'a eu lieu si l'émetteur ne reçoit pas l'accusé de réception, alors retransmet la trame après un ACK-TIMEOUT jusqu'à ce qu'il l'obtienne ou abandonne au bout d'un certain nombre de retransmission. La couche MAC et la couche physique travaillent en collaboration pour surveiller l'activité du réseau.

La couche physique utilise l'algorithme CCA pour évaluer la disponibilité du canal et mesure la puissance reçue par l'antenne appelée RSSI. Elle vérifie donc si le canal est libre en comparant la valeur de RSSI à un certain seuil et transmet par la suite à la couche MAC un indicateur de canal libre.

Dans le cas contraire, la transmission est différée selon les règles citées précédemment.

Globalement, le protocole CSMA/CA est basé sur :

- L'étude du support avec la détection de porteuses CS,
- Les temporisateurs IFS,
- L'utilisation d'acquittements positifs et l'évitement de collision,
- L'algorithme de Backoff,
- L'accès multiple.

A – Espace entre deux trames (IFS) (figure II.20) [7]

La norme **802.11** définit quatre types d'espace entre deux trames qui peuvent être vus comme des temporisateurs classés par ordre croissant.

- **SIFS :** Ce temporisateur est utilisé pour séparer les transmissions appartenant à un même dialogue (eg. Fragment – Ack). C'est le plus petit écart entre deux trames, il y a toujours, au plus, une seule station pour transmettre à cet instant, ayant donc la priorité sur toutes les autres stations. Cette valeur est fixée par la couche physique et est calculée dans le but que la station émettrice puisse commuter en mode réception pour décoder le paquet entrant. Pour la couche physique FH de **802.11**, cette valeur est de 28 microsecondes.

- **PIFS :** est utilisé par le Point d'Accès (appelé point coordinateur dans ce cas) pour gagner l'accès au support avant n'importe quelle autre station. Cette valeur est SIFS plus un certain temps (Slot Time, défini dans le paragraphe suivant), soit 78 microsecondes.

- **DIFS :** est l'IFS utilisé par une station voulant commencer une nouvelle transmission, et est calculé comme étant PIFS plus un temps, soit 128 microsecondes.

- **EIFS :** est l'IFS le plus long. Il est utilisé par une station quand la couche physique indique à la couche MAC qu'une transmission de trame a débutée et qu'aucune réception de trame MAC avec un FCS correcte n'a eu lieu. Ceci est nécessaire pour éviter que la station ne provoque de collision avec un futur paquet du dialogue en cours.

Ces temporisateurs définissent les degrés de priorités. La station voulant émettre les trames les plus prioritaires peut les envoyer en premier. Les informations les moins importantes concernant le trafic asynchrone seront émises après un temps d'attente plus long.

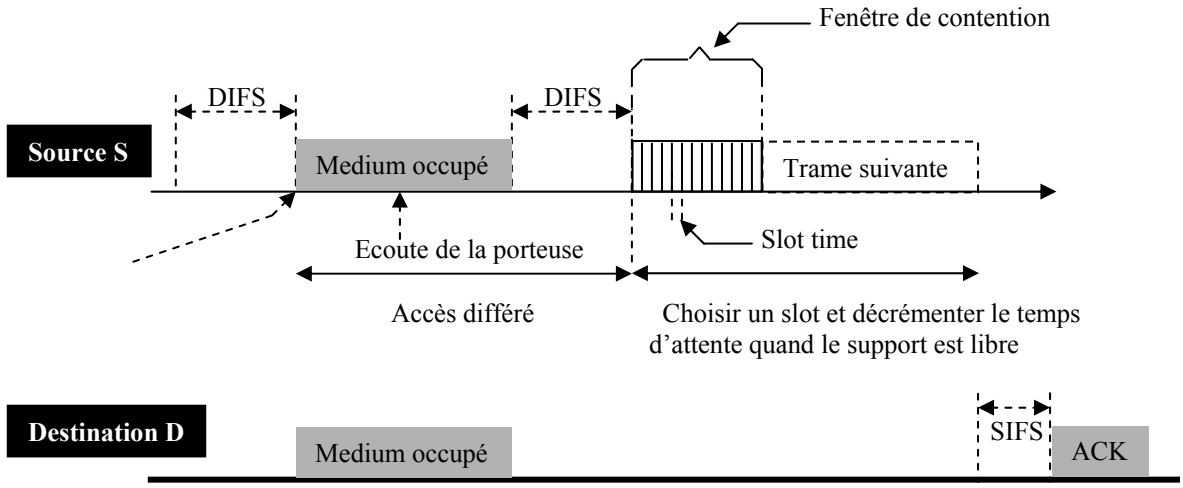


FIG II.20 –*Méthode d'accès CSMA/CA* **[20]**.

B – Algorithm de back off exponentiel

L'algorithme BEB est conçu pour résoudre le problème d'équité d'accès concurrent de plusieurs stations à un support partagé. Dans cette méthode, chaque station doit choisir un *« délai d'attente »*

aléatoire (appelé *backoff time*) compris entre 0 et la taille d'une fenêtre de contention. Ce nombre est exprimé en Slot : chaque station doit s'assurer qu'aucune station n'a émis avant elle **[20]**.

La durée d'un slot est définie de telle sorte que la station a accédé au support au début du slot précèdent. La valeur moyenne du délai d'attente croit exponentiellement avec le nombre de retransmissions en attente. Le standard **802.11** définit l'algorithme de back off exponentiel pour servir dans les cas suivants :

- Si une station veut émettre et trouve le support occupé, elle attend le temps aléatoire du back off avant d'essayer d'émettre à nouveau ;
- Après chaque retransmission ;
- Après une transmission réussie.

C – Mécanisme de réservation

C.1 – Ecoute du support [3]

Cette fonction est possible grâce aux procédures suivantes :

- Une procédure d'écoute nommée PCS au niveau de la couche physique. PCS effectue une analyse de toutes les trames passant sur le support hertzien et en détectant l'activité sur le support grâce à la puissance relative du signal des autres stations pour détecter la présence d'autres stations.
- Une procédure d'écoute au niveau de la couche MAC nommée VCS dans le cas d'une réservation du support.

Ces deux mécanismes peuvent être exploitées par un attaquant pour faire un audit sur le réseau et y pénétrer. Une étude a été effectuée à l'université de Californie aux USA à propos des vulnérabilités des réseaux 802.11 examinées ainsi que les mesures de sécurité à prendre. Le WEP n'est sans aucun doute plus un mécanisme de sécurité à déployer, d'un autre côté, l'authentification par filtrage MAC est susceptible au spoofng et donc n'est plus une méthode pour contrôler l'accès aux réseaux. L'analyse du trafic est un risque pour le réseau, cela pourrait compromettre à des attaques plus sérieuses, l'article avait pour bit de soulever les problèmes de sécurité et des solutions temporaires pour les réseaux **[28]**.

Le mécanisme de base est décrit par la figure II.20**,** en considérant le cas de la transmission de données asynchrones d'une source S à un destinataire D. Un fonctionnement similaire est adopté dans le cas de transmission des autres types de trames, il suffit de considérer le IFS adéquat.

C.2 – Mécanisme CSMA/CA avec échange de messages courts RTS et CTS (figure II.21) [20]

Malgré l'algorithme de reprise après collision BEB et l'acquittement des trames, il peut survenir des pertes dues à des collisions. Par contre, dans le cas où il existe des stations cachées, ou dans le cas de transmission de trames très longues, le standard définit un mécanisme qui permet de faire des

réservations du canal. Ce mécanisme est appelé écoute virtuelle de porteuses. Dans ce qui suit, nous allons décrire le mécanisme de fonctionnement.

Avant de commencer la transmission des données, une station transmet d'abord un petit paquet de contrôle appelé RTS, qui comprend la source, la destination et la durée de la transmission (c-à-d la durée totale de la transmission du paquet et de son accusé de réception). La station destination répond (si le support est libre) avec un paquet de contrôle de réponse appelé CTS, qui inclura les mêmes informations sur la durée.

Les stations qui reçoivent soit la trame comprenant la demande de réservation de canal RTS, soit la trame de réservation CTS, déclencheront leur indicateur de l'écoute virtuelle (Virtual Carrier Sense, appelé NAV), pour une certaine durée, et utiliseront cette information avec la procédure d'écoute du support.

Elles considèrent que le support est occupé pendant la durée précise dans les paquets de contrôle RTS et CTS. Si la source ne reçoit pas le paquet de contrôle CTS, elle suppose qu'il y a eu collision et retransmet le paquet RTS après une durée d'attente aléatoire selon le principe de base.

Si le destinataire reçoit correctement le paquet CTS, la source émet un acquittement pour signaler au destinataire que le paquet CTS a bien été reçu.

La communication pourra ensuite avoir lieu. Cette procédure s'apparente aux procédures d'allocation de ressources par le biais de la durée précise dans les paquets RTS et CTS.

Ce mécanisme réduit la probabilité de collision qui peut être causée par une station cachée de l'émetteur dans la zone du récepteur grâce à la courte durée de transmission du RTS, parce que la station entendra le paquet de contrôle CTS et considérera le support comme occupé jusqu'à la fin de la transmission. L'information durée dans le paquet RTS protége la zone de l'émetteur des collisions pendant la transmission de l'accusé de réception.

Le diagramme suivant montre une transmission entre deux stations et la valeur NAV de leurs voisins.

Grâce au fait que RTS et CTS sont des trames courtes, le nombre de collisions est réduit. Ces trames étant reconnues plus rapidement que si toute la trame MAC devait être transmise.

Le mécanisme CSMA/CA avec RTS/CTS est un mécanisme qui permet la transmission de données et la réception de l'ACK sans collision. Cependant, il est conseillé de l'utiliser également pour envoyer de longues trames pour lesquelles une retransmission serait trop coûteuse en termes de bande passante.

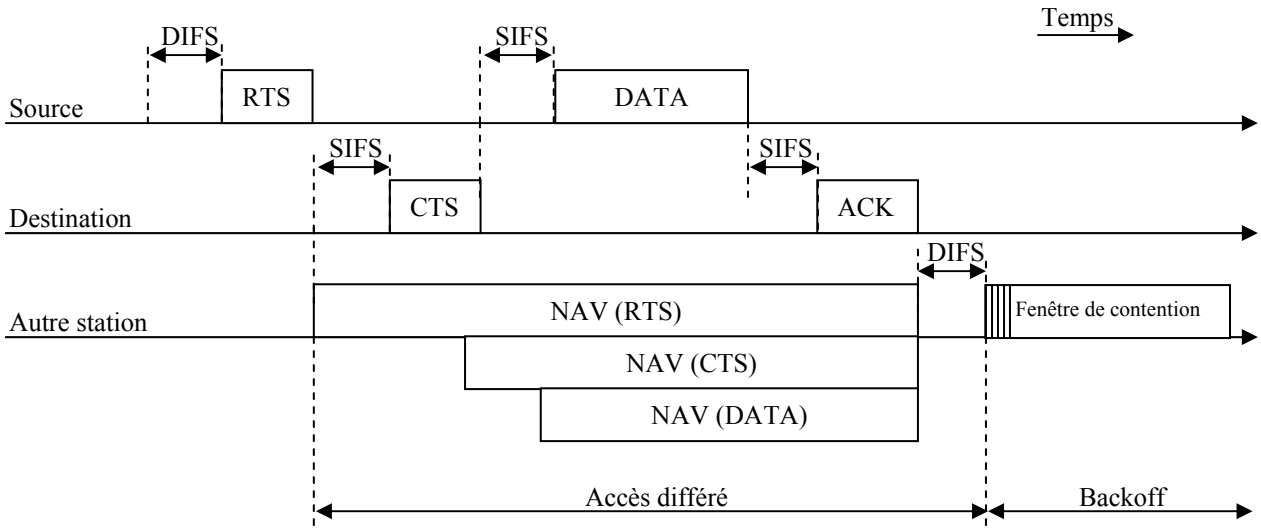


FIG II.21 – *Mécanisme d'écoute virtuelle de porteuse avec messages RTS/CTS* **[20]**.

❖ Comment peut-on apporter une solution au problème des stations cachées grâce à ce mécanisme ?
Considérons la structure réseau représentée dans la figure II.18.

La station C est cachée par rapport à la station A. considérons le cas ou la station A transmet des données à B. la station C ne détecte pas l'activité de la station A. dans ce cas, la station B peut transmettre librement sans interférer avec la transmission de la station C. si les stations A et B s'échangent des messages RTS/CTS, la station C est informée grâce à l'envoi d'un message CTS par la station B que le support est occupé.

C n'essaie donc pas de transmettre durant la transmission entre A et B.

Si l'on fait l'écoute virtuelle de porteuse, l'envoi de paquets de contrôle CTS par le destinataire B permet de résoudre le problème des nœuds cachés. En effet, grâce à son paquet CTS, B va atteindre toutes les stations de sa zone de couverture et donc avertir toutes les stations qui voudraient potentiellement émettre.

La norme **802.11** de base spécifie que la technique de base DCF est celle qui est utilisée par défaut et que les autres procédures CSMA/CA avec RTS/CTS et PCF sont optionnelles **[20]**.

II.3.2.1.2 – La fonction PCF

Cette méthode est spécifique pour les transmissions de données temps réel. Concrètement, les stations envoient des trames spéciales appelées PR, auxquelles l'AP répond en envoyant les données demandées.

Pour contrôler l'accès au support, l'AP dispose d'une priorité supérieure en utilisant des PIFS, qui sont plus courts que les DIFS, utilisés par les stations. Cependant, l'AP doit également s'assurer que les stations puissent accéder au support au moyen de la DCF, c'est pourquoi les deux méthodes

sont alternées : une période dite CFP pour la PCF, et une période dite CP pour la DCF, alternée par une trame balise permettant de synchroniser les stations. A notre connaissance, aucun équipement **802.11** grand public n'implémente la PCF, mais on peut la trouver sur les équipements professionnels.

Des analyses de performances de ce protocole ont montré qu'il n'était pas adapté aux transmissions d'un trafic avec des contraintes de temps fortes et donc de ce fait aucun produit sur le marché ne l'a implémenté. Il est possible que si une station prend le canal, elle peut le monopoliser pendant un temps long et les trames balises peuvent être retardées. Un successeur, le mécanisme HCF proposé par le groupe de travail **802.11**e, sera intégré dans les produits futurs.

II.4 – FORMATS DES TRAMES USUELLES [29]

II.4.1 – Trame MAC

Les figures II.22 et II.23 montrent le format général de la trame MAC, certains champs sont seulement présents dans une partie des trames, comme décrit ultérieurement.

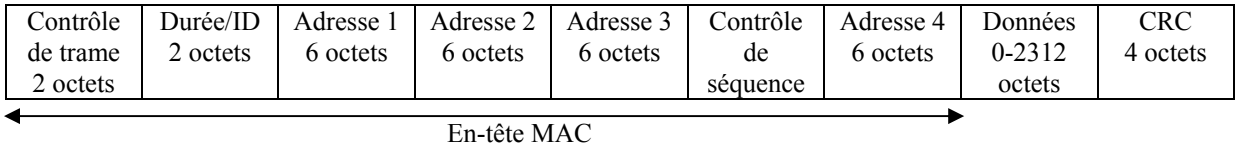


FIG II.22 – *Trame MAC* **[29]**.

Contrôle de trame : champ de 2 octets se divisant comme suit :

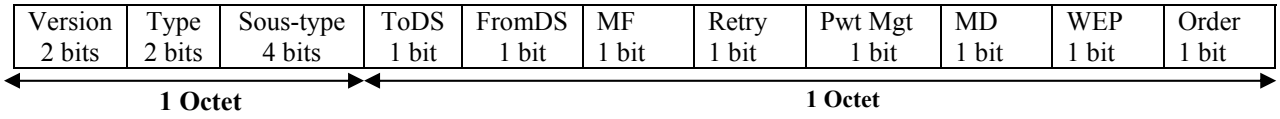


FIG II.23 – *En-tête MAC* **[29]**.

II.4.2 – Trame RTS (figure II.24)

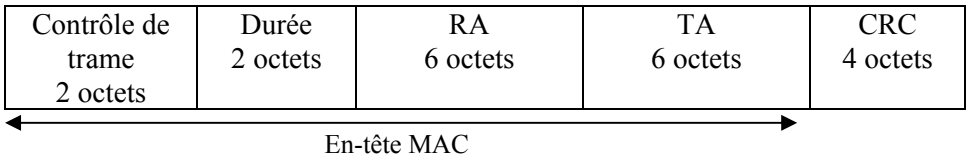


FIG II.24 – *Trame RTS* **[29]**.

– **Durée** : temps nécessaire, en microsecondes, à la transmission de la trame de données ou de gestion suivante, plus une trame CTS, ACK et trois SIFS.

– **RA** : adresse du récepteur de la prochaine trame de données ou de gestion.

– **TA** : adresse de la station qui émet la trame.

– **CRC** : somme de contrôle.

II.4.3 – Trame CTS (figure II.25) [20]

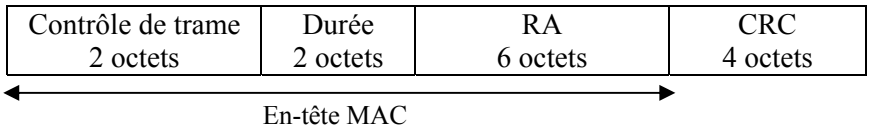


FIG II.25 – *Trame CTS* **[29]**.

– Durée : valeur obtenue dans la trame RTS, moins le temps de transmission, en microsecondes, de la trame CTS et d'un intervalle SIFS.

– RA : adresse du récepteur de la trame CTS, obtenue du champ TA de la trame RTS.

– CRC : somme de contrôle.

II.5 – FONCTIONNALITES

Plusieurs fonctionnalités sont supportées par le standard **802.11**. Dans cette partie, nous ferons appel à quelques fonctionnalités importantes.

II.5.1 – Fragmentation et réassemblage [20]

La technique de fragmentation est utilisée dans le contexte de communications sans fil pour permettre d'optimiser la fiabilité de transmission. Les trames de taille importante sont ainsi divisées en petits fragments.

Dans les réseaux locaux sans fil, il est essentiel de manipuler des paquets de petite taille pour les raisons suivantes :

- Le taux d'erreur par bit est plus important sur une liaison radio que sur un support physique fixe. La probabilité d'un paquet d'être corrompu augmente proportionnellement avec sa taille.
- Le surdébit par les retransmissions successives de paquets corrompus : plus les détails des paquets sont petits, tout en ayant une taille minimale pour laquelle l'overhead reste négligeable par rapport à la charge utile de la trame, moins ce surdébit est important.

Lorsque la taille de la trame **802.11** excède une valeur seuil, elle doit subir une fragmentation. Cette valeur seuil est appelée fragmentation_threshold, initialisée par l'administrateur du réseau.

Les fragments de la trame sont alors transmis séquentiellement. Le support n'est libéré que si tous les fragments sont transmis correctement.

Si un ACK n'est pas correctement reçu, la station arrête de transmettre et essaie d'accéder de nouveau au support et reprend la transmission à partir du dernier fragment non acquitté.

Dans le cas où le mécanisme RTS/CTS est utilisé par les stations, seul le premier fragment envoyé utilise les trames RTS/CTS (figure II.26). Le canal sera donc réservé pour la durée totale de transmission des fragments.

La transmission de chacun des fragments est encadrée par deux SIFS et les stations non concernées par l'échange mettent à jour progressivement leurs NAVs respectifs.

Du coté récepteur, il y aura besoin d'une procédure de réassemblage des fragments.

Les procédures de fragmentation/réassemblage sont assez simples, elles se basent sur un algorithme d'envoi et d'attente d'accusé de réception, où la station émettrice n'est pas autorisée à transmettre un nouveau fragment tant qu'un des deux événements suivants n'est pas survenu :

- Réception d'un acquittement ACK du fragment en question,
- Décision que le fragment a été retransmis trop souvent et abondan de la transmission de la trame.

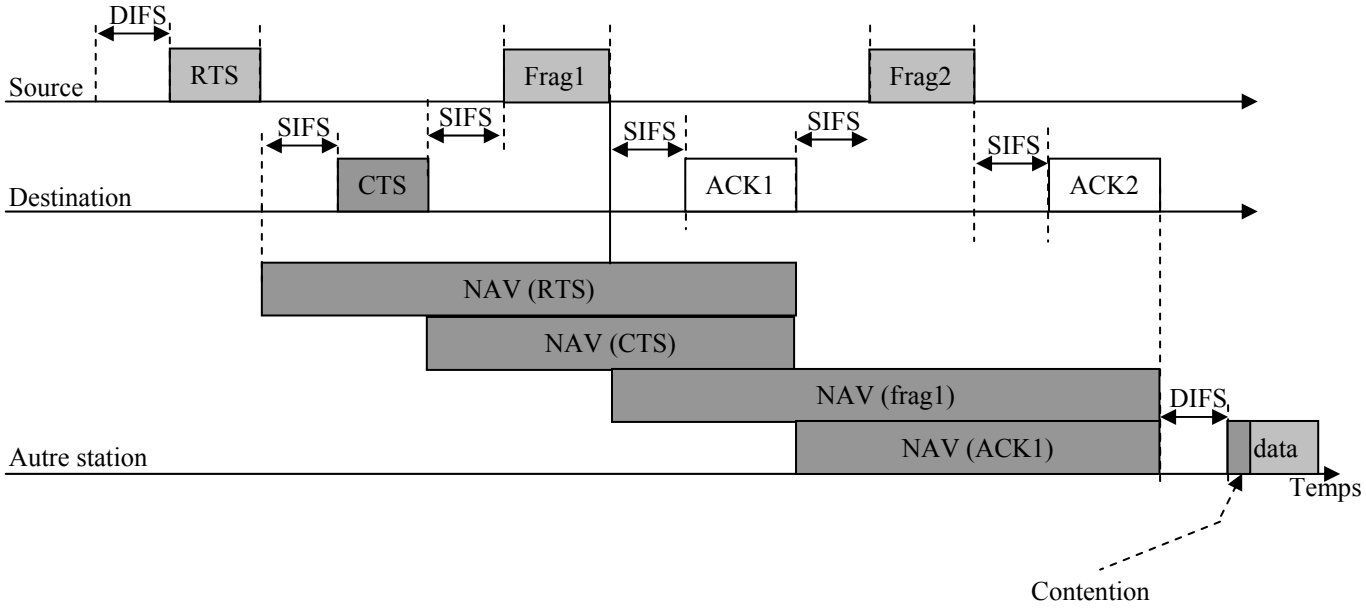


FIG II.26 – *CSMA/CA avec RTS/CTS et fragmentation/réassemblage.*

II.5.2 – Le handover

Le service du *handover* est primordial pour garantir une QoS constante lors d'un déplacement d'une cellule à une autre.

Lors d'un changement de cellule, les terminaux doivent pouvoir rester synchronisés. Au sein d'un BSS, une station synchronise son horloge avec celle de l'AP. Celui-ci doit envoyer périodiquement des trames, appelées BF et contenant la valeur de son horloge, afin de garder la synchronisation.

A la réception des BF, la station met à jour sa propre horloge en la synchronisant avec le point d'accès. Pour qu'un terminal puisse accéder à un BSS ou à un ESS formé de plusieurs AP, deux méthodes se présentent alors pour choisir l'AP le plus approprié (en fonction de la puissance du signal, du taux d'erreur des paquets et de la charge du réseau) :

– ***L'écoute passive :*** la station se met en attente de réception d'une BF venant d'un point d'accès.

– ***L'écoute active :*** lorsque la station a trouvé l'AP le plus approprié, elle lui envoie une requête d'association sous forme de trame PRF et attend la réponse du point d'accès avant de s'y associer.

Lorsqu'un terminal est accepté par un AP, il se règle sur son canal radio le plus approprié.

Cependant, il reste à l'écoute des autres canaux du réseau afin d'évaluer les performances d'autres points d'accès et les comparer à sa connexion. Si un AP possède de meilleures performances, le terminal s'y associe. Pour éviter les encombrements sur un point d'accès, une fonction d'équilibrage de charge, le Load Balancing, permet de mieux répartir la charge au sein d'un ESS **[30]**.

II.5.3 – Le roaming

Le roaming est un processus qui permet le mouvement d'une cellule vers une autre sans déconnexion. Cette fonction est semblable au *« handover »* des téléphones portables, avec deux différences majeures :

- Les LAN véhiculent des paquets entre deux cellules, contrairement à la téléphonie mobile où les transitions peuvent survenir au cours d'une conversation.

- les conversations peuvent ne pas être affectées par une déconnexion, alors que la communication des paquets, les performances seront considérablement réduites à cause de la retransmission qui sera exécutée par les protocoles des couches supérieures.

Le standard **802.11** ne définit pas comment le roaming est fait, mais en définit cependant les règles de base. Celles ci comprennent l'écoute active ou passive, le processus de ré-association, où une station qui passe d'un Point d'Accès à un autre sera associée au nouveau Point d'Accès **[30]**.

Le processus de roaming procure plusieurs avantages qui sont :

- Simplicité de l'extension de la couverture radio,
- Equilibrage de la charge du réseau,
- Evolutivité du réseau ;
- Transparence pour l'utilisateur.

II.5.4 – Synchronisation (figure II.27) [20]

Le déplacement des terminaux nécessite une synchronisation pour pouvoir communiquer. Au niveau d'un BSS, les stations synchronisent leurs horloges avec l'horloge du point d'accès. Pour le maintient

de la synchronisation, le point d'accès envoie périodiquement des trames balises qui contiennent la valeur de l'horloge du point d'accès. Dés réception de ces trames, les stations mettent à jour leurs horloges. La structure qui permet de maintenir les temporisateurs de toutes les stations de la même cellule synchronisées est appelée TSF ; elle est diffusée périodiquement dans la trame balise (beacon).

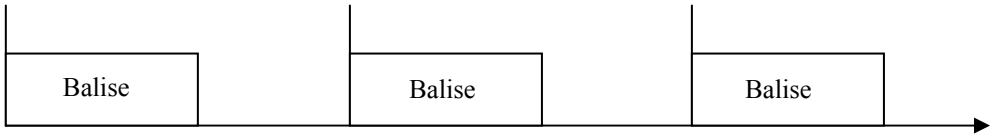


FIG II.27 – *Mécanisme de synchronisation selon l'espace temps.*

II.5.5 – La gestion d'énergie

La plupart des terminaux mobiles ont peu d'autonomie. Afin d'en augmenter le temps d'activité, le standard a prévu un mode d'économie d'énergie. Deux modes de travail sont ainsi disponibles pour un terminal : le CAM et le PSPM. Le CAM représente le fonctionnement par défaut : la station reste allumée et écoute constamment le support.

Le PSPM permet une économie d'énergie. L'AP tient à jour un enregistrement de toutes les stations qui sont en mode d'économie d'énergie, tout en stockant les données qui leurs sont adressées. Les stations en veille s'activent à des périodes de temps régulières pour recevoir un type de trame bien particulier, la trame TIM, envoyée par l'AP. Les stations retournent en mode veille entre deux trames TIM, mais elles partagent toutes le même intervalle de temps, de façon à s'activer au même moment pour les recevoir.

Les trames TIM font savoir aux terminaux mobiles si elles ont ou non des données stockées dans le point d'accès. Lorsqu'un terminal reçoit une trame TIM annonçant que l'AP contient des informations qui lui sont destinées, il envoie au point d'accès une requête, appelée Polling Request Frame, pour mettre en place le transfert de données. Après réception complète des données, le terminal se remet en mode veille **[29]**.

II.5.6 – Qualité de service

La qualité de service est toujours un élément essentiel dans n'importe quel réseau. Les réseaux **802.11** posent de nombreux problèmes en ce point.

Le débit réel du réseau n'est pas stable et peut varier dans le temps de plus, le réseau étant partagé, les ressources sont divisées entre tous les utilisateurs se trouvant dans la même cellule.

En ce qui concerne la première difficulté, les points d'accès **Wi-Fi** ont la particularité assez astucieuse de s'adapter à la vitesse des terminaux. Lorsqu'une station n'a plus la qualité suffisante pour émettre à 11 Mbps, elle dégrade sa vitesse à 5.5 puis 1 Mbps.

Cette dégradation provient soit d'un éloignement, soit d'interférences. Cette solution permet de conserver des cellules assez grandes, puisque le point d'accès s'adapte. L'inconvénient est qu'il est impossible de prédire le débit d'un point d'accès.

Le groupe de travail **802.11**a défini la norme **IEEE 802.11**e dans le but d'améliorer la qualité de service dans les réseaux **Wi-Fi** **[3]**.

Cette extension permet de faire transiter plus facilement les applications à fortes contraintes temporelles, comme les applications multimédias. Pour cela, il a fallu définir des classes de services et permettre aux terminaux de choisir la bonne priorité en fonction de la nature de l'application transportée. La gestion des priorités s'effectue au niveau du terminal par l'intermédiaire d'une technique d'accès au support physique modifiée par rapport à celle utilisée dans la norme de base **IEEE 802.11**. Les stations prioritaires ont des temporisateurs d'émission beaucoup plus courts que les stations non prioritaires, ce qui leur permet de prendre l'avantage lorsque deux stations de niveaux différents essayent d'accéder au support.

II.5.7 – Sécurité [20]

Les problèmes de sécurité et de confidentialité compliquent la mise en place d'un réseau local sans fil. Même si certains dispositifs de sécurité sont intégrés aux réseaux locaux sans fil, leur sécurité peut être aisément violée si les précautions pertinentes ne sont pas prises en compte.

Le comité **802.11**a apporté une solution au problème de sécurité en élaborant tout au début un protocole appelé WEP, mais les défaillances importantes ont vite été décelées dans les mécanismes proposés. Les mécanismes de sécurité dans les réseaux **Wi-Fi**, seront développés dans le chapitre suivant.

II.6 – Wi-Fi ET LES AUTRES TECHNOLOGIES

Le succès de la technologie **Wi-Fi**, grâce aux avantages qu'elle offre aux utilisateurs, attire un grand nombre d'opérateurs Télécom qui considère le **Wi-Fi** comme complémentaire de la **3G**.

Le **Wi-Fi** apparaît comme une technologie complémentaire à la BLR car elle apporte la capillarité du *« dernier mètre»* en complément du *« dernier kilomètre »* des réseaux d'accès qui collectent le trafic sachant que les débits offerts par la BLR sont inférieurs à 3 Mbits/s **[20]**.

La BLR est implémentée en Algérie. C'est Algérie Télécom et l'opérateur *«* Huawei *»* qui détient le marché. C'est une solution efficace pour résoudre le problème des zones difficiles ou là où il y a une pénurie de lignes bifilaires.

II.7 – CONCLUSION

Une description d'une manière générale des réseaux **Wi-Fi** a fait l'objet de ce chapitre. Les réseaux **Wi-Fi** connaissent une croissance considérable, leur souplesse d'utilisation et de déploiement séduit les administrateurs réseau. D'autre part les organismes de régulation se mobilisent pour répondre à tous les points noirs de cette technologie notamment la sécurité et la qualité de service.

La sécurité constitue un problème crucial, les entreprises et les administrateurs deviennent plus exigeants sur les garanties de sécurité que leurs apportent les fournisseurs. La sécurité apparaît comme l'un des enjeux majeurs pour les fabricants. Leur objectif principal est donc de pallier aux limitations des mécanismes de sécurité dans les systèmes actuels.

Le prochain chapitre est consacré à la description des mécanismes de base de la sécurité des réseaux sans fil.

3

Les mécanismes de sécurité Wi-Fi

L'installation des réseaux **Wi-Fi** dans les entreprises et les établissements nécessite une étude détaillée des risques encourus avant la mise en service du réseau.

Cependant les normes de sécurité proposent des solutions plus ou moins efficaces, selon l'architecture du réseau et les services pour lesquels il est destiné. Ces solutions proposées doivent correspondre aux fonctionnalités des réseaux étudiés, tous cela pour ne pas nuire au bon fonctionnement du réseau et ne pas encombrer le trafic par de lourds algorithmes de sécurité.

Ce chapitre inclût les mécanismes de sécurité mis en œuvre dans les environnements **Wi-Fi**. Ces mécanismes sont implémentés directement dans les matériels commercialisés. Pour ce fait, nous commencerons par l'introduction des mécanismes de sécurité proposés par les normalisations. Ces mécanismes ne résistent pas pour autant aux attaquants aguerris; car les concepteurs n'ont pas prévu des technologies suffisamment en avance pour résister à l'effet du temps.

Malgré ces limitations, il existe des solutions pour protéger efficacement un réseau **Wi-Fi**. C'est le cas du WPA2, ou des mécanismes VPN et de carte à puce.

La sécurité des réseaux Informatiques est un domaine très vaste. Les attaques réseau sont aujourd'hui si nombreuses qu'il serait illusoire de prétendre les décrire toutes. Il est important de dresser une topologie des faiblesses de sécurité afin de mieux appréhender ces attaques, qui ont pour point commun d'exploiter des faiblesses de sécurité.

La sécurité réseau est recensée beaucoup plus dans les réseaux sans fil que dans les réseaux filaires (câblés).

Les organismes de sécurité ont mis au point des mécanismes pour remédier aux problèmes de sécurité des réseaux locaux face aux intrusions illicites et les attaques.

Dans ce qui suit, nous allons donner un aperçu sur la sécurité des réseaux informatiques d'une manière générale, afin de connaître les menaces, les attaques et les protocoles de sécurité existants.

III.1 – INTRODUCTION Á LA SÉCURITÉ RÉSEAU

III.1.1 – Architecture Réseau

La conception d'une architecture réseau doit être préméditée. Le terme *« architecture réseau »* contient les exigences, les méthodes, l'organisation et les équipements utilisés pour créer un réseau, composants physiques et mesures de sécurité compris **[30]**.

Une fois l'organisation des composants et la gestion des menaces assimilées, une architecture valable peut être élaborée.

III.1.2 – Les menaces

Avant la conception d'un réseau quelconque, une étude au préalable doit être effectuée concernant les attaques auxquelles le réseau doit faire face. Ces attaques peuvent être classées en trois catégories :

- Attaques externes.
- Attaques internes.
- Attaques physiques **[30]**.

La connaissance des menaces qui pèsent sur un réseau connecté à Internet permet aux concepteurs du réseau de protéger les systèmes des attaques, de limiter la vulnérabilité en cas de faille et d'isoler les interactions possibles.

« Une architecture réseau sécurisée affecte la rapidité de réaction des établissements et des entreprises en cas d'attaque et permet d'améliorer la restauration d'un système saint tout en augmentant la fiabilité et les performances » **[30]**.

« Une bonne maintenance et une veille régulière au niveau des nouvelles techniques de sécurité permettent également de réduire les risques » **[30]**.

III.1.2.1 – Attaque externes

Ces attaques découlent d'Internet ou de systèmes se trouvant au-delà du périphérique d'accès et ciblent des systèmes internes ou externes. Ce sont les attaques les plus médiatisées. C'est le cas d'une modification de page Web, de Chevaux de Troie ou d'Interruption de services dues à des hackers.

La protection contre ces attaques passe par l'utilisation de pare-feu ; de périphériques de surveillance réseau, par la distribution de services sur plusieurs réseaux et par la mise en place d'une restriction de bande passante par service et par protocole **[30]**.

III.1.2.2 – Attaques Interne

Cette attaque provient du cœur de l'entreprise. Les attaques internes sont les plus fréquentes. C'est le cas d'un employé en colère, d'utilisateurs curieux ou de manipulations accidentelles. Pour faire face à ces attaques, les concepteurs doivent parvenir à une sécurité maximale sans pour autant nuire au fonctionnement du réseau.

Pour remédier à ces problèmes, il faudrait attribuer aux utilisateurs suffisamment d'accès et de privilège pour leur permettre d'effectuer leur travail tout en assurant la protection au niveau interne **[30]**.

III.1.2.3 – Attaque physiques

L'accès physique représente la dernière catégorie de menace. La possibilité d'atteindre physiquement un système ou une partie du réseau représente un danger majeur.

L'emplacement et l'accès aux équipements réseaux doivent être protégés physiquement. La conséquence d'une telle attaque est de pouvoir sniffer les paquets qui circulent et intercepter les mots de passes ou toute autre information privée **[30]**.

❖ Les réseaux qu'ils soient d'entreprise, domestiques ou de l'université subissent des attaques. Le dimensionnement d'un réseau en matière de sécurité est une sécurité primaire. Il faudrait la proposition d'architectures réseau sécurisées.

III.1.3 – Les Attaques

III.1.3.1 – Attaques par TCP

Le protocole TCP utilise des numéros de port qui permettent de déterminer une adresse de socket, c-à-d d'un point d'accès au réseau **[31]**. Cette adresse de socket est obtenue par la concaténation de l'adresse IP et de l'adresse de port. Une attaque par TCP revient à utiliser un point d'accès pour faire

autre chose que ce pour quoi le point d'accès a été défini. En particulier, un pirate peut utiliser un port classique pour entrer dans un ordinateur ou dans le réseau d'une entreprise **[31]**.

Le schéma de la figure III.1 représente une attaque par le protocole TCP, l'utilisateur ouvre une connexion TCP sur un port correspondant à l'application qu'il projette de dérouter. Le pirate commence à utiliser le même port en se faisant passer pour l'utilisateur et se fait envoyer les réponses. Éventuellement, le pirate peut prolonger les réponses vers l'utilisateur de telle sorte que celui-ci reçoive bien l'information demandée et ne puisse pas se douter de quelque chose.

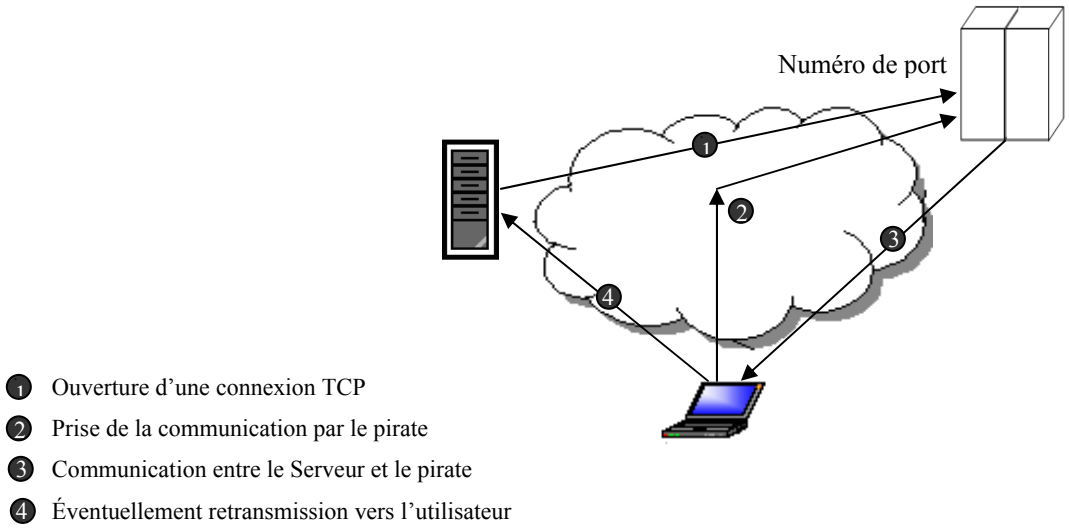


FIG III.1 – *Une attaque par le protocole TCP.*

III.1.3.2 – Les Attaques par Cheval de Troie

Le nom de cette attaque est tiré de la ruse imaginée par Ulysse durant la guerre de Troie. L'attaque par Cheval de Troie consiste à installer un programme, qui permet de mémoriser le login et le mot de passe, est introduit dans la station terminale. Ces informations sont envoyées vers l'extérieur par un message sur une boite aux lettres anonymes. Diverses techniques peuvent être utilisées, pour cela, allant d'un programme qui remplace le gestionnaire de login jusqu'à un programme piraté qui espionne ce qui se passe dans le terminal **[31]**.

III.1.3.3 – Les attaques par dictionnaire

La plupart des mots de passe utilisés existent sur le dictionnaire. Un automate est capable de les essayer tous.

La solution la plus simple est d'utiliser des mots de passe compliqués en rajoutant des lettres majuscules, des chiffres et des signes **[31]**.

III.1.3.4 – Les autres attaques

Les attaques sont tellement nombreuses qu'il serait difficile de les évoquer toutes.

Les attaques par écoute consistent, pour un pirate à écouter une ligne de communication et à interpréter les éléments binaires interceptés.

Les attaques par fragmentation sont possibles grâce aux informations de reconnaissance qui se trouvent dans le premier paquet provenant de la fragmentation d'un message. La valeur de bit de fragmentation peut être modifiée dans le but de faire croire que le message est composé de plusieurs segments. Le *firewall* doit donc arriver une succession de fragments sans se douter que le seul fragment de la communication est le premier et que ceux qui suivent sont ceux du pirate.

Les algorithmes de routage sont à la base de nombreuses attaques. Le fait de modifier les tables de routage, le pirate peut récupérer de nombreuses informations qui ne lui sont pas destinées.

De la même façon, de nombreuses attaques sont possibles par une perturbation de protocoles comme ARP, soit pour prendre la place d'un utilisateur, soit en captant des données d'un autre **[31]**.

III.1.4 – Les services de sécurité

Le terme sécurité dans le domaine Informatique concerne la protection des informations. L'ISO a pris en charge toutes les mesures nécessaires pour assurer la sécurité des données durant leur transmission. Ces travaux ont procréé un standard international, ISO 7498- 2. Cette architecture est très utile pour l'implémentation des éléments de sécurité dans un réseau car elle décrit en détail les grandes fonctionnalités et leur emplacement par rapport au modèle de référence **[31]**.

Trois concepts ont été définis :

- Les fonctions de sécurité, qui sont déterminées par les actions pouvant compromettre la sécurité d'un établissement.
- Les mécanismes de sécurité, qui définissent les algorithmes à mettre en œuvre.
- Les services de sécurité, qui représentent les logiciels et les matériels mettant en œuvre des mécanismes dans le but de mettre à la disposition des utilisateurs les fonctions de sécurité dont ils ont besoin.

Cinq types de sécurité ont été définis :

- La confidentialité, qui doit assurer la protection des données : contre des attaques non autorisées.
- L'authentification, qui doit permettre de s'assurer que celui qui se connecte est bien celui qui correspond au nom indiqué.

- L'intégrité, qui garantit que les données reçues sont exactement celles qui ont été émises par l'émetteur autorisé.
- La non-répudiation, qui permet d'assurer qu'un message a été bien envoyé par une source spécifiée et reçu par un récepteur spécifié.
- Le contrôle d'accès, qui a pour fonction de prévenir l'accès à des ressources sous des conditions définies et par des utilisateurs spécifiés.

En combinant les cinq services de sécurité présentés précédemment et les besoins de l'émetteur et du récepteur, nous obtenons le processus suivant :

1- Le message ne doit parvenir qu'au destinataire.
2- Le message doit parvenir au bon destinataire.
3- L'émetteur de message doit pouvoir être connu avec certitude.
4- Il doit y avoir identité entre le message reçu et le message émis.
5- Le destinataire ne peut contester la réception du message.
6- L'émetteur ne peut contester l'émission du message.
7- L'émetteur ne peut accéder à certaines ressources que s'il en a l'autorisation.

Le besoin 1 correspond à un service de confidentialité. Les besoins 2 et 3 à un service d'authentification, le besoin 4 à un service d'intégrité des données les besoins 5 et 6 à un service de non-répudiation et le besoin 7 au contrôle d'accès **[31]**.

III.1.4.1 – Confidentialité

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

Un message écrit en clair est transformé en un message chiffré, appelé *« cryptogramme »* grâce aux algorithmes de chiffrement. Cette transformation est fondée sur une ou plusieurs clés **[3]**.

III.1.4.1.1 – Chiffrements

Le chiffrement se distingue en deux types :

A – Le chiffrement symétrique

Le chiffrement le plus simple est celui où les seuls émetteur et récepteur partagent une clé unique et secrète. Les systèmes à clés secrètes sont des systèmes à *« clés symétriques »*. Ils utilisent la même clé pour effectuer la transformation f et sa transformation inverse f^{1}. La figure III.2 illustre cet algorithme **[3]**.

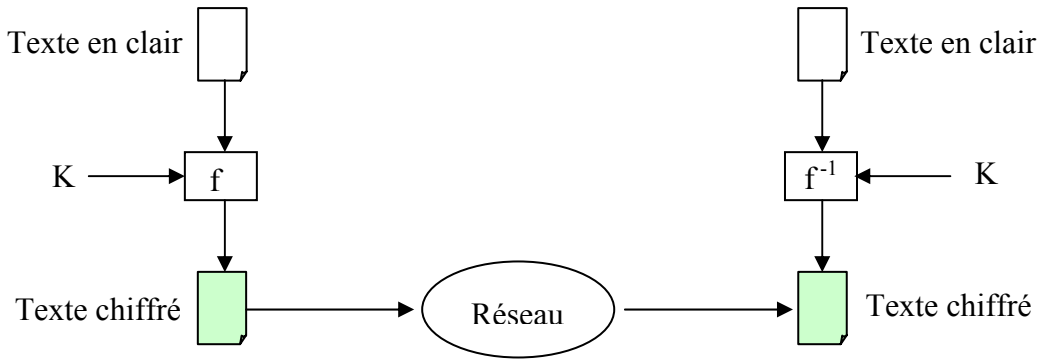


FIG III.2 – *Chiffrement symétrique* **[3]**.

B – Le chiffrement asymétrique

Le principe des algorithmes de chiffrement asymétriques est identique à celui des systèmes à clé publique. Le destinataire est le seul qui détient la clé de chiffrement. Le degré de sécurité est élevé, puisque même l'émetteur ne connaît pas cette clé. L'algorithme le plus répandu est RSA, où la fonction d'inversion d'une puissance est quasi-impossible. La clé permettant de déchiffrer le message est constituée de deux nombres, P et Q, d'environ 250 bits chacun. La clé publique est obtenue par la formule **[3]** :

$$N = P*Q. \qquad \textbf{(III.1)}$$

Le fait que n est très grand, il est presque impossible de trouver toutes les factorisations possibles. La connaissance de n ne permet donc pas de déduire ni P ni Q **[3]**.

À partir de P et de Q, E et D sont choisi, tels que :

$$E.D = 1 \bmod (P-1)\,(Q-1). \qquad \textbf{(III.2)}$$

De même, la connaissance de E ne permet pas de déduire la valeur de D.

Soit M un message à chiffrer. L'algorithme de chiffrement du message est obtenu par :

$$M^e \bmod N. \qquad \textbf{(III.3)}$$

Et l'algorithme de déchiffrement par : $(M^e)^D$

La figure III.3 illustre le fonctionnement de l'algorithme asymétrique **[3]**.

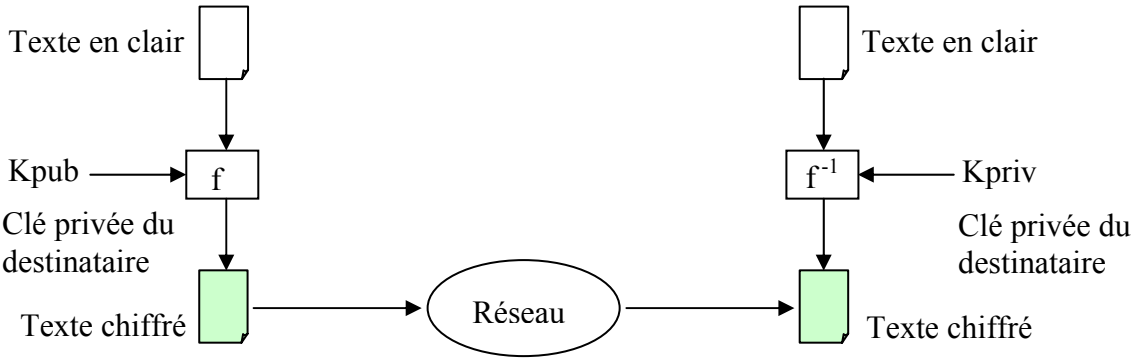


FIG III.3 – *Chiffrement asymétrique* **[3]**.

C – Les autres alogorithmes de chiffrement

Le résumé de ces algorithmes se trouve dans l'**Annexe B**.

III.1.4.1.2 – Certificats

La communication entre les différentes stations d'un réseau nécessite un service sécurisé et fiable pour délivrer des certificats. Un certificat se compose d'une suite de symboles et d'une signature. Le format de certificat le plus courant est celui du standard x.509.v2 ou v3. La figure III.4 illustre la composition d'un tel certificat **[3]**.

Un certificat contient un numéro de série, qui est unique par autorité de certification ou CA, l'algorithme de signature utilisé par le CA, le DN de l'autorité signataire du certificat, la période de validité du certificat et de sa clé publique, le DN du titulaire de la clé publique, les caractéristiques de la clé publique ainsi que l'algorithme utilisé, la clé publique elle-même puis des extensions facultatives. Le certificat se termine par la signature de l'empreinte numérique de l'autorité de certification, ou estampille du CA (figure III.4) **[3]**.

Les mécanismes à base de certificats supposent qu'une confiance s'installe entre les utilisateurs et l'entité qui produit les clés privées. Un organisme offrant un service de gestion de clés publique est une autorité de certification appelée tiers de confiance. Cet organisme émet des certificats au sujet de clés permettant à une entreprise de les utiliser avec confiance.

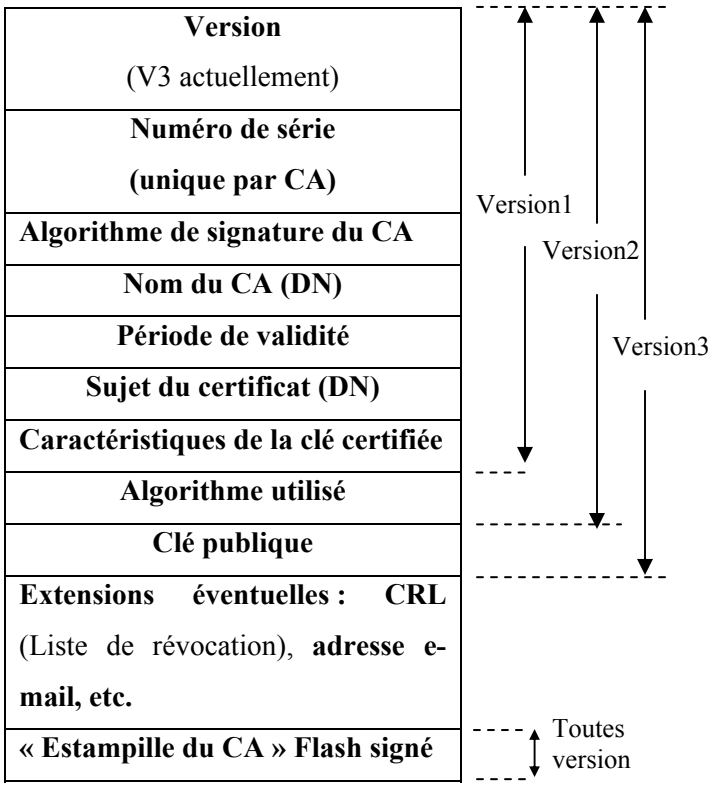


FIG III.4 – *Exemple de certificat x.509* **[3]**.

III.1.4.2 – Authentification

L'authentification permet de vérifier l'identité des processus communicants. Parmi Les solutions simples qui existent, l'utilisation d'un identificateur et d'un mot de passe, une méthode de défi basée sur une fonction cryptographique et un secret. L'authentification peut s'effectuer par un numéro d'identification personnel, comme le numéro inscrit dans une carte à puce, ou code PIN

Au début des années 2000, des techniques d'authentification beaucoup plus sophistiquées, comme la vérification d'une identité par prise d'empreinte digitale ou rétinienne, se sont développées de façon industrielle.

L'authentification peut être simple ou mutuelle. Elle consiste surtout à comparer les données provenant de l'utilisateur qui se connecte à des informations stockées dans un site protégé. Les sites mémorisant les mots de passe sont les plus susceptibles au piratage **[3]**.

III.1.4.3 – Intégrité des données

L'intégrité des données consiste à prouver que les données sont inchangées. Elles peuvent être copiées, mais aucun bit ne doit avoir été modifié **[3]**.

III.1.4.4 – La non-répudiation

Les services de non-répudiation consistent à assurer que l'information a été effectivement reçue par la station qui l'a réclamée **[3]**. Cette fonction peut s'effectuer par une signature à clé privée ou publique. La signature consiste alors à chiffrer une empreinte du message avec la clé RSA privée de son auteur et permet d'authentifier l'émetteur **[3]**.

L'émetteur est le seul à connaître cette clé, par laquelle il va signer son message. La vérification d'une signature se fait par une clé publique, l'émetteur signe le message M en utilisant l'algorithme RSA **[3]**:

$$M^e \bmod N. \qquad \textbf{(III.4)}$$

Le récepteur porte cette valeur à la puissance D pour vérifier que :

$$(M^e)^D = M. \qquad \textbf{(III.5)}$$

Si cette égalité se vérifie, la signature est authentifiée. La figure III.5 relate un exemple de signature.

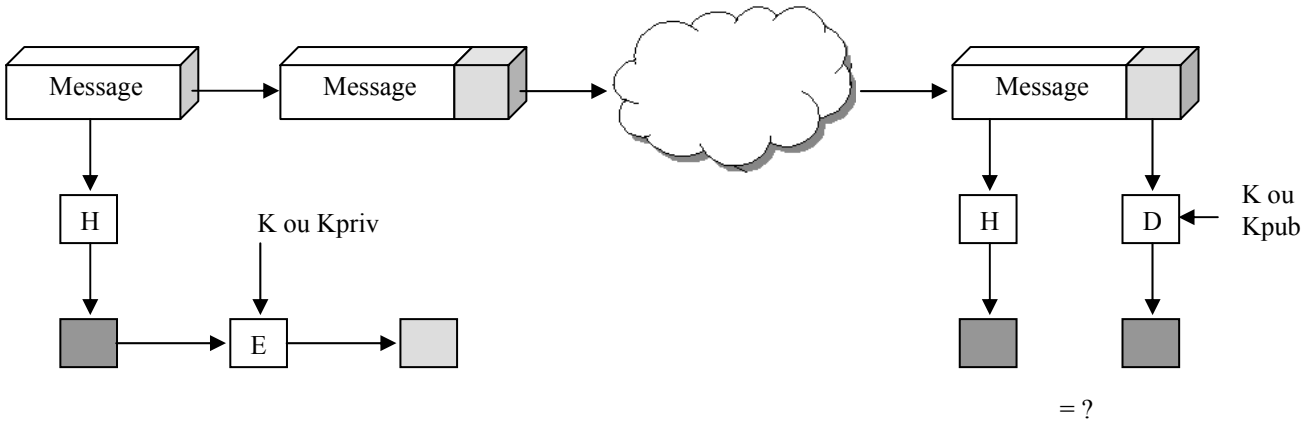


FIG III.5 – *Exemple de signature* **[3]**.

E : Emetteur, D : Destinataire, H : le message chiffré.

III.1.4.5 – Le contrôle d'accès

Les entreprises ont adapté des solutions de sécurité des points d'accès situés aux frontières de leurs réseaux privés face à la demande des utilisateurs d'accès distants sécurisés. Dans ce domaine, nous nous intéressons aux Firewalls.

Les Firewalls

Un Firewall (pare-feu) permet aux administrateurs réseaux de gérer et de représenter une politique de contrôle d'accès. Tout le trafic sortant/entrant du réseau Intranet vers le réseau Internet doit passer par le Firewall.

Les Firewalls sont destinés aux accès non authentifiés du réseau externe et au filtrage à différents niveaux de la couche OSI. Ils empêchent les intrus de se logger sur des machines du réseau interne.
La figure III.6 illustre une architecture classique de sécurité utilisant un Firewall :

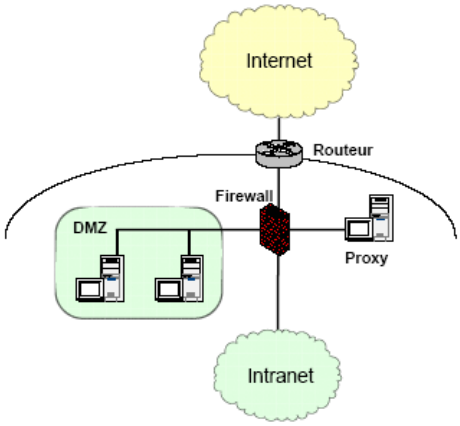


FIG III.6 – *Architecture classique de sécurité utilisant un Firewall.*

Un routeur peut précéder le Firewall pour assurer que les paquets entrants lui sont exclusivement destinés. Un routeur offre également l'accès à un sous réseau dénommé DMZ (zone démilitarisée) dans laquelle résident les serveurs publics de l'entreprise. La DMZ est une zone protégée de l'extérieure et de l'intérieur.

Nonobstant, ce système de Firewall est insuffisant s'il n'est pas accompagné d'autres protections. Il ne fournit pas les services de sécurité tels que (authentification, intégrité, confidentialité, etc.). Les attaques passives et actives ne sont pas protégées (analyse de trafic, IP Spoofing, IP Flooding, etc.) et les failles de configuration par des outils d'analyse automatique des vulnérabilités du système **[32]**.

III.1.5 – Les algorithmes de sécurité

III.1.5.1 – PGP

PGP est un algorithme conçu pour la sécurisation de la messagerie électronique. Il offre à cette application une authentification et une confidentialité. PGP permet le chiffrement et la signature de documents.

Le texte à envoyer est chiffré par l'algorithme IDEA. La signature utilise MD5. L'algorithme RSA a été choisi pour l'échange de la clé privée nécessaire à IDEA. D'autres fonctions peuvent être mises en jeu, telles que l'authentification par signature en utilisant une fonction de hash SHA-1 et la

confidentialité par un des nombreux algorithmes disponibles, comme IDEA, Triples DES, Diffie-Helmann, RSA, etc. **[30]**

III.1.5.2 – L'infrastructure PKI

Un système sécurisé requiert une distribution de clés publiques avec sécurité. L'infrastructure PKI propose une solution à ce problème.

Les principales fonctions réalisées par une infrastructure PKI pour la gestion des certificats sont les suivantes **[30]** :

- Enregistrement de demandes et de vérification des critères pour l'attribution d'un certificat. L'identité du demandeur est vérifiée ainsi que le fait qu'il soit bien en possession de la clé privée associée.
- Création des certificats.
- Diffusion des certificats entraînant la publication des clés publiques.
- Archivage des certificats pour assurer la sécurité et la pérennité.
- Renouvellement des certificats en fin de période de validité.
- Suspension de certificats
- Révocation des certificats : sur date de péremption, perte, vol ou compromission de clés.
- Création et publication (au sens gestion) des listes de révocation des certificats.
- Délégation de pouvoir à d'autres entités reconnues de confiance. Toute communauté peut créer sa propre infrastructure PKI. Dans ce cas, une étude de faisabilité est nécessaire en s'appuyant sur de nombreux critères **[30]**

III.1.5.3 – PKCS

PKCS est un ensemble de standard pour la mise en place des IGC. Pour plus de détails, les standards se trouvent dans **[30].**

III.1.5.4 – Kerberos

L'algorithme d'authentification Kerberos fondé sur une cryptographie est utilisé pour éviter qu'une personne malveillante puisse prendre l'identité de quelqu'un d'autre.

Grâce à ce système, un processus client qui travaille pour un utilisateur donné peut prouver son identité à un serveur, sans envoyer de données dans le réseau, qui pourraient permettre à un tiers de découvrir le code de l'authentification **[30]**.

III.1.6 – La sécurité dans les protocoles

Conçus avant les années 2000, les protocoles du monde IP n'ont pas intégré de fonction de sécurité. De nombreuses failles de sécurité existent donc et elles sont comblées régulièrement par des RFC spécifiques **[30]**.

III.1.6.1 – La sécurité dans SNMP

Le RFC 2274 définit le modèle USM de sécurité de SNMP, USM permet une authentification et un service de sécurité **[30]**.

SNMP peut être l'objet des attaques suivantes :

- Modification de l'information.
- Mascarade.
- Modification à l'intérieur d'un flot de message.

Le modèle de sécurité ne prend pas en compte les deux fonctionnalités suivantes **[30]**:

- Refus de service.
- Analyse de trafic.

Pour freiner ces différentes attaques, deux fonctions cryptographiques ont été définies dans USM : l'authentification et le chiffrement. Pour cela, le moteur SNMP a besoin de deux valeurs, une clé privée et une clé d'authentification. Ces valeurs sont des attributs de l'utilisateur qui ne sont pas accessibles par des primitives SNMP **[29]**. Dans ce cadre, deux algorithmes d'authentification sont disponibles : HMAC-MD5-96 et HMAC – SHA- 96.

L'algorithme HMAC utilise une fonction de hachage sécurisée et une clé secrète pour produire un code d'authentification de message. C'est un protocole fortement utilisé dans Internet **[29]**.

III.1.6.2 – IPsec

Le commerce électronique représente une portion importante des activités principales sur Internet, par conséquent une certaine confidentialité est nécessaire pour la transmission des numéros de carte bancaire, par exemple.

Les mécanismes de sécurité appropriés au commerce sur Internet sont choisis par une association de sécurité. En effet, toutes les communications n'ont pas les mêmes caractéristiques et leur sécurité ne demande pas les mêmes algorithmes.

Les principaux éléments d'une association de sécurité sont les suivants :

- L'algorithme d'authentification ou de chiffrement utilisé.

- Les clés globales ou spécifiques à prendre en compte.
- D'autres paramètres de l'algorithme, comme les données de synchronisation ou les valeurs d'initialisation.
- Les durées de validité des clés ou des associations.
- La sensibilité de la protection apportée (secret, top secret, …).

IPsec introduit des mécanismes de sécurité au niveau du protocole IP. Le but de ce protocole de sécurité est de garantir les critères : Intégrité, l'authentification, la confidentialité et la protection contre les techniques rejouant des séquences précédentes **[30]**.

Le format de paquets IPsec est illustré sur la figure III.7.

La partie (1) correspond au format d'un paquet IP dans lequel est encapsulé un paquet TCP, la partie (2) illustre le paquet IPsec et l'on voit qu'entre l'en-tête IP et l'en-tête TCP vient de se mettre l'en-tête d'IPsec. La partie (3) montre le format d'un paquet dans un tunnel IP. On y voit que la partie intérieure correspond à un paquet IP encapsulé dans un paquet IPsec de telle sorte que le paquet IP intérieur soit bien protégé.

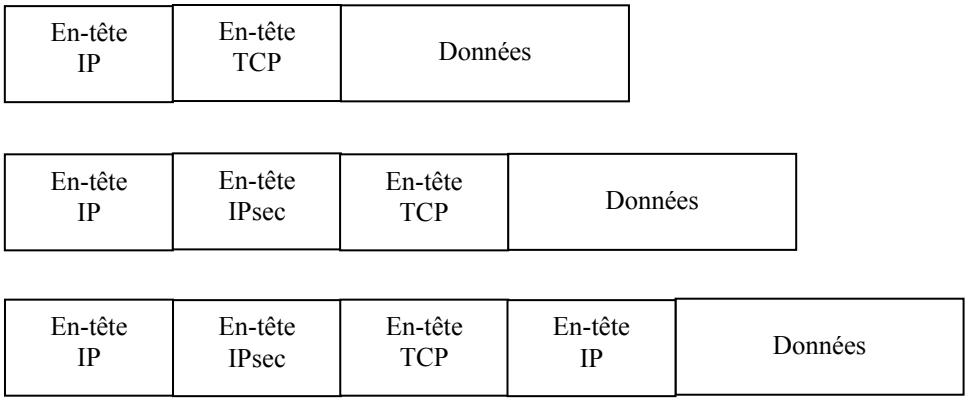


FIG III.7 – *Format de paquets IPsec* **[30]**.

Dans un tunnel IPsec, tous les paquets IP d'un flot sont transportés de façons totalement chiffrées.

Dans ce cas, il est impossible de voir les adresses IP et même les valeurs du champ de supervision du paquet IP encapsulé **[30]**.

III.1.6.3 – SSL

SSL est un logiciel permettant la sécurité des communications sous HTTP ou FTP. Ce logiciel a été développé par Netscape pour son navigateur et les services Web. Il permet de chiffrer les messages entre un navigateur et le serveur Web interrogé. La figure III.8 montre le niveau d'architecture où se place SSL. C'est un niveau compris entre TCP et les applicatifs.

Une communication SSL est initialisée par un handshake, c'est-à-dire une poignée de main qui permet l'authentification réciproque grâce à un tiers de confiance. Ensuite, une négociation du niveau

de sécurité à mettre en œuvre permet de poursuivre la communication. Enfin, le déroulement de la communication se fait avec un chiffrement associé au niveau négocié dans la phase précédente.

SSL a pris plus d'importance que la simple sécurisation d'une communication Web. Ce protocole est également utilisé dans le commerce électronique pour sécuriser la transmission du numéro de carte de crédit.

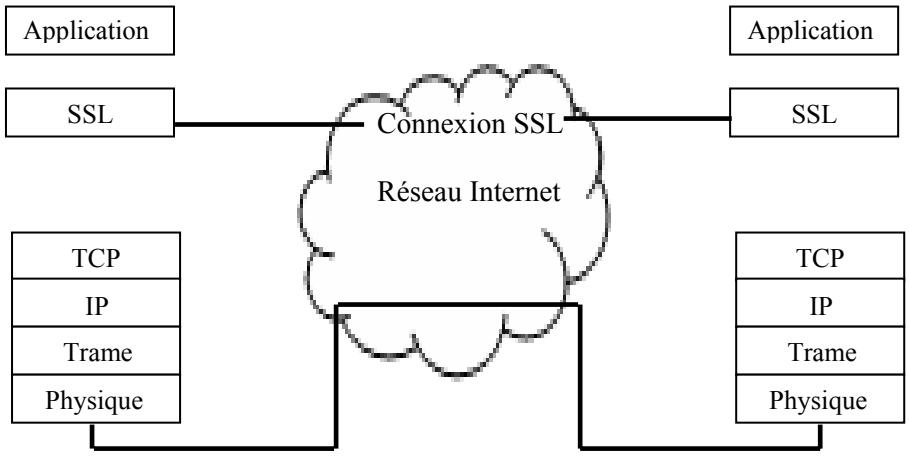


FIG III.8 – *L'architecture SSL* **[30]**.

III.1.6.4 – Les VPN et le protocole PPP

Définition

Les réseaux privés virtuels (VPN) sont une mesure de sécurité qui permet à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Tous se fait dans un tunnel où chaque extrémité est identifiée, les données transitent après avoir été chiffrées.

Un des grands intérêts des VPN est de réaliser des réseaux privés à moindre coût. En chiffrant les données, tout se passe exactement comme si la connexion se faisait en dehors d'Internet.

Principe du VPN

Les réseaux VPN se basent sur la technique du tunnelling. Après avoir identifié l'émetteur et le destinataire un chemin virtuel est construit. Ensuite les données seront chiffrées et acheminées par la source en empruntant ce chemin virtuel (figure III.9).

Les données à transmettre peuvent appartenir à un protocole différent d'IP. Le routage des trames dans le tunnel se fait grâce au protocole de tunneling qui encapsule les données en rajoutant une entête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.

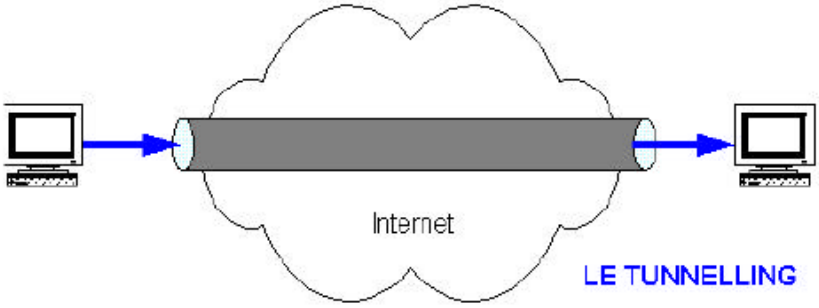


FIG III.9 – *Principe du VPN.*

Applications des VPNs

L'application principale des VPN est de garantir et de permettre à un hôte distant d'accéder à l'intranet de son entreprise ou à celui d'un client grâce à Internet tout en garantissant la sécurité des échanges. Il crée un réseau privé virtuel entre l'appelant et le serveur VPN de l'entreprise.

Les VPN peuvent également être utilisé à l'intérieur même de l'entreprise, sur l'intranet, pour l'échange de données confidentielles.

Services des VPN

La sécurité des échanges est assurée à plusieurs niveaux et par différentes fonctions comme le cryptage des données, l'authentification des deux extrémités communicantes et le contrôle d'accès des utilisateurs aux ressources **[33]**.

III.2 – LES MÉCANISMES DE SÉCURITÉ DANS LES RÉSEAUX SANS FIL

Pour bien comprendre où se placent les attaques et les algorithmes de sécurisation, nous introduisons le modèle de sécurité en couche.

III.2.1 – Le modèle de sécurité en couche

Un réseau assure à deux applications distantes le transport des messages. Dans un modèle OSI, les services déployés par le réseau sont en sept couches, physique, liaison, réseau transport, session, présentation et application. Le modèle classique des réseaux TCP/IP ne comporte que cinq couches, physique (PMD+PHY), liaison/trame (MAC+LLC), réseau/paquet (IP), transport/message (UDP+TCP) et application. Le modèle en couches est illustré sur la figure III.10 **[3]**.

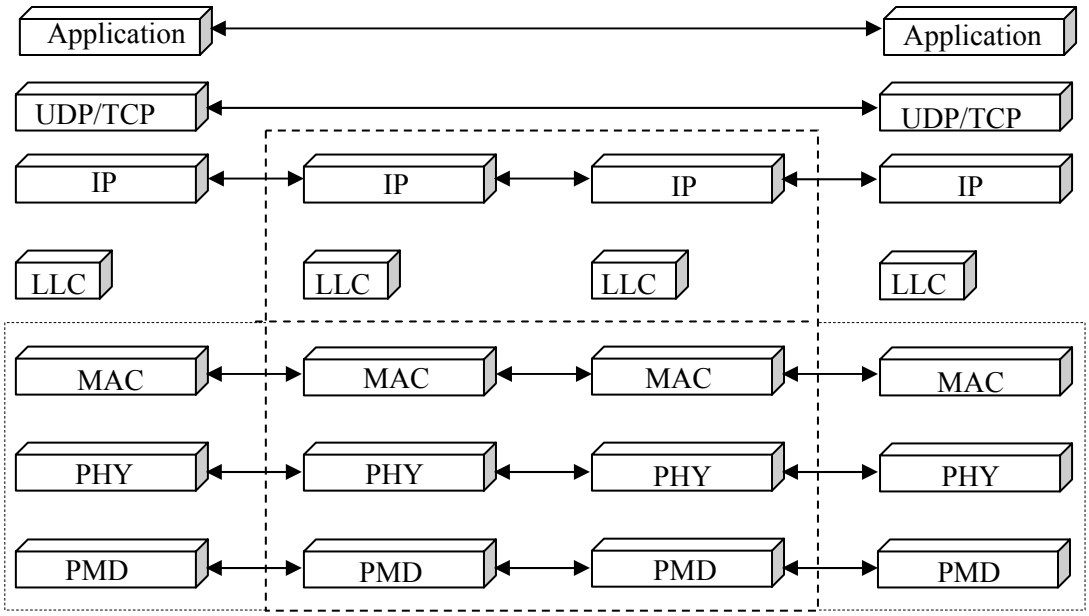


FIG III.10 – *Modèle en couches de l'architecture TCP/IP* **[3]**.

Les différents mécanismes tels que la confidentialité ou l'intégrité sont supportés sur les différents niveaux des couches TCP/IP, des données peuvent être supportés. La gestion des clés cryptographiques peut aussi être réalisée.

Les procédures d'identification, d'authentification, de non-répudiation et les autorisations sont mises en œuvre dans le réseau d'accès, qui peut être sans fil. Le réseau de transport IP et les réseaux de destination, un intranet, par exemple. Ces services peuvent être offerts au niveau applicatif **[3]**.

Les infrastructures de sécurité des réseaux peuvent être classées en cinq catégories.

- ***Chiffrement au niveau physique sur des liaisons point à point :*** les clés sont distribuées manuellement.
- ***Confidentialité, intégrité des données, signature de trame MAC :*** cette technologie est adoptée par les réseaux **802.11**. Les clés sont distribuées dans un plan particulier, décrit par la norme **802.1x**. De ce fait, la notion de contrôle d'accès au réseau LAN est introduite, c-à-d à la porte de communication avec la toile d'araignée mondiale.
- ***Confidentialité, intégrité des données, signature des paquets IP ou TCP :*** c'est la technologie IPsec en mode tunnel. Un paquet IP chiffré et signé est encapsulé dans un paquet IP non protégé. Le routage à travers Internet implique l'analyse de l'entête IP par les passerelles traversées. IPsec crée un tunnel sécurisé entre le réseau d'accès et le domaine du fournisseur de services. L'utilisation du réseau d'accès est libre. Les réseaux traversés ne peuvent pas détecter les échanges malveillants entre deux criminels.

- ***Insertion d'une couche de sécurité additive :*** le protocole SSL fondé sur la cryptographie asymétrique assure la protection d'applications telles que la navigation web ou la messagerie électronique. SSL se charge d'une authentification entre serveur et client et négocie un secret partagé (Master, secret) qui génère des clés de chiffrement utilisées par l'algorithme de chiffrement négocié entre les deux parties. Après l'établissement du tunnel sécurisé, le client s'authentifie à l'aide d'un login et d'un mot de passe. Il aura une identité temporaire associée à un simple cookie.

- ***Gestion de la sécurité par l'application elle-même :*** le protocole S-MIME par exemple réalise la confidentialité, l'intégrité et la signature des contenus critiques d'un message électronique.

- ***Infrastructure de réseau sans fil sécurisé :*** La procédure d'authentification est la clé voûte d'une infrastructure de réseau sans fil. Deux choix sont possibles **[3]**:

* L'utilisateur protège ses clés d'authentification qu'il connaît à l'aide d'un mot de passe. Le logiciel open SSL permet de chiffrer la clé privée RSA par un triple DES, dont les clés déduites d'une phrase.

* L'utilisateur ne connaît pas ses clés d'authentification, qui sont la propriété du prestataire de service. Une carte à puce par exemple réalise après renseignement d'un code PIN les calcules d'authentification.

La sécurisation des communications dans un réseau sans fil nécessite un environnement équipé d'un certain nombre de matériel pour réaliser une infrastructure permettant la mise en œuvre des fonctions requises dans le réseau. Autrement dit, il faut intervenir auprès de quatre types d'éléments infrastructures, l'infrastructure qui permet l'authentification des clients et des équipements de réseau, le matériel et le logiciel nécessaires pour réaliser la sécurité sur l'interface radio, les éléments de réseau nécessaires pour filtrer les paquets et détecter les attaques, et enfin les machines nécessaires pour gérer les accès distants lorsque les utilisateurs se déplacent **[3]**.

III.2.2 – Infrastructure de réseau sans fil sécurisé

La procédure d'authentification est l'étape essentielle d'une infrastructure de réseau sans fil sécurisée **[3]**.

Deux choix sont possibles :

- L'utilisateur connaît ses clés d'authentification qu'il protège à l'aide de mots de passe.
- L'utilisateur ne connaît pas ses clés d'authentification, qui sont la propriété du prestataire de service.

Pour qu'une communication soit sécurisée dans un réseau sans fil, il faut que l'environnement dispose d'un certain nombre de fonctions qui peuvent être prises en charge soit par l'infrastructure

achetée pour réaliser le réseau lui-même, soit par de nouveaux éléments de réseau à ajouter. Nous pouvons citer :

- Infrastructure d'authentification : La norme **IEEE 802.1x** recommande l'usage de serveurs radius. L'authentification peut être effectuée par un serveur situé dans le domaine visité ou à l'extérieure de ce dernier. Cette architecture établit un cercle de confiance, grâce auquel un message d'authentification est relayé par plusieurs serveurs liés les uns aux autres par des associations de sécurité.

- Sécurité radio : l'objectif de la sécurité de l'interface Radio est d'assurer la confidentialité, l'intégrité et la signature des paquets. Ces services sont délivrés par des protocoles tels que WEP, TKIP ou CCMP, normalisés par le comité **IEEE 802**. Ils utilisent des clés, déduites d'une clé maître au terme de la procédure d'authentification.

- Filtrage des paquets : cette opération est fiable puisqu'elle repose sur la signature des paquets à l'aide des clés déduites de l'authentification. Grâce à ce mécanisme, les trames qui pénètrent dans le système de distribution sont sûres (pas de risques de spoofing). Des systèmes de filtrage (point d'accès ou portail) gèrent les privilèges des paquets IP (destruction des paquets illicites) et permettent de réaliser et de facturer des services de QoS.

- Accès aux services distants (roaming) : l'accès aux services distants peut être désigné de façon générique sous l'appellation de services VPN **[3]**.

III.2.3 – Les Attaques dans les réseaux sans fil

En raisonnant par analogie, implanter un réseau sans fil est similaire au fait de placer en pleine rue une prise téléphonique connectée à la ligne téléphonique d'un particulier ou d'un organisme, ou bien de positionner des prises Ethernet sur un réseau filaire en dehors de tout contrôle.

Les risques encourus en employant ce type de réseaux sont de même nature que pour les réseaux filaires, ils sont simplement plus élevés. En effet, un intrus est capable d'écouter un message ou de s'introduire dans un réseau **802.11.b** grâce à la disponibilité en accès libre sur l'Internet d'outils d'agression **[3]**.

Les attaques réseaux sont divisées en deux catégories : les attaques Passives et les attaques Actives, d'autres types d'attaques sont déduits. La figure III.11 résume ces attaques.

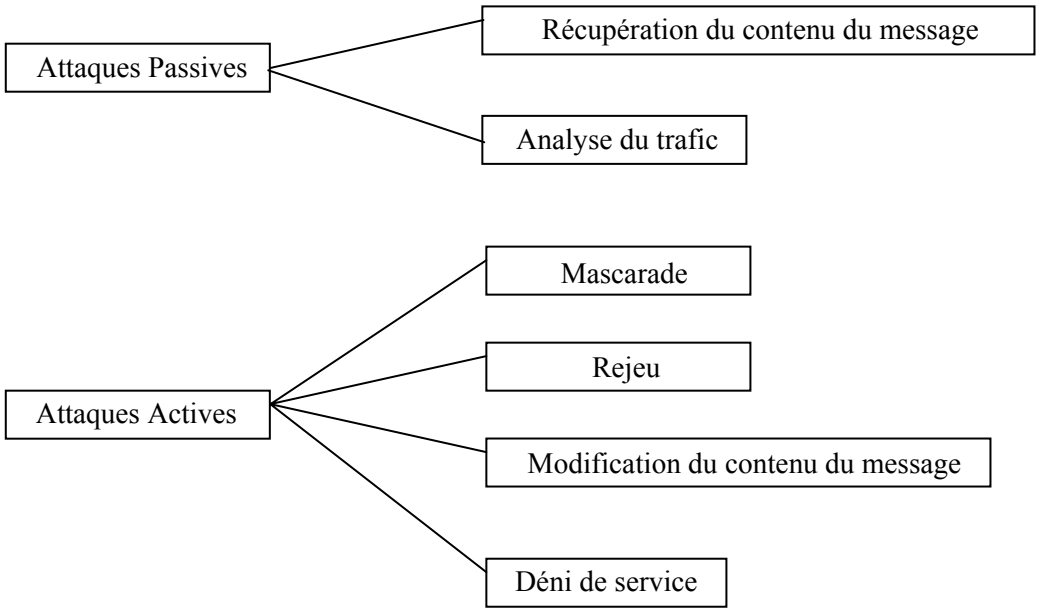


FIG III.11 – *Les types d'attaques réseau.*

Les risques associés aux réseaux sans fil **802.11** sont le résultat d'une ou plusieurs de ces attaques.

Les conséquences de ces dernières engendrent une perte d'informations, un coût légal et de recouvrement ainsi que la perte de services réseau.

III.2.3.1 – Les attaques passives

Une attaque est dite *passive* quand un utilisateur non autorisé obtient un accès à une ressource sans modifier son contenu. Les attaques *passives* peuvent être des écoutes ou des analyses de flots de trafic.

III.2.3.1.1 – Le sniffing

– Analyse réseau

Un *« analyseur réseau »* (*sniffer*) est un dispositif permettant d'*écouter* le trafic d'un réseau. Les données d'un réseau non commuté sont envoyées à toutes les machines du réseau. Il est possible d'écouter tout le trafic passant par un adaptateur réseau **[34]**.

– Utilisation du sniffer

Un *sniffer* comme *Ethereal* permet d'étudier le trafic d'un réseau. Il sert pour le diagnostique des problèmes du réseau ainsi que pour connaître le trafic qui y circule. Ainsi les détecteurs d'intrusion (IDS) sont basés sur un sniffeur pour la capture des trames, et utilisent une base de données de règles pour détecter des trames suspectes.

Le sniffer est utilisé par une personne malveillante pour collecter des informations. Ce risque est d'autant plus important sur les réseaux sans fils.

Les informations sont transitées en clair par les protocoles, c'est-à-dire de manière non *chiffrée*. Ainsi, lorsqu'un utilisateur du réseau entre sur des sites Internet dont l'adresse ne commence pas par HTTPS, toutes les informations envoyées ou reçues peuvent être interceptées. C'est de cette manière que des sniffers réussissent à récupérer les mots de passe circulant dans le flux réseau **[34]**.

III.2.3.1.2 – Les parades

Il existe plusieurs façons de se protéger contre les désagréments que pourrait provoquer l'utilisation d'un sniffer sur le réseau :

- Utiliser des protocoles chiffrés pour transmettre les informations confidentielles.
- Segmenter le réseau afin de limiter la diffusion des informations. Il est notamment recommandé de préférer l'utilisation de switchs (*commutateurs*) à celle des hubs (*concentrateurs*) car les informations sont délivrées uniquement aux machines destinataires.
- Utiliser un détecteur de sniffer. Il s'agit d'un outil sondant le réseau à la recherche de matériels.

Pour les réseaux sans fils il est conseillé de réduire la puissance des matériels de telle façon à ne couvrir que la surface nécessaire. Cela réduit le périmètre géographique dans lequel les pirates ont la possibilité de s'introduire **[34]**.

III.2.3.2 – Les attaques actives

Une attaque est dite *active* lorsqu'un intrus apporte des modifications sur les messages de flux de données ou de fichier. La détection de ces attaques est très facile. Cette catégorie d'attaques a plusieurs formes, citons comme exemple les mascarades, le rejeu, la modification des messages et le déni de service **[3]**.

III.2.3.2.1 – les Mascarades

– L'usurpation d'adresse IP

L' *« usurpation d'adresse IP »* (*spoofing IP*) est une technique qui consiste à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine.

Certains tendent à introduire un proxy (permettant de masquer d'une certaine façon l'adresse IP) avec du spoofing IP. Toutefois, le proxy ne fait que relayer les paquets. Ainsi même si l'adresse est

apparemment masquée, un pirate peut facilement être retrouvé grâce au fichier journal (logs) du proxy **[35]**.

– Attaque par usurpation

La technique de l'usurpation d'adresse IP peut permettre à un pirate de faire passer des paquets sur un réseau sans que le système de filtrage de paquets (pare-feu) les intercepte. Ainsi, un paquet contenant une adresse IP externe sera automatiquement rejeté par le pare-feu (figure III.12).

Cependant, le protocole TCP repose sur des liens d'authentification et d'approbation entre les machines d'un réseau, ce qui signifie que pour accepter le paquet, le destinataire doit auparavant accuser réception auprès de l'émetteur, ce dernier devant à nouveau accuser réception de l'accusé de réception **[35]**.

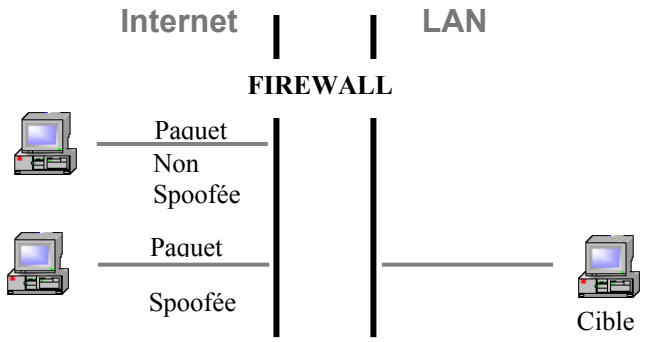


FIG III.12 – *Attaque par usurpation d'adresse IP.*

– Modification de l'en-tête TCP

Le protocole IP assure l'encapsulation des données dans des structures appelées paquets (ou plus exactement *datagramme IP*). La structure d'un datagramme est exposée sur la figure III.13.

Version	Longueur d'en-tête	Type de service	Longueur totale	
Identification			Drapeau	Décalage fragment
Durée de vie		Protocole	Somme de contrôle en-tête	
Adresse IP source				
Adresse IP destination				
Données				

FIG III.13 – *Format de l'entête IP.*

Usurper une adresse IP revient à modifier le champ *source* afin de simuler un datagramme provenant d'une autre adresse IP.

Avant d'accepter un paquet, une machine doit auparavant accuser réception de celui-ci auprès de la machine émettrice, et attendre que cette dernière confirme la bonne réception de l'accusé **[35]**.

– Les liens d'approbation

Le protocole TCP permet, au niveau des applications, de gérer les données en provenance (ou à destination) de la couche inférieure du modèle (c'est-à-dire le protocole IP). Il permet entre autre d'assurer le transfert des données de façon fiable, bien qu'il utilise le protocole IP grâce à un système d'accusés de réception (ACK) permettant au client et au serveur de s'assurer de la bonne réception mutuelle des données. Les datagrammes IP encapsulent des paquets TCP (appelés *segments*) dont la structure est reprise sur la figure III.14.

<table>
<tr><th colspan="8">0 1 2 3 4 5 6 7 8 9 10 11</th><th colspan="8">12 13 14 15</th><th colspan="16">16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31</th></tr>
<tr><td colspan="16">Port Source</td><td colspan="16">Port destination</td></tr>
<tr><td colspan="32">Numéro d'ordre</td></tr>
<tr><td colspan="32">Numéro d'accusé de réception</td></tr>
<tr><td colspan="4">Décalage données</td><td colspan="6">Réservée</td><td colspan="2">URG</td><td colspan="2">ACK</td><td colspan="2">PSH</td><td colspan="2">RST</td><td colspan="2">SYN</td><td colspan="2">FIN</td><td colspan="16">Fenêtre</td></tr>
<tr><td colspan="16">Somme de contrôle</td><td colspan="16">Pointeur d'urgence</td></tr>
<tr><td colspan="24">Options</td><td colspan="8">Remplissage</td></tr>
<tr><td colspan="32">Données</td></tr>
</table>

FIG III.14 – *Format de l'entête TCP* **[35]**.

Lors de l'émission d'un segment, un numéro d'ordre (ou de séquence) est associé, et un échange de segments contenant des champs particuliers (appelés *drapeaux* (*flags*)) permet de synchroniser le client et le serveur. Ce dialogue (appelé *poignée de mains en trois temps*) permet d'initier la communication, il se déroule en trois temps, comme sa dénomination l'indique :

- Dans un premier temps, la machine émettrice (le client) transmet un segment dont le drapeau SYN est à 1 (pour signaler qu'il s'agit d'un segment de synchronisation), avec un numéro d'ordre N, que l'on appelle numéro d'ordre initial du client.
- Dans un second temps la machine réceptrice (le serveur) reçoit le segment initial provenant du client, puis lui envoie un accusé de réception, c'est-à-dire un segment dont le drapeau ACK est non nul (accusé de réception) et le drapeau SYN est à 1 (car il s'agit là encore d'une synchronisation). Ce segment contient un numéro de séquence égal au numéro d'ordre initial du client. Le champ le plus important de ce segment est le champ accusé de réception (ACK) qui contient le numéro d'ordre initial du client, incrémenté de 1.

- Enfin, le client transmet au serveur un accusé de réception dont le drapeau ACK est non nul, et dont le drapeau SYN est à zéro. Son numéro d'ordre est incrémenté et le numéro d'accusé de réception représente le numéro de séquence initial du serveur incrémenté de 1.
- La machine spoofée va répondre avec un paquet TCP dont le drapeau RST (*reset*) est non nul, ce qui mettra fin à la connexion.

– Annihiler la machine spoofée (figure III.15)

L'attaquant qui effectue une attaque par usurpation d'adresse IP, n'a aucune information en retour car les réponses de la machine cible vont vers une autre machine du réseau (on parle alors d'*attaque à l'aveugle (blind attack*)).

De plus, la machine *« spoofée »* prive le hacker de toute tentative de connexion, car elle envoie systématiquement un drapeau RST à la machine cible. Le travail du pirate consiste alors à invalider la machine spoofée en la rendant injoignable pendant toute la durée de l'attaque.

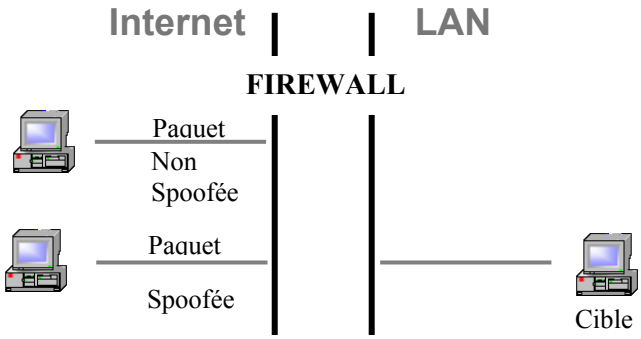


FIG III.15 – *Annihilation de la machine.*

– Prédire les numéros de séquence (figure III.16)

Lorsque la machine spoofée est invalidée, la machine cible attend un paquet contenant l'accusé de réception et le bon numéro de séquence. Le pirate doit *« deviner »* le numéro de séquence à renvoyer au serveur pour que la relation de confiance soit établie. Pour cela, les pirates utilisent généralement la *source routing*, c'est-à-dire qu'ils utilisent le champ *option* de l'en-tête IP afin d'indiquer une route de retour spécifique pour le paquet.

Le fait de connaître le dernier numéro de séquence émis, le pirate établit des statistiques concernant son incrémentation et envoie des accusés de réception jusqu'à obtenir le bon numéro de séquence.

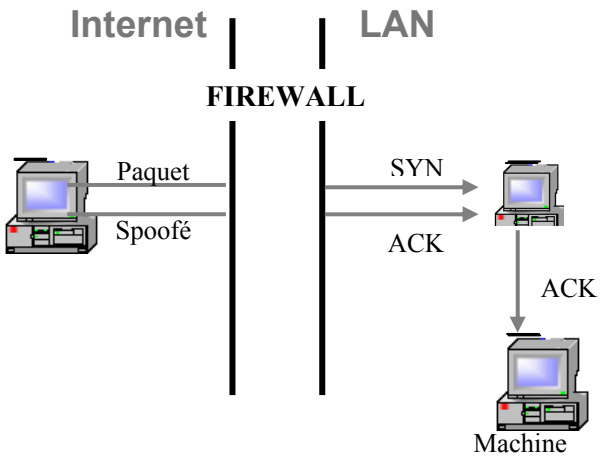


FIG III.16 – *Prédiction des numéros de séquence.*

III.2.3.2.2 – Attaque (Man in the Middle)

L'attaque *« Man In The Middle »* ou *« Attaque de l'homme au milieu »* porte bien son nom. Il s'agit d'un type d'attaque où une tierce personne s'interpose de manière transparente dans une connexion pour écouter sans se faire remarquer.

Le but de cette attaque est de remplacer les tables ARP des victimes afin de mettre le poste attaquant en position d'écoute entre les cibles **[35]**. Pour bien comprendre le déroulement de cette attaque, prenons comme exemple celui de la figure III.17.

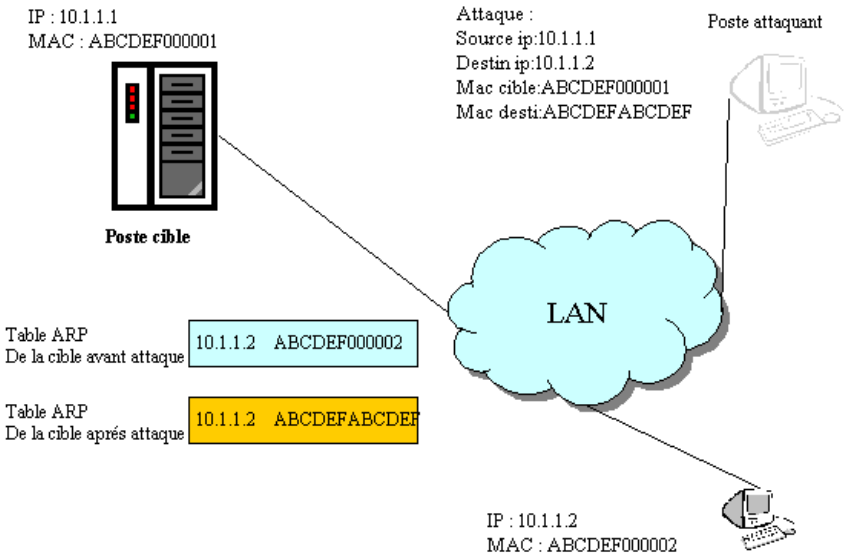


FIG III.17 – *Attaque Man In The Middle.*

En premier lieu, le poste attaquant va émettre deux paquets ARP falsifiés vers les deux postes cibles. Ces paquets indiqueront aux postes cibles que l'adresse ARP du poste distant (le poste cible 1 pour le poste cible 2 et vice versa) a changé. Chaque poste cible recevra une requête ARP indiquant l'adresse ARP **ABCDEF000003** pour le poste distant.

La table ARP (dynamique) du poste cible sera mise à jour avec les informations erronées. Les prochains paquets envoyés seront donc envoyés à l'adresse MAC de la machine attaquante. Cette requête est envoyée régulièrement pour éviter un retour à la normale, car un poste cible remet à jour sa table ARP très fréquemment (toutes les 30 secondes ou les 2 mn par exemple, ce laps de temps étant configurable sur la plupart des systèmes d'exploitation), puis émet un broadcast ARP pour connaître les adresses MAC des postes avec lesquels il souhaite communiquer. Le poste attaquant réceptionne toutes les communications entre les deux postes cibles. Il doit ensuite retransmettre les paquets aux cibles correspondantes pour que le dialogue entre les deux machines continue et qu'il puisse continuer d'écouter ce qui se passe, tout en restant invisible au milieu de la connexion **[36]**.

III.2.3.2.3 – Le déni de service

L'attaque par Déni de service est une des plus simples à réaliser et est très répandue dans les réseaux sans fil. L'objectif de cette attaque est de rendre indisponible un service, un système ou un réseau, elle s'appuie généralement sur une faiblesse d'implémentation, un bogue, ou sur une faiblesse de protocole.

Dans un réseau sans fil, un déni de service consiste à émettre un grand nombre de requête d'association vers le point d'accès jusqu'à le faire tomber. De nombreuses attaques de déni de service peuvent s'effectuer par l'intermédiaire du protocole ICMP. Ce protocole est utilisé par les routeurs pour transmettre des messages de supervision. Un serveur peut également subir une telle attaque en générant des messages ICMP en grande quantité et en les envoyant au serveur à partir d'un nombre de sites importants **[3]**.

Les premières attaques par déni de services sont parues entre 1998 et l'an 2000. Elles visaient de grands sites Internet (yahoo ! Ebay, eTrade, etc.…), le site yahoo ! Premier annuaire de recherche au monde a été attaqué en février 2000 et a été inondé (flood) pendant plus de 3 heures sous un gigaoctets et données provenant d'au moins 50 points réseaux différents.

III.3 – LA SÉCURITÉ DANS 802.11

Les points d'accès **Wi-Fi** diffusent les données vers toutes les stations situées dans leur champ d'émission. Du coup, un attaquant peut s'introduire au sein du réseau, récupérer des informations et obtenir l'accès au réseau.

Pour remédier à ce problème, un client doit établir une relation particulière, appelée une association avec un point d'accès.

Pour qu'un client puisse s'associer au point d'accès, il doit passer par les trois états suivants :

- Non authentifié, non associé ;
- Authentifié, non associé ;
- Authentifié, associé.

La figure III.18 illustre une machine d'état de l'authentification dans un réseau **802.11**. Les trames échangées entre le point d'accès et le client peuvent être de deux types, de gestion ou de données. Pour transiter d'un état vers un autre, les trames échangées sont des trames de gestion.

Pour authentifier un client dans un réseau sans fil **802.11**, un mécanisme de sécurité spécifique : le WEP, a été défini **[3]**.

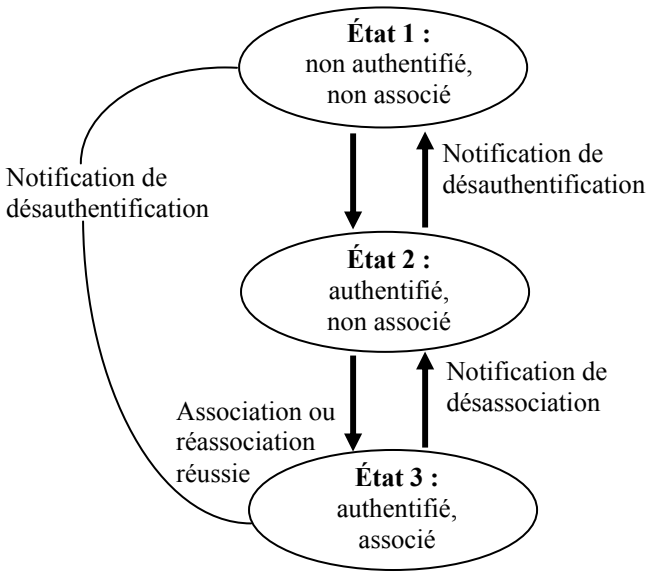


FIG III.18 – *Machine d'états de l'authentification dans un réseau 802.11* **[3]**.

III.3.1 – Cryptage : WEP

Le protocole WEP, fondé sur l'algorithme de chiffrement symétrique par flot RC4 a été introduit afin de protéger les communications des écoutes malveillantes. Sa création avait pour but d'apporter une couche de sécurité aux réseaux **IEEE 802.11** **[8]** en se basant sur l'authentification et le chiffrement des transmissions **[3]**.

III.3.1.1 – Le chiffrement

La norme **802.11** avait pour objectif de trouver un compromis entre efficacité et faible coût en calcul. Pour cela, il a été décidé d'utiliser la méthode de cryptage RC4 (RSA) en association avec une

méthode de génération de clé pseudo-aléatoire basée sur l'utilisation d'un « Vecteur d'Initialisation (IV) **[8]**.

III.3.1.2 – La clé partagée

Selon les équipements, La clé utilisée par le WEP est rentrée en binaire, hexadécimal ou en ASCII ; cela pose des problèmes sur un réseau **802.11** hétérogène. Cette clé est codée sur 48 ou 104 bits dans le standard WEP. Dans les standards récents, la longueur de la clé est poussée à 232 bits **[8]**.

III.3.1.3 – Le Vecteur d'Initialisation (IV)

Le vecteur d'initialisation (IV) est une série de 24 bits diffusés en clair par tout équipement **802.11**. Il est modifié aléatoirement, pour chaque trame émise. Dans **802.11**, il est associé à la clé privée pour définir, au fur et à mesure des changements du IV, ce qui mène à un grand nombre de clés dérivées possibles ainsi qu'une rotation rapide de ces clés **[8]**.

III.3.1.4 – L'algorithme RC4

RC4 est un standard créé par Ran Rivest en 1987, il fut rendu public en 1994 car il n'était plus considéré comme une méthode de cryptage. À partir d'une clé privée K et d'un vecteur d'initialisation (IV), RC4 génère une séquence pseudo-aléatoire S pour crypter un contenu.

La clé privée K et le vecteur d'initialisation IV passent dans un algorithme appelé KSA. Cet algorithme va générer une table d'états T qui aura la même taille que la clé dérivée. En suite, cette table d'état passe dans un système de génération de séquences pseudo-aléatoires basé sur l'utilisation de deux compteurs qui servent à organiser un pseudo-aléatoire.

La clé de cryptage effective est plus exactement une séquence pseudo-aléatoire S générée (ayant la même taille que la clé dérivée).

Le cryptage des données se fait par un (XOR) des bits en clair de S qui est beaucoup plus petite sur les données en clair. La méthode utilisée consiste à donner à S une taille égale à la taille du texte plus son CRC32 **[8]**.

Les données cryptés C consistent en un simple ou-exlusif du texte clair couplé à son CRC32 avec la version étendue de S comme le montre le schéma de la figure III.19.

Le cryptage complet consiste en la formule suivante :

$$C = (D \backslash\backslash c(D)) \text{ XOR } RC4(IV \backslash\backslash K).$$

(D : sont les données en clair, c (D) : le checksum (ou CRC de D)).

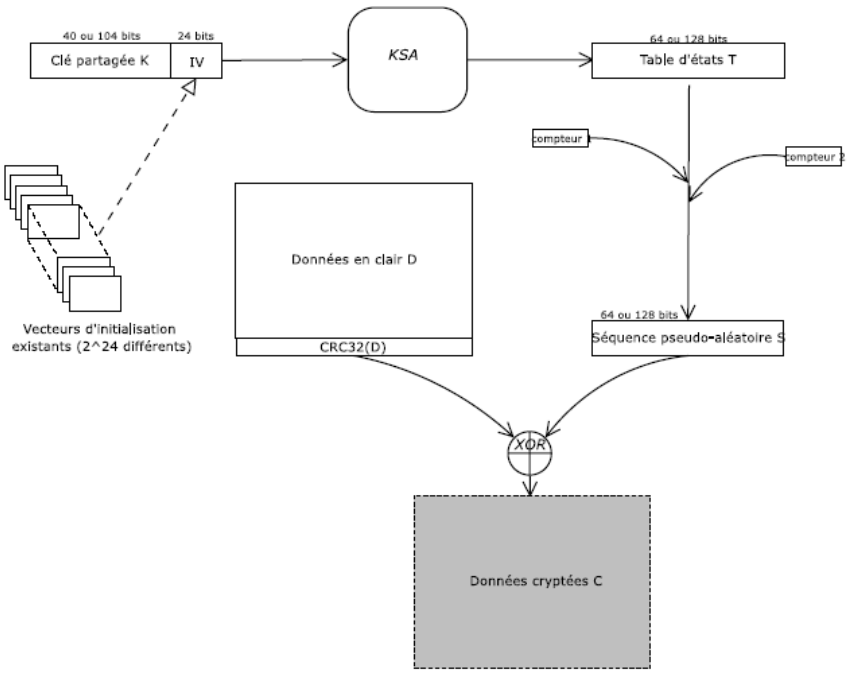


FIG III.19 – *Principe du cryptage WEP* **[8]**.

III.3.1.5 – L'authentification

L'établissement de la communication entre deux équipements **802.11** doit passer par deux étapes disponibles dans le WEP **[3]**:

*** *Open Authentification :*** est la procédure par défaut. Elle consiste à associer un terminal avec le point d'accès qui diffuse son SSID.

*** *Shared Key Authentification :*** fournit un certain niveau de sécurité en utilisant un mécanisme de clé partagée.

L'authentification se déroule en 4 étapes (figure III.20).

1- Une station voulant s'associer à un point d'accès lui envoie une requête d'authentification.

2- Lorsque le point d'accès reçoit cette trame, il envoie à la station une trame contenant un défi de 128 bits généré par le protocole WEP.

3- La station copie le défi dans une trame d'authentification, qu'elle chiffre avec la clé secrète puis envoie le tout au point d'accès.

4- Le point d'accès déchiffre le message à l'aide de la clé secrète et le compare avec celui qu'il a envoyé. Il envoie ensuite le résultat de l'authentification au client **[3]**.

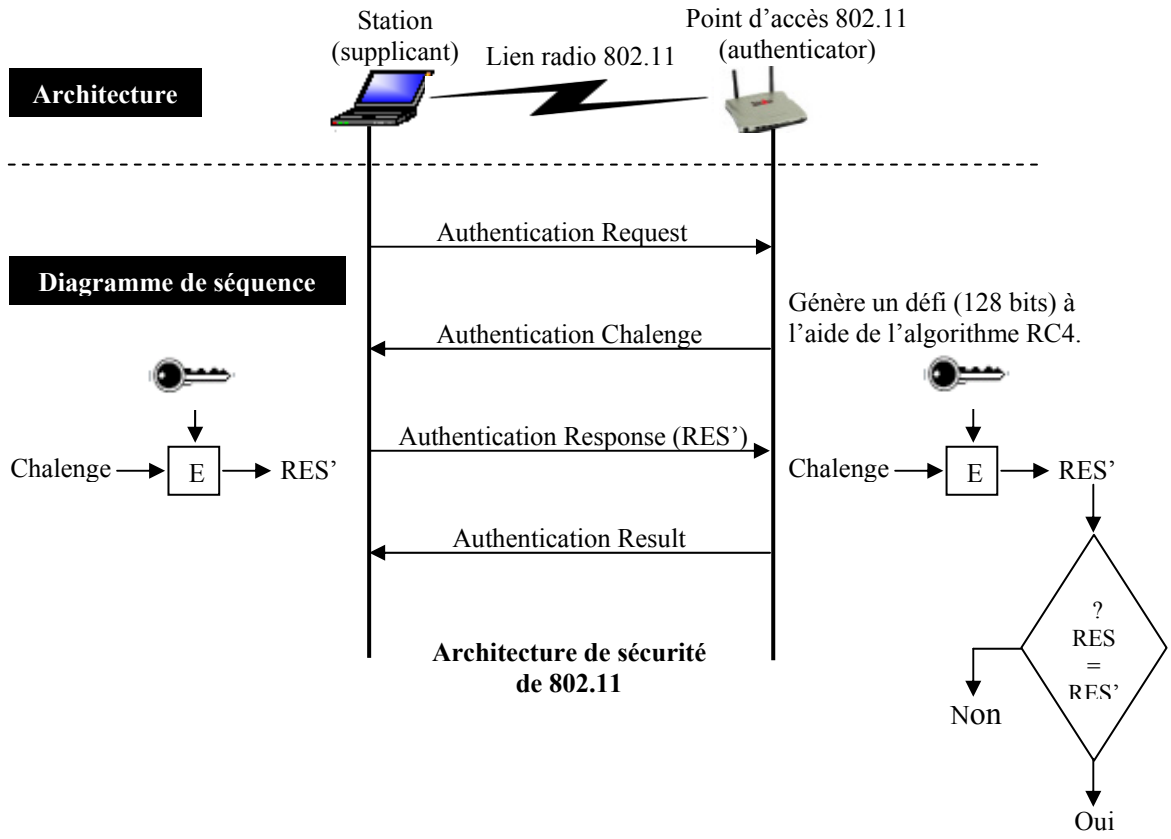


FIG III.20 – *L'authentification WEP* **[3]**.

III.3.1.6 – L'intégrité des données

Pour garantir ce critère, les messages transmis doivent être chiffrés. L'ICV est un CRC de 32 bits calculé sur le bloc de données. Il est chiffré ave la même clé que celle utilisée pour le chiffrement **[3]**.

III.3.1.7 – Les failles du WEP

Les failles du WEP ne sont pas liées seulement à l'algorithme de chiffrement RC4, mais à l'ensemble des mécanismes mis en œuvre, comme le vecteur d'initialisation ou le contrôle d'intégrité. Chacun de ces mécanismes comporte des défauts, qui, ajoutés les uns aux autres, permettent facilement de casser le WEP **[3]**.

Un groupe d'étudiants a démontré en 2005 au sein du laboratoire de recherche **STIC** (université de Tlemcen- Département de Télécom) que la clé WEP est cassable en quelques minutes **[3]**, constatation faite aussi bien avant, en 2001, par Scott Fluhrer, Itrik Mantin, et Adi Shamir **[3]**.

Donc, les faiblesses du WEP, le rendement non fiable pour gérer la confidentialité, l'authentification et l'intégrité des données.

La faille principale du WEP provient du fait que la règle *« Défense de réutiliser le même keystream plus d'une seule fois »* de l'algorithme de chiffrement par flot basé sur le XOR ne soit pas respectée. Le champ IV a été introduit dans le WEP parce que la clé *k* change rarement.

III.3.2 – Le SSID

L'accès au réseau se fait par l'intermédiaire du SSID. Ce dernier est transmis périodiquement en clair par le point d'accès dans des trames balises, ou *beacon frames*. Il est assez facile de le récupérer, que ce soit par l'utilisation d'un sniffer, ou d'un logiciel tel que *Netstumbler* **[3]**.

Il faudrait aussi penser à changer la configuration par défaut dans laquelle les SSID sont WaveLan Network chez Lucent ou Tsunami chez Cisco Systems. Cependant le mot de passe sera facilement obtenu.

III.3.3 – Les ACL

Le premier inconvénient des ACL est qu'il s'agit d'un mécanisme optionnel, très rarement utilisé. De plus, même si une personne possède une adresse MAC qui ne se trouve pas dans la liste ACL, elle peut toujours écouter le réseau et identifier les adresses MAC autorisées qui sont transmises en clair et les remplacer par sa propre adresse MAC **[3]**.

❖ La principale difficulté posée par le déploiement d'une architecture fondée sur le WEP réside dans la nécessité de partager un même secret entre stations et point d'accès. Le WEP n'est malheureusement pas suffisant pour assurer la sécurité dans les réseaux sans fil. les failles recensées ont démontré qu'il ne remplissait pas les objectifs pour lesquels il a été conçu.

De ce fait, les groupes d'études sur la sécurité des réseaux **Wi-Fi** se sont mis au travail pour pallier cette défaillance. Les travaux de la **Wi-Fi Alliance**, sont allés dans deux directions complémentaires : améliorer l'authentification en choisissant le standard **IEEE 802.1x**, et procéder à un changement de clé de chiffrement pour l'algorithme WEP. Ces modifications concernent la deuxième génération de sécurité pour les réseaux **Wi-Fi**. La troisième génération consiste en un changement de l'algorithme lui-même : au lieu du RC4, c'est l'algorithme AES qui est mis en œuvre. La partie qui va suivre du chapitre sera consacrée à la norme **802.1x [3]**.

III.4 – LA SÉCURITÉ DANS 802.1x

Le protocole d'authentification **IEEE 802.1x**, ou Port Based Network Access Control, permet de bloquer le flux de données d'un utilisateur non authentifié.

Puisqu'il est le standard le plus important, en matière d'authentification, il a été repris pour les réseaux sans fil.

III.4.1 – Le protocole IEEE 802.1x

Pour résoudre les problèmes de sécurité du standard **802.11**, l'**IEEE** propose le standard **802.1x** utilisant pour le contrôle d'accès, l'authentification et la gestion de clés. Son objectif est de bloquer le flux de données d'un utilisateur non authentifié. Le **802.1x** utilise un modèle qui s'appuie sur trois entités fonctionnelles **[37]** :

• Le système à authentifier (*supplicant*) : c'est un poste de travail (terminal informatique) demandant un accès au réseau.

• Le certificateur (*authenticator*) : c'est l'unité qui contrôle et fournit la connexion au réseau.

Un port contrôlé par cette unité peut avoir deux états : non autorisé ou autorisé.

• Le serveur d'authentification : il réalise la procédure d'authentification avec le certificateur et valide la demande d'accès.

Schématiquement, l'insertion d'une station mobile dans un environnement **802.1x** se déroule de la manière suivante :

• Après la phase d'association avec le point d'accès, ce dernier envoie au terminal une requête d'identité *EAP-Request.Identity*.

• La station mobile produit en retour une réponse *EAP-Response Identity.* Cette réponse comporte l'identité du client et les méthodes d'authentification supportées.

• A ce moment, le point d'accès transmet au serveur d'authentification le message *EAPResponseIdentity* encapsulé dans une requête RADIUS. Durant l'échange des messages EAP (requêtes et réponses) entre le serveur d'authentification et la station mobile.

• Le serveur d'authentification prend la décision d'accepter ou de refuser l'accès au réseau et il l'indique via le message *EAP-Success* ou *EAP-Failure*. Si le serveur d'authentification accepte le client, alors l'état du port change. Il passe à l'état autorisé, sinon, le port reste dans l'état non autorisé (figure III.21).

Après le succès de la phase d'authentification, le serveur transmet une clé (*Unicast*) de chiffrement (partagée avec la station mobile) au point d'accès qui l'utilise pour la génération de clés servant à chiffrer les données échangées avec la station.

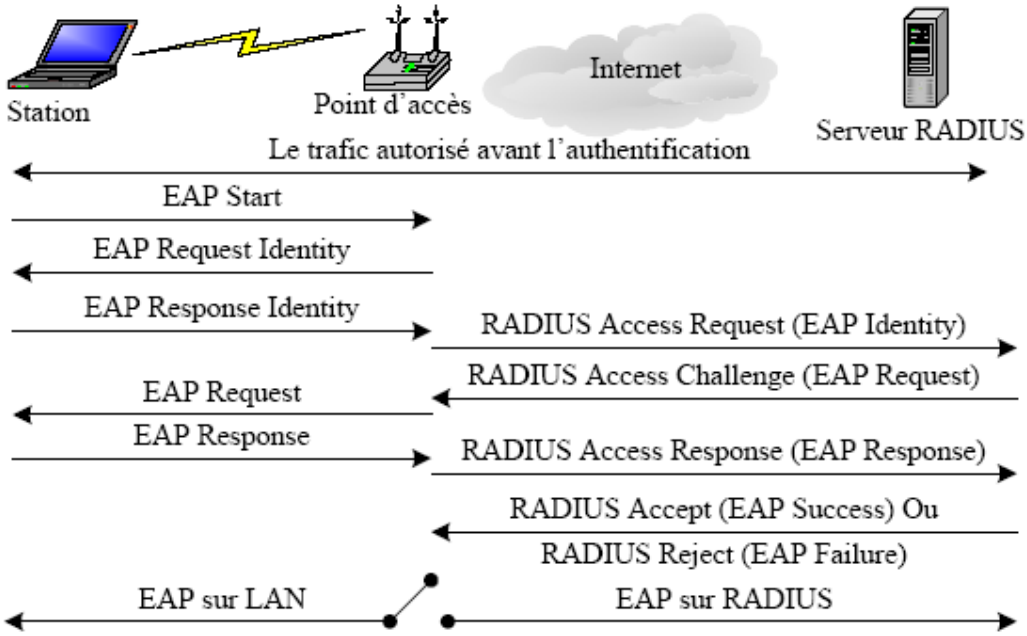


FIG III.21 – *L'architecture 802.1x.*

III.4.2 – Authentification par port [3]

La norme **802.1x** définit des mécanismes d'authentification des équipements fondés sur les ports :

- Dans l'état *unauthorized,* seules les trames EAP dédiées à l'authentification ne sont pas bloquées.
- Dans l'état *authorized*, le flux d'information transite librement **[3]**.

Le standard **802.1x** utilise les techniques d'encapsulation pour le transport des paquets EAP entre le port du client **802.1x** et le port du point d'accès ou du commutateur. Ces ports sont appelés PAE. L'encapsulation est connue sous le nom d'EAPoL (figure III.22).

EAPoL indique les débuts et fin d'une session d'authentification avec les messages de notification EAPOL-START et EAPOL-LOGOFF.

Ces mécanismes sont illustrés aux figures III.23 et III.24 **[3]**.

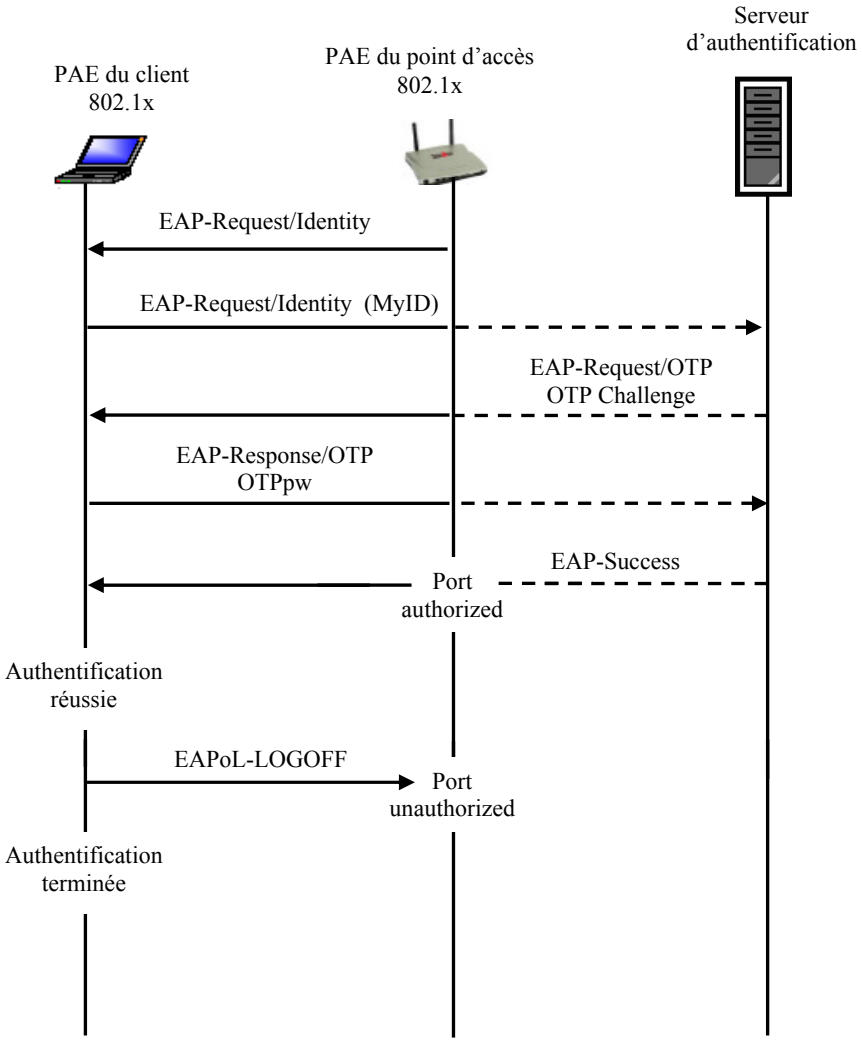


FIG III.22 – *Mécanisme de gestion de port* **[3]**.

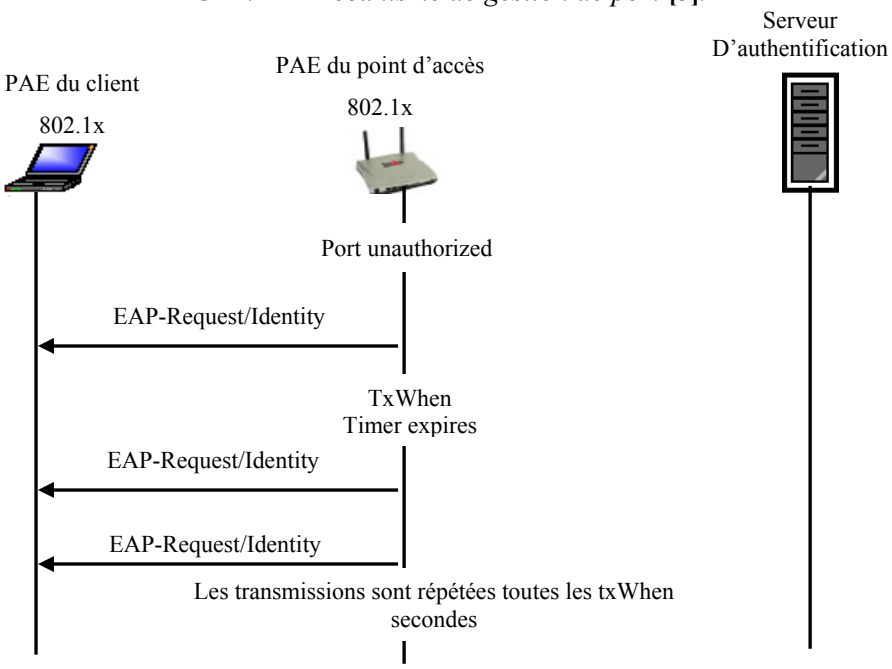


FIG III.23 – *Contrôle de l'entité PAE du point d'accès 802.1x* **[3]**.

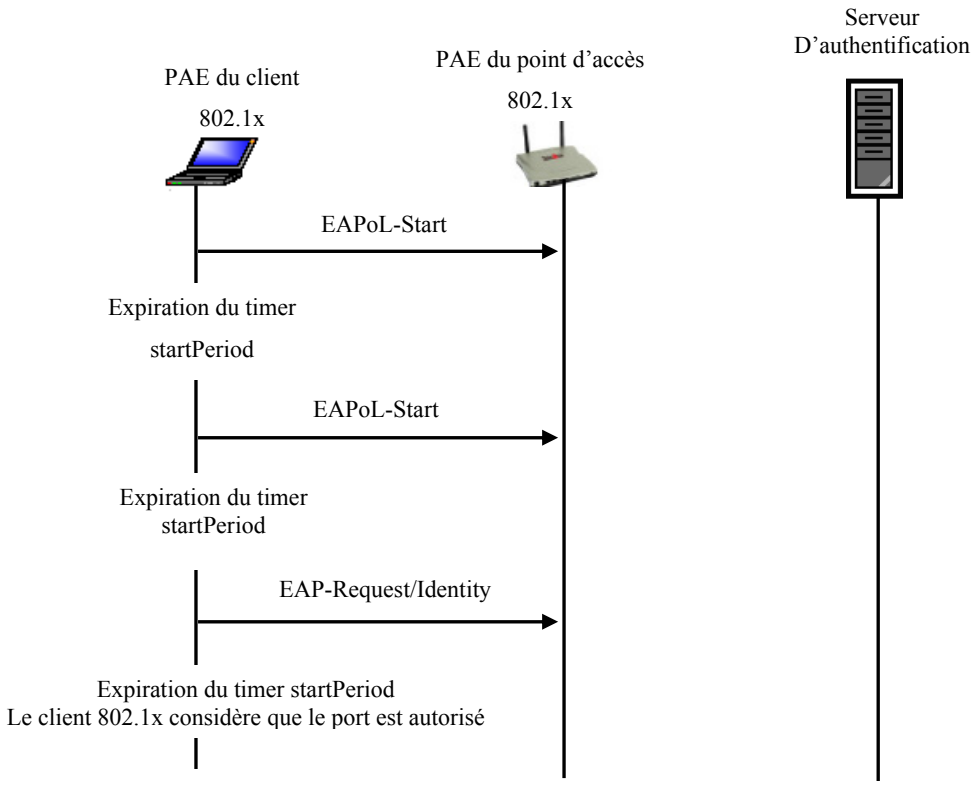


FIG III.24 – *Machine d'états du PAE du client 802.1x* **[3]**.

III.4.3 – Les méthodes d'authentification de 802.1x

EAP est l'actuel protocole d'authentification utilisé par les entités de **802.1x**. Dans le cas des réseaux **802.11** sans fil, les messages EAP sont transportés par des trames EAPoL.

Un message EAP comporte une entête de cinq octets et un champ optionnel des données. Les messages EAP se décomposent en quatre classes (figure III.25):

• Requête : utilisé pour les demandes d'authentification.

• Réponse : utilisé pour répondre à des demandes d'authentification.

• Succès et Echec : utilisés afin d'informer le point d'accès et la station mobile à propos du résultat de la procédure d'authentification.

La requête et la réponse sont étiquetées par le même *Identifier* compris entre 0 et 255. En plus, le message EAP contient un champ *Type* sur un octet qui désigne le protocole d'authentification transporté ou des opérations particulières.

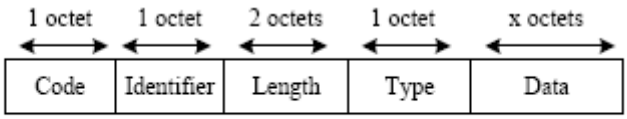


FIG III.25 – *Le format du message EAP* **[38]**.

Le protocole EAP est utilisé avec **802.1x** d'une manière transparente entre la station mobile et le serveur d'authentification passant par le certificateur. Ce protocole nécessite alors la coopération entre

un serveur d'authentification (comme RADIUS) et une méthode d'authentification, qui est une couche au-dessus d'EAP et définit des mécanismes de sécurité et de distribution de clés. Néanmoins, **802.11** n'a pas précisé la façon d'implémenter EAP avec **802.1x**. Pour cette raison, plusieurs couches sont définies au-dessus de EAP, citons LEAP, EAP-FAST, EAP-SIM, EAP-TLS, EAP-TTLS et PEAP **[38].**

III.4.3.1 – LEAP [3]

L'architecture de la méthode LEAP se base sur la procédure d'authentification disponible sur les plates-formes Windows.

L'authentification LEAP fonctionne de la façon suivante (figure III.26) :

1. À partir mot de passe utilisateur, une empreinte MD4 de 16 octets est calculée qui sera complétée par cinq octets nuls. Une suite de 21 octets est obtenue, interprétée sous la forme de trois clés DES de 7 octets soit 56 bits.

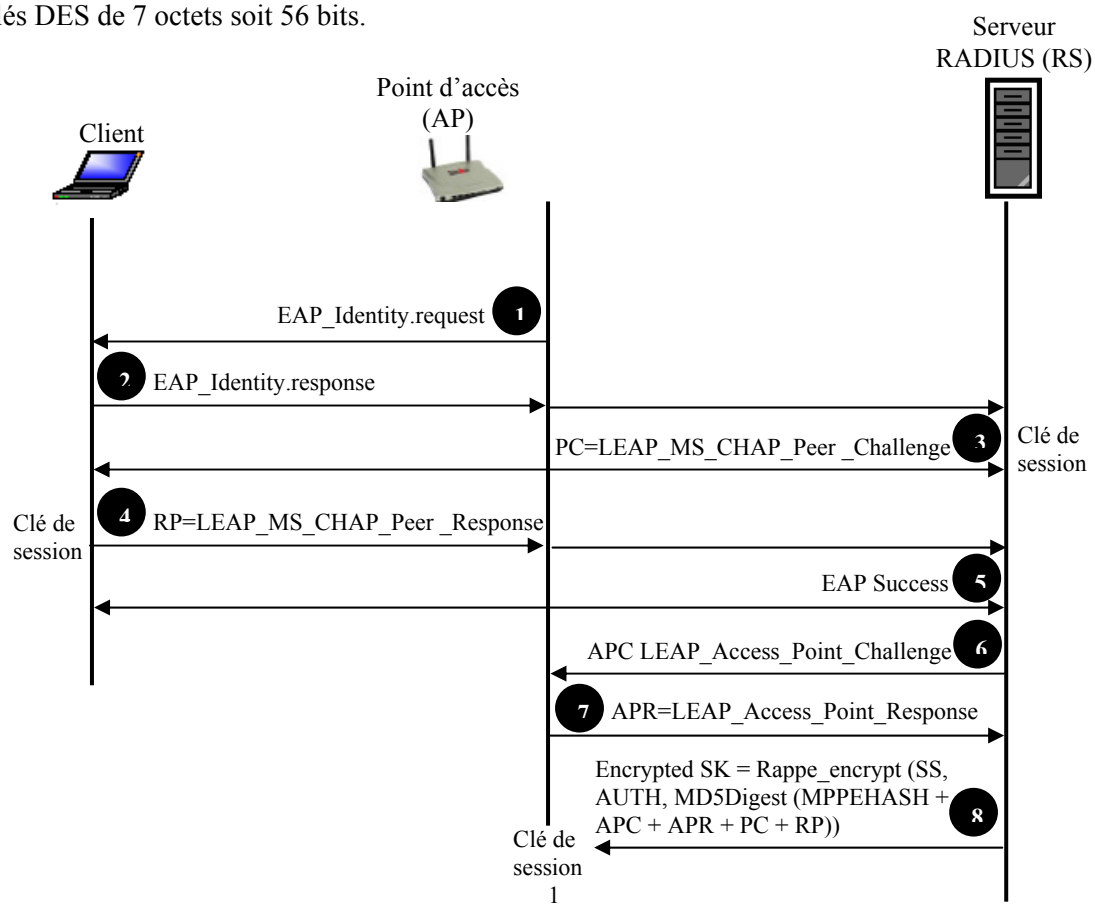


FIG III.26 – *Processus d'authentification LEAP* **[3]**

2. D'après un scénario d'authentification réussi entre supplicant et serveur RADIUS (correspondant aux phases 1 à 5 de la figure III.26), une clé de session SK est déduite par les deux entités (unicast), qui est transportée à l'aide d'un attribut propriétaire (CISCO-AVPAIR, LEAP SESSION KEY) du protocole RADIUS. LEAP supporte également des mécanismes de mise à jour de clés WEP, soit par la négociation d'une session RADIUS limitée (Session Timeout), soit par des

demandes périodiques de ré authentification par le supplicant à l'aide des trames EAP LOGOFF et EAP START **[3]**.

III.4.3.2 – EAP-FAST

EAP-FAST est un protocole d'authentification proposé par Cisco Systems, conçu pour résoudre les failles de sécurité du protocole LEAP dues aux mots de passes.

EAP-FAST est intégré dans l'ensemble des produits *Aironet* de *Cisco* ainsi que dans son serveur VPN Cisco Secure ACS. C'est une architecture de sécurité de type client-serveur, qui chiffre les transactions EAP au moyen d'un tunnel TLS. Cette solution est analogue à PEAP, à la différence essentielle prés que le tunnel EAP-FAST est établi à l'aide de secrets forts appartenant aux utilisateurs appelés PAC. Ils sont générés par le serveur Cisco Secure ACS à l'aide d'une clé maître connue uniquement du serveur Cisco Secure ACS. EAP-FAST est plus simple à mettre en place que les solutions qui chiffre les transactions EAP, comme EAP-TLS ou PEAP **[3].**

III.4.3.3 – EAP-TLS (figure III.27)

EAP-TLS est une méthode d'authentification standardisée par l'IETF, elle est basée sur le protocole TLS qui est actuellement une solution crédible pour la sécurisation des échanges.

L'authentification de TLS avec EAP est simple. Le serveur et la station mobile s'authentifier après la phase *« Handshake »* de TLS en utilisant des certificats de type **X.509**. Les messages TLS seront fragmentés et encapsulés dans des paquets EAP-TLS. Ceci est dû au fait que, la taille d'un *record* TLS est d'au plus 16384 octets alors que le protocole RADIUS limite sa charge utile à 4096 octets et de surcroît la taille des trames **802.11** est limitée à 2312 octets.

La clé de la session TLS est utilisée afin de générer d'autres clés servant à établir un canal chiffré entre la station et le certificateur. Les étapes suivantes expliquent en détail le déroulement d'une session EAP-TLS :

La session EAP-TLS commence précisément entre la station et le point d'accès. Après la phase d'association, le point d'accès envoie une requête d'authentification à la station.

La station répond avec l'identifiant de l'utilisateur. Ce message est relayé par le point d'accès vers le serveur d'authentification.

Le serveur d'authentification initie le processus d'authentification de TLS après l'envoi du paquet *EAP-TLS/start*.

La station envoie le paquet *EAP-Response* contenant le message *ClientHello* de TLS indiquant la version du protocole TLS supportée par le client, une valeur aléatoire et une liste d'algorithmes cryptographiques supportés par le client mobile **[38]**.

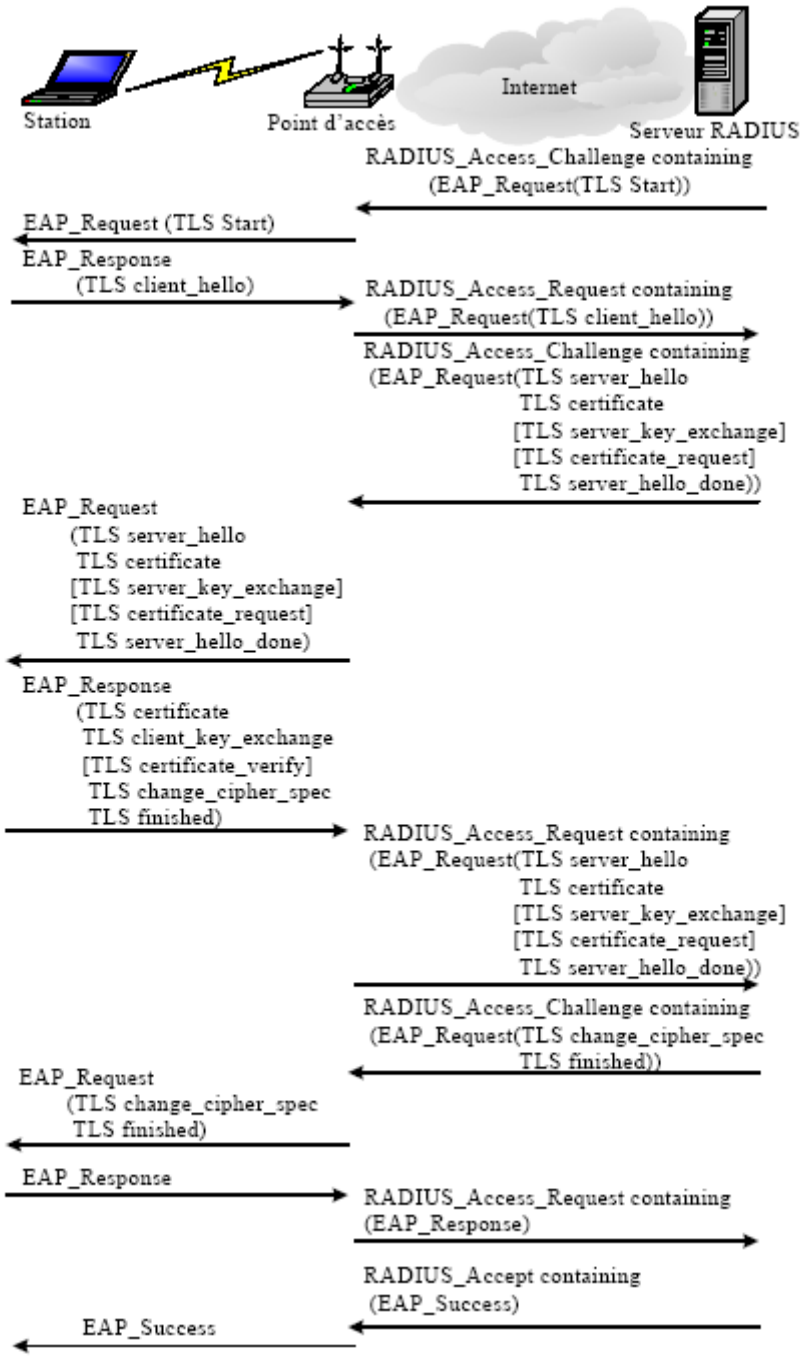


FIG III.27 – *L'authentification EAP-TL S* **[38].**

Le serveur doit répondre par un paquet *EAP-Request* contenant le message *ServerHello* du TLS. Le message hello du serveur est suivi par son certificat contenant sa clé publique, par une demande du certificat du client et par le message *ServerHelloDone* pour d'indiquer la fin de son hello.

Le client répond par un paquet *EAP-Response* contenant les messages certificat, le *ClientKeyExchange* comportant la clé secrète *pre_master_secret*, *CertificateVerify*, *ChangeCipherSpec* et *Finished*.

Le client et le serveur définissent une clé de session et calculent les clés de chiffrement et d'authentification et les vecteurs d'initialisation. Ensuite, le serveur répond par un paquet *EAPRequest,*

le champ de données encapsule les messages *ChangeCipherSpec* et *Finished* de TLS. Le message *Finished* termine la phase d'authentification de TLS.

Un paquet *EAP-Response* est envoyé par le client, le serveur répond alors par un *EAP-Success*.

Á la fin de la phase d'authentification, le serveur envoie la clé de chiffrement au point d'accès en utilisant l'attribut RADIUS *« MS-MPPE-Recv-Key »*. Cette clé sera utilisée par le point d'accès afin de chiffrer et signer la clé (par exemple WEP ou WPA) avant d'être transmise au client.

La méthode EAP-TLS assure une authentification efficace à l'aide de certificats numériques. L'utilisation du certificat protége les entités contre plusieurs attaques ; notamment l'attaque *Man-In-The-Middle*. L'utilisation des certificats avec EAP-TLS exige une infrastructure à clé publique (PKI). Cette infrastructure ne peut pas être toujours déployée dans plusieurs types d'entreprises. En plus, elle entraîne un surplus important en terme de gestion et de ressources machines et humaines **[38]**.

III.4.3.4 – EAP-TTLS

EAP-TTLS une méthode qui utilise le protocole EAP et le tunnel TLS dans le but d'établir une session authentifiée et sécurisée entre la station **802.1x** et le serveur d'authentification. Elle étend l'EAP-TLS. Les certificats PKI ne sont en effet nécessaires que sur le serveur d'authentification. L'authentification du client peut se réaliser par d'autres moyens que le certificat ; mot de passe (CHAP, MSCHAPv2) ou carte à puce.

EAP-TTLS distingue deux phases d'authentification :

• Tunnel TLS, c'est une session TLS avec l'authentification du serveur par un certificat valide.
Elle sert à protéger les échanges de la deuxième phase.

• Identification du client par le serveur en utilisant une méthode simple (CHAP, MSCHAPv2), carte à puce, etc.).

L'avantage qu'a EAP-TTLS par rapport à EAP-TLS, est d'assurer la protection de la notification du mécanisme d'authentification et de l'identité du client grâce au tunnel TLS établi durant la première phase. Ce tunnel garantit la confidentialité des échanges pour la deuxième phase. Ce qui donne l'avantage à l'administrateur du réseau de choisir une simple méthode d'authentification pour ses utilisateurs (mot de passe transit en clair dans le Tunnel TLS) et donc de supprimer la complexité de gestion liée aux certificats et à l'infrastructure à clé publique.

En revanche, EAP-TTLS n'est pas toujours protégée contre l'attaque *Man-In-The-Middle*. En effet, le protocole d'authentification utilisé durant la deuxième phase ne peut pas être conscient s'il est accompli en mode tunnel ou non, c'est-à-dire qu'EAP-TTLS ne relie pas cryptographiquement les clés de session dérivées par le protocole interne avec celles dérivées par le protocole externe. L'intrus peut intervenir comme un utilisateur légitime dans la première phase du protocole EAP-TTLS.

Cela lui permet d'établir une connexion TLS avec le serveur et d'avoir les clés du tunnel TLS. Cette étape est possible puisque aucune authentification n'est exigée du côté de l'intrus.

L'intrus cherche ensuite à provoquer les clients qui sont attachés avec son point d'accès. Son objectif étant de les inciter à utiliser un mécanisme d'authentification autorisé avec le tunnel. D'autres conditions doivent être obtenues afin de réaliser cette attaque : le client doit utiliser les mêmes crédits (i.e. login et mot de passe) en mode tunnel et non-tunnel et l'intrus doit être capable de jouer le rôle du serveur d'authentification.

III.4.3.5 – PEAP [3]

PEAP et EAP-TTLS sont presque semblables. Les deux protocoles utilisent un canal TLS pour protéger un second échange EAP. Ils conservent les fondations cryptographiques de TLS mais appliquent d'autres mécanismes d'authentification du côté client. Par exemple, l'authentification du client PEAP n'ayant pas un certificat, elle peut être établie en utilisant MSCHAPv2 durant la phase 2.

III.4.3.6 – EAP-SIM [3]

Une solution classique d'authentification est proposée par les opérateurs de téléphones mobiles de deuxième génération, ou **GSM**, selon une procédure d'authentification réalisée entre le serveur de l'opérateur et la carte SIM située dans le terminal de l'utilisateur. Cette authentification utilise des protocoles provenant de l'ETSI.

Le protocole EAP-SIM est une extension normalisée d'EAP pour le monde IP que les opérations peuvent utiliser dans les hotspots.

Dans les lieux de densité importante de population, les cartes à puce du réseau **GSM** peut être utilisée pour les réseaux sans fil, avec une convention entre les différents opérateurs pour une extension possible de leurs réseaux.

III.4.4 – le serveur d'authentification RADIUS

L'évolution du standard **802.1x** intègre l'ensemble des évolutions du protocole RADIUS spécifié par le RFC 2869. Le protocole RADIUS s'appuie sur une architecture client/serveur et permet l'accès à distance. Il assure également l'interface avec une infrastructure AAA gérant les comptes utilisateurs en collaboration avec un annuaire LDAP. Ainsi que le transport des données d'authentification, d'autorisation et de facturation entre un serveur d'authentification partagé et les NAS distribués voulant authentifier leurs clients.

L'accès d'un client à un fournisseur de services, nécessite l'envoi de son accréditation d'authentification (login et mot de passe) au NAS. Il réalise un pont entre le client et le serveur RADIUS et transmet l'accréditation à ce serveur par le message *« Access-Request »*.

Après les échanges *Access-Challenge* et *Access-Request*, le serveur RADIUS vérifie l'identifiant du NAS et l'appartenance du client à sa base de données. Ensuite, à l'aide de l'un des deux messages *Access-Reject* ou *Access-Success*, il indique au NAS le succès ou l'échec de la demande du client.

Le point d'accès dans les réseaux **802.1x** sans fil joue le rôle du NAS. Il transmet les informations d'authentification fournies par la station vers le serveur RADIUS. Dans ce cas, le transport quasi transparent du message EAP par RADIUS permet de mettre en place une architecture générique indépendante de la méthode d'authentification utilisée par les ISP **[38]**.

Scénario d'une session d'authentification EAP avec RADIUS

Le scénario d'une session d'authentification EAP peut se dérouler comme suit :

• Le NAS transmet au serveur RADIUS le message *EAP-Response.Identity* dans un *Access-Request*.

• Le serveur RADIUS recherche l'utilisateur dans la base de données de clients. Il obtient le type du scénario d'authentification (TLS, TTLS, MD5, etc.) et les lettres de crédits nécessaires (mot de passe, secrets partagés, certificats, etc.).

• Plusieurs paires de messages *EAP-Request*.type et *EAP-Response*.type sont transmises par des paquets RADIUS *Access-Challenge* et *Access-Request*. Le succès de l'opération est notifié par un *Acces-Success* (et le message *EAP-Success*). L'échec est indiqué par un *Access-Reject* (et le message *EAP-Failure*).

Au bout de l'authentification, certaines méthodes EAP calculent une clé nommée Master Key (MK).

Dans les environnements Microsoft, ce secret est un couple de clés *MS-MPPE-Send-Key* et *MS-MPPE-Recv-Key* (2 fois 32 octets).

Ces éléments sont transportés dans le message *Access-Success* et sont chiffrés par une clé qui est déduite du secret partagé, et un nombre aléatoire (le champ *Authenticator*) contenu dans un précédent message *Access-Request*. Le point d'accès choisit une clé WEP. Il réalise son chiffrement à l'aide de MK et délivre le résultat au *Supplicant* en utilisant une trame *EAPoL-Key* (chiffrée par *MS-MPPE-Send-Key* et signée par *MS-MPPE-Recv-Key*) **[38]**.

III.4.5 – Les risques avec l'authentification 802.1x

La plupart des méthodes d'authentification offrent deux phases : d'authentification, de chiffrement et d'intégrité. Etant donné que le protocole **802.1x** est purement un protocole d'authentification, cette deuxième phase reste inutilisable. En plus, il ne résout pas totalement le problème du WEP **[38].**

III.4.5.1 – Une authentification à sens unique

Le traitement asymétrique d'authentification entre la station et le certificateur pose problème pour le **802.1x**. Le port devient contrôlé après le succès de la phase d'authentification. Ce n'est pas applicable pour la station dont le port reste toujours à l'état authentifié. L'authentification à sens unique expose la station à plusieurs attaques ; notamment *« Man-In-The-Middle »* et *« Denial-of-Service »*.

III.4.5.2 – L'attaque "Man-In-The-Middle"

L'intrus agit comme : un légitime certificateur pour la station et un client authentifié pour le réseau. Dans l'architecture **802.1x**, la machine d'état de la station n'accepte que les requêtes EAP du certificateur et ne lui répond que par des réponses EAP. Par conséquent, la machine d'état du certificateur n'accepte aucune requête EAP de la station. Les états de machine n'effectuent donc qu'une authentification à sens unique et un changement significatif sera obligatoire dans le protocole afin d'assurer l'authentification mutuelle **[38]**.

III.4.5.3 – Le détournement des sessions

Le standard **802.1x** propose une architecture robuste pour la sécurité du réseau appelée RSN. Cette architecture basée sur **802.1x**, fournit un contrôle d'accès reposant sur une authentification forte de la couche supérieure. Pour cela, deux machines d'états doivent être créées : une pour **802.1x** et une autre pour RSN.

Par l'absence de communication entre les deux machines d'états et le manque de l'authenticité des messages, un intrus peut détourner la session en profitant de la faille de synchronisation entre ces deux machines.

L'attaque peut se dérouler comme suit (figure III.28):

• Phase 1: La station s'authentifie auprès du certificateur en utilisant une méthode d'authentification EAP.

• Phase 2 : L'intrus envoie un message de gestion *«* **802.11** MAC *disassociate »* en utilisant (*Spoofing*) l'adresse MAC du certificateur. Ce message a pour but de changer l'état de machine de RSN à l'état *Unassociated,* mais l'état de machine de **802.1x** du certificateur reste toujours à l'état *authenticated*.

• Phase 3 : L'intrus reprend le port authentifié du certificateur en *« Spoofing »* l'adresse MAC de la station.

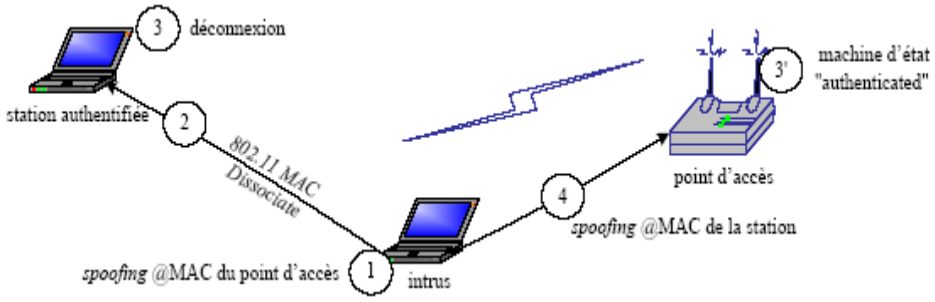


FIG III.28 – *Détournement de la session.*

III.4.6– Les perspectives de 802.1x

Le standard **802.1x** a été conçu afin de protéger l'infrastructure de réseau **Wi-Fi** et non pas le terminal du client.

Conçu pour sécuriser les réseaux **802.11** fixes, les protocoles EAP et **802.1x** ne répondent pas aux besoins de sécurité du réseau **Wi-Fi** et ils deviennent inefficaces face à plusieurs attaques ; notamment celles qui s'adressent à l'infrastructure du réseau. Une raison majeure de cette faiblesse réside dans la séparation entre la machine d'états de **802.1x** et celle du RSN.

Le protocole TLS fait appel à des documents électroniques appelés C*ertificats* pour garantir l'authentification du client.

III.5 – CERTIFICATS ET AUTORITÉ DE CERTIFICATION [39]

III.5.1 – Définition

Un certificat est un document électronique, c'est la combinaison entre une clef publique, son propriétaire (une personne, une application, un site) et l'application pour laquelle il est émis :

- Il permet de prouver l'identité d'un utilisateur ;
- Pour une application il assure que celle-ci n'a pas été détournée de ses fonctions ;
- Pour un site, il garantie à l'utilisateur qu'il est bien sur le site qu'il voulait accéder.

Le certificat est signé: une empreinte du certificat est effectuée à l'aide d'algorithme (MD5 par exemple), l'empreinte obtenue est chiffrée.

Le chiffrement s'effectue avec la clé privée de l'autorité de certification qui possède elle même son propre certificat **[39].**

III.5.2 – Vérification d'un certificat (figure III.29)

La vérification s'effectue avec la clé publique de l'autorité de certification. Sur la figure ci-dessous, un test est effectué sur la validité du certificat de Wassila délivré par l'Autorité de certification.

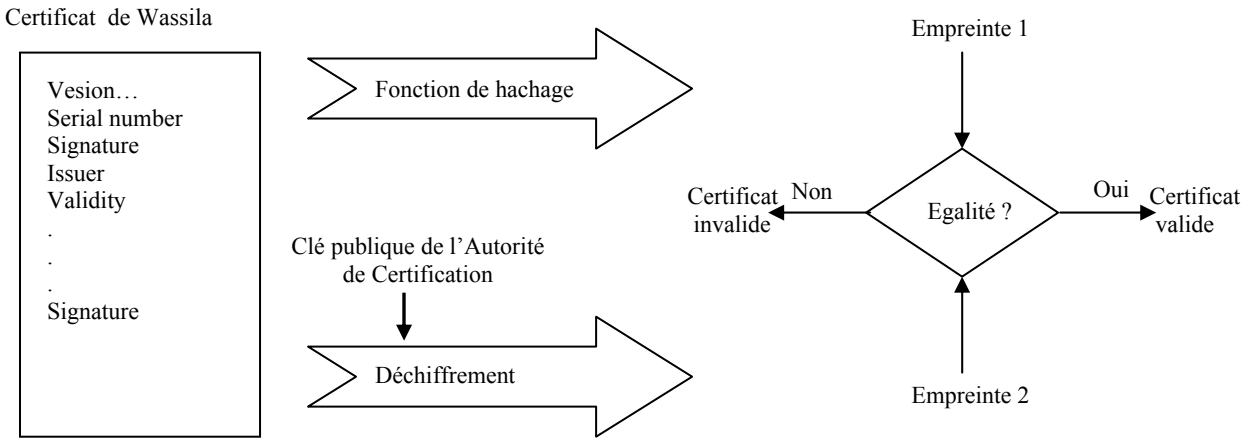


FIG III.29 – *Vérification de certificat.*

III.5.3 – Autorité de Certification [39]

Une Autorité de Certification est une organisation qui délivre des certificats électroniques à un ensemble d'utilisateurs.

Une AC possède elle-même un certificat, son certificat est autosigné ou délivré par une autre AC. Elle utilise sa clé privée pour créer les certificats qu'elle délivre, une AC joue le rôle de tiers de confiance.

Les certificats délivrés ont un champ d'applications important :

- limité à l'intérieur d'un organisme ;
- échanges inter-organismes ;
- … ;

III.5.4 – Certification croisée et certification hiérarchique

Il est possible de mettre en place des relations de confiance hiérarchiques ou croisées entre ACs (figure III.30).

Dans le cas d'une relation hiérarchique, un certificat est délivré par une AC dite racine à une ou plusieurs autres ACs, qui elles mêmes peuvent délivrer un certificat à d'autres ACs et ainsi de suite.

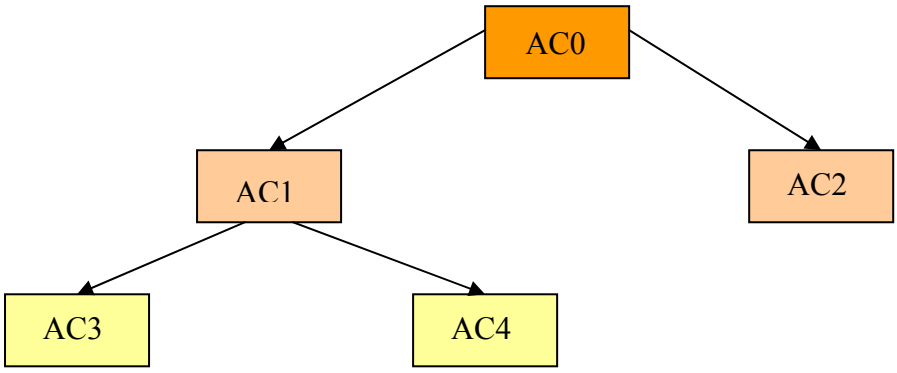


FIG III.30 – *Hiérarchie d'ACs.*

Les relations de confiance sont appelées à établir une relation confiante entre deux organismes ayant chacun leur propre AC, AC1 et AC2, n'appartenant pas à une même arborescence. Dans ce cas, AC1 et AC2 peuvent chacun créer un certificat en signant la clé publique de l'autre **[39]**.

III.5.5 – IGC [39]

Un certificat électronique est similaire à une carte d'identité. Dans ce cas, l'AC peut être comparée à la préfecture qui délivre les pièces d'identités.

Les certificats électroniques sont mis en oeuvre à travers une infrastructure qui est l'IGC.

L'IGC est constituée de l'ensemble des matériels, logiciels, personnes, règles et procédures nécessaire à une Autorité de Certification pour la création, la gestion et la distribution des certificats X509. Les fonctions principales d'une IGC sont (figure III.31):

- Émettre et révoquer des certificats
- Publier les certificats dans un annuaire
- Éventuellement, fournir un service de séquestre et de recouvrement des clés privées.

Elle est constituée par :

- Une autorité de certification (**AC**)
- Une autorité d'enregistrement (**AE**)
- Un opérateur de certification (**OC**)
- Un annuaire de publication de certificats
- Un service de validation
- Éventuellement, un service de séquestre de clés.

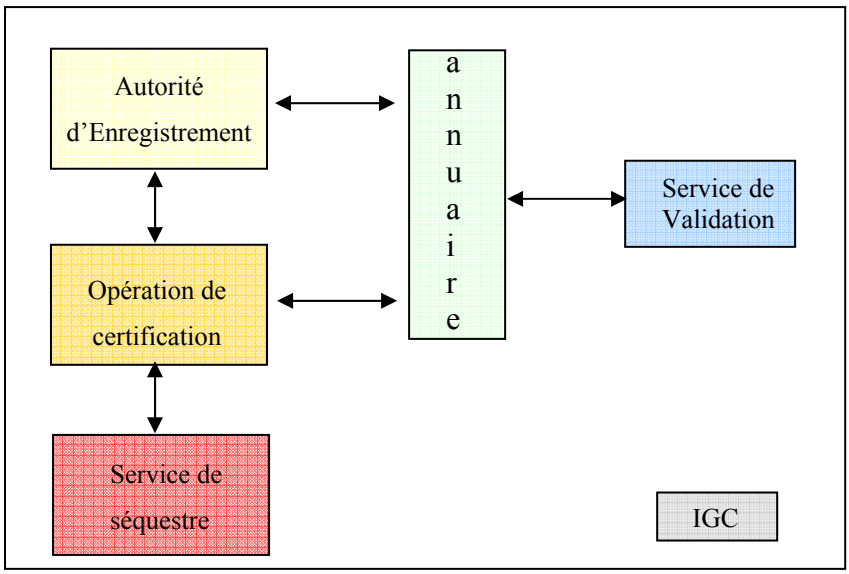


FIG III.31 – *Structure d'une IGC.*

III.5.6– Autorité d'Enregistrement [39]

L'AE est chargée de la réception et le traitement des demandes de création, de renouvellement et de révocation des certificats, elle doit :

- Assurer le contrôle des données identifiant le demandeur de certificat,
- Valider les demandes de révocation,
- Assurer lors de la délivrance d'un nouveau certificat (sur date de péremption atteinte) un recouvrement des certificats afin d'assurer la continuité pour la fonctionnalité signature et/ou chiffrement.

III.5.7 – Opérateur de certification [39]

L'Autorité de Certification délègue à l'Opérateur de Certification toutes les opérations nécessitant la clé privée de l'AC : création et distribution sécurisée des certificats, révocation, production de cartes à puces…

L'OC gère en collaboration avec l'autorité d'enregistrement les cycles de vie des certificats. La sécurisation physique de l'OC doit également être étudié avec soin.

III.5.8 – Annuaire de publication [39]

Une IGC doit rendre publique les certificats pour les rendre accessibles aux partenaires voulant échanger leurs clés publiques. L'annuaire contenant ces certificats peut également contenir le certificat de l'AC et les CRLs.

III.5.9 – Scénario de demande de certificat [39]

La figure III.32 donne un exemple de scénario possible pour une demande de certificat. Dans ce scénario, la bi-clé est générée par l'utilisateur.

1. l'utilisateur fait sa demande à l'AE.
2. l'AE vérifie les données d'identification et vérifie la possession de la clef privée. Si tout est OK, l'AE valide la requête qui est transférée à l'OC.
3. l'OC vérifie la validité de la requête et génère le certificat. Le certificat est publié dans l'annuaire et transmis à l'AE.
4. l'AE avertit l'utilisateur que son certificat est disponible.
5. l'utilisateur récupère le certificat dans l'annuaire.

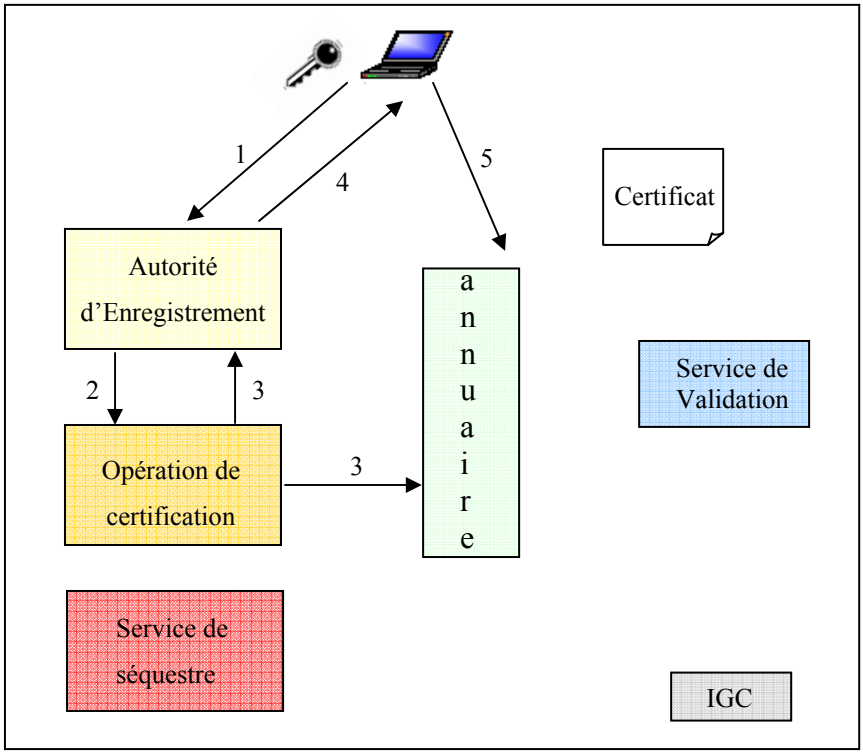


FIG III.32 – *Scénario de demande de certificat* **[39]**

III.5.10 – Service de validation [39]

Un certificat émis par une IGC peut devenir invalide pour différentes raisons :

- Perte ou vol de la clé privée associée ;
- Fin de mandat ;
- Date de péremption ;
- … ;

Une IGC doit fournir un service de validation permettant à tout instant de vérifier la validité des certificats qu'elles délivrent. Ceci se fait par la publication d'une liste appelée CRL.

Une CRL a un format standardisé et est signée à l'aide de la clé privée de l'AC émettrice. Elle peut être publiée via le même annuaire de publication que les certificats.

Cette technique pourrait être substituée par un nouveau protocole : OCSP à travers lequel un client OCSP pourra vérifier la validité d'un certificat donné en interrogeant un serveur OCSP. Cela permettra la diffusion quasi instantanée de l'information concernant la révocation d'un certificat.

III.6 – PRINCIPES DU STANDARD SSL [39]

Le standard SSL a été proposé par Netscape, la version 3 de ce protocole date de 1996, elle est disponible dans de très nombreuses applications et est très utilisée. TLSv1 est largement compatible avec SSLv3.

La figure III.33 montre la place de SSL dans l'empilement des couches de protocole.

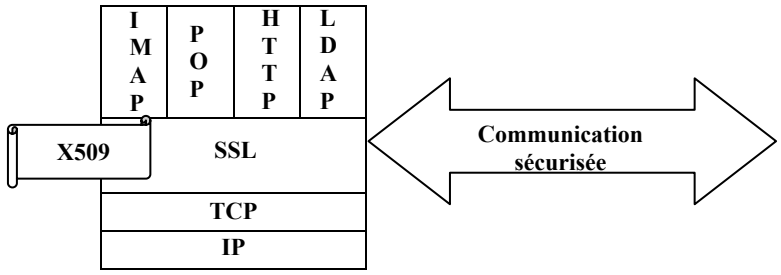


FIG III.33 – *Couche SSL.*

Un certain nombre d'applications a été adapté pour exploiter la couche SSL ; des ports standard ont été attribués à ces applications (tableau III.1):

Protocole	Port
LDAP	636
POP3S	995
IMAPS	993
NNTPS	563
HTTPS	443

TAB III.1 – *Les ports standard.*

SSL est divisé en deux sous-couches :

- La sous-couche basse « ssl record protocol », appuyée sur une couche transport, principalement TCP, encapsule les éléments de protocoles supérieurs.
- La sous-couche « SSL handshake protocol » permet en premier lieu au client de s'authentifier et de négocier un algorithme de chiffrement.

Les apports de SSL sont:

- Confidentialité de la communication. Les utilisateurs disposent d'une clef secrète à usage unique utilisée pour le chiffrement symétrique (DES RC4, …) de la suite des échanges.
- Les parties peuvent s'authentifier en utilisant leurs clefs publiques et des algorithmes de chiffrement asymétriques (RSA, DSS, …)
- L'intégrité des échanges est garantie par l'emploi d'une empreinte numérique (SHA, MD5, …).

La négociation initiale (SSL handshake protocol) permet de faire un choix sur les paramètres de chiffrement de la session. Les paramètres retenus au début de la session sont : la version du protocole SSL et la d'algorithmes de chiffrements.

Pour assurer la confidentialité de la suite des échanges par du chiffrement symétrique, un secret partagé est généré par des techniques de chiffrement à clés publiques.

SSL handshake protocole assure la coordination entre les parties qui partagent un état de la session comprenant en particulier :

- Un identificateur de session (une séquence d'octets arbitraire choisie par le serveur et permettant d'identifier de part et d'autre une session SSL parmi plusieurs),
- Les certificats X509 V3 des partenaires si utiles,
- La méthode de compression des données (compression avant chiffrement),
- L'algorithme de chiffrement choisi pour cette session,
- Les clefs de chiffrement symétriques.

III.6.1 – TLS [39]

TLS est une évolution du protocole de Netscape SSL V3. Il est voisin de SSL. La plupart des implémentations de SSL (clients et serveurs) supporte les deux protocoles de la version 1 et 3.

III.6.2 – Openssl : l'implémentation de référence de SSL

Openssl est une suite logicielle de chiffrement destinée aux développeurs. Ce produit fait partie de la plupart des distributions Linux. Openssl se présente sous la forme d'un ensemble de librairie, la commande en ligne Openssl peut être utilisée pour manipuler des certificats x509.

III.7 – IPSec et VPN [38]

Le protocole **802.1x** offre un niveau de chiffrement au niveau 2 en utilisant le WEP et/ou le TKIP (WPA). Le réseau VPN, utilisant IPSec, peut offrir un chiffrage au niveau 3 entre la station mobile et la destination. Avec EAP et dans le cas où le NAS supporte IPSec, il serait mieux d'abandonner les services de sécurité fournis par la couche applicative du RADIUS et d'exécuter RADIUS sur IPSec en mode ESP *non-null transform.*

Malgré les avantages de la solution IPSec/VPN, il est préférable d'utiliser le **802.1x** entre une station mobile et un agent dans le réseau puisque:

Dans la norme **802.1x** le canal est chiffré avant qu'un utilisateur mobile soit authentifié et ait une adresse IP, cette norme offre une protection au niveau 2.

Dans le cas d'IPSec, après l'association entre le client mobile et le point d'accès et après l'authentification du client (l'absence de **802.1x**) donne la possibilité de réaliser plusieurs attaques ; notamment l'attaque *«* Man-In-The-Middle *»*. Le chiffrement sera établi au niveau 3.

- L'IPSec ne supporte pas la transmission de trafic en mode broadcast/multicast. Il a été construit pour les liens point à point.
- Les clients ont la possibilité de changer leur point d'accès à n'importe quel moment. Cette étape oblige les clients mobiles à se ré authentifier dans le cas où ils gardent la même adresse IP.
- L'utilisation de l'IPSec requière une puissance significative de traitement nécessaire pour établir un canal VPN par un terminal. Dans **802.1x**, le chiffrement WEP utilise RC4 et il est achevé par un

co-processeur intégré dans la carte adaptée sans fil, il n'ajoute donc aucune charge cryptographique aux processeurs du mobile. Néanmoins, IPSec utilise DES et 3DES comme algorithmes de chiffrement symétrique, ils sont plus coûteux en temps d'exécution que RC4. en plus, IPSec n'est pas intégré dans les cartes adaptées sans fil mais il utilise directement le CPU du terminal mobile et du serveur. Ce qui oblige les serveurs fréquemment accessibles d'ajouter des accélérateurs hardware ou Software afin de réduire le coût du calcul cryptographique exigé par l'IPSec.

❖ Bien que l'apport en sécurité dans la norme **802.1x** soit important, les risques d'attaques existent toujours. Les méthodes d'authentification et les protocoles de sécurité **802.1x** garantissent à un certain niveau la sécurité du réseau.

Chaque norme a ses propres mécanismes de sécurité, donc à nous de choisir quelle est la méthode la plus adéquate à notre réseau.

La norme **802.11i** plus particulièrement se charge de renforcer la sécurité des réseaux **Wi-Fi.** Il est important de citer ses principales caractéristiques et les protocoles utilisés.

III.8 – LA NORME 802.11i [3]

Les faiblesses du WEP sont incontestables, le groupe IEEE **802.11i** a mis au point une architecture pour remédier à ces lacunes.

Le comité industriel de la **Wi-Fi** alliance, anciennement WECA, a édité le 29 avril 2003 la recommandation WPA, fondée sur un sous ensemble du standard IEEE **802.11i.** Depuis l'année 2004 le WPA fut implémenté dans les équipements **Wi-Fi**.

La norme 802.11i fut finalisée en janvier 2004, elle marque une étape plus importante puisqu'elle projette de sécuriser les réseaux sans fil pour les années à venir.

Cette norme de troisième génération, estampillée WPA2 sur les produits n'est pas compatible avec les générations précédentes. Elle met en cause tous leurs investissements considérables en sécurité.

Ceci est du à l'utilisation de l'algorithme de chiffrement AES, qui ne peut être chargé dans le firmware des cartes **Wi-Fi**.

Les apports de **802.11**i peuvent être classés en trois catégories.

- Définition de multiples protocoles de sécurité radio ;
- Eléments d'information permettant de choisir l'un d'entre eux ;
- Nouvelle méthode de distribution **[32]**.

III.8.1 – Le mécanisme WPA

Pour sauver les ventes des équipements **Wi-Fi**, les constructeurs se sont vus obligés de trouver une parade devant les failles du WEP. Pour cela l'IEEE préparait la norme **802.11i** basée sur le chiffrement

AES. Cependant, cela nécessitait de mettre à jour tout le parc : les cartes **Wi-Fi** actuelles n'ont pas la puissance nécessaire pour faire du chiffrement AES.

III.8.1.1 – Un WEP amélioré

Le protocole WPA repose sur le WEP et permet de conserver le matériel existant en nécessitant uniquement une mise à jour du *firmware*, qui est le logiciel embarqué dans le matériel.

WPA est un sous-ensemble de la norme **802.11i** regroupant **802.1x** et TKIP et visant à pallier les failles de sécurité du WEP. Le standard WPA est transitoire et est déjà en cours de remplacement par la version de **802.11i** appelé WPA2, qui utilise le mécanisme de chiffrement AES.

WPA et WPA2 présentent des différences significatives. En particulier, le protocole par défaut WPA et TKIP et celui de WPA2 CCMP.

Ces deux protocoles sont censés garantir la sécurité des réseaux sans fil au moins pour quelques anées. WPA a la possibilité d'être introduit dans le firmware des cartes **802.11** construites avant 2004. Du fait que le WPA utilise les mêmes protocoles que le WEP. En revanche, l'algorithme de chiffrement AES n'étant pas implémenté en natif dans les cartes **802.11**, une modification du firmware n'est pas possible.

Etant donné l'incompatibilité des deux générations, il faudrait que la nouvelle génération de carte intègre les deux algorithmes de chiffrement. De tells cartes seraient compatibles WPA et WPA2, ce qui permettrait de les utiliser en TKIP avec la sécurité nécessaire.

III.8.1.2 – Les défauts

Le WPA est considéré un mécanisme sûr de sécurité, il est cependant supporté par une grande partie du matériel **Wi-Fi** existant.

Les risques existent pour casser WPA. Des techniques ont été découvertes et permettent de casser WPA. Un autre défaut, comme la nécessité de mettre en place une PKI et de distribuer des certificats. C'est un mécanisme assez lourd à mettre en place malgré le gain non négligeable de sécurité d'une telle procédure. Ces défauts sont loin d'être rédhibitoires.

III.9 – CONCLUSION

Depuis la création de **Wi-Fi**, des groupes de travail se forment pour pallier aux failles de sécurité de cette norme. De ce fait l'apparition de nouvelles procédures et mécanismes fut nécessaire.

Les normes présentées dans ce chapitre permettent de donner une vue claire sur l'évolution de la sécurité qui dépend des attaques recensées.

Cependant, il faudrait faire des études au préalable, dimensionner le réseau, connaitre ses failles de sécurité et proposer une solution propre à lui.

Il est très important, lors de la conception du réseau de se fixer des objectifs de sécurité, connaitre les vulnérabilités du réseau et superviser ses failles de sécurité.

Toutefois, il est indispensable d'avoir une idée globale et sensibiliser les utilisateurs de ce type d'attaques qui peuvent induire de graves conséquences.

Le chapitre suivant fera l'objet de l'étude du réseau sans fil de l'université de Tlemcen pour proposer une solution adéquate de sécurité.

4

Une politique de sécurité pour le réseau de l'université de Tlemcen

Le but principal de notre projet est de faire une étude sur la sécurité du réseau sans fil de l'université de Tlemcen et de proposer une solution souple à mettre en œuvre.

L'université Abou Bakr Belkaid est en pleine évolution Elle est amenée à devenir parmi les grands pôles universitaires Algérien. L'étendu de ce pôle ne cesse de s'élargir. Chaque année de nouveaux sites sont construits, certains d'entre eux sont éphémères, et d'autres sont difficiles à joindre. Pour cela les modifications de l'architecture du réseau et l'installation des nouveaux sites deviennent difficiles, ce qui nous mène à aller vers le sans fil, pour sa facilité de déploiement ainsi que la possibilité de se déplacer facilement sans à se soucier de se déconnecter.

Néanmoins, le manque de sécurité du réseau est un handicap persistant qui laisse les administrateurs sceptiques face à l'utilisation du réseau sans fil pour faire transiter des informations délicates.

Au cours de ce chapitre, nous allons faire une description du réseau de l'université de Tlemcen, faire l'analyse des risques encourus par son système d'information et proposer quelques solutions pour remédier à ces failles.

IV.1 – LES OBJECTIFS DE LA POLITIQUE DE SÉCURITÉ

La définition d'une politique de sécurité est une démarche de toute université visant à protéger son personnel et ses biens d'éventuels incidents de sécurité dommageables pour son activité **[40]**.

La définition d'une politique de sécurité réseau fait intégralement partie de la démarche sécuritaire de l'université. Elle s'étend à de nombreux domaines, dont les suivants :

- Audit des éléments physiques, techniques et logiques constituant le système d'information de l'université ;
- Sensibilisation des responsables des différents secteurs de l'université aux incidents de sécurité et aux risques associés ;
- Formation du personnel utilisant les moyens informatiques du système informatique ;
- Ingénierie et maîtrise d'œuvre des projets incluant les contraintes de sécurité dés la phase de conception ;
- Classification des informations de l'université selon différents niveaux de confidentialité et de Criticité **[39]**.

La définition de la politique de sécurité se base sur l'audit du réseau, qui nous permet par la suite de fixer les besoins en sécurité et les mesures à prendre.

L'audit consiste à faire un travail de prospection et d'analyse de l'architecture du réseau, des services disponibles, de leurs utilisateurs et du trafic que véhicule ce réseau. Cette phase nous permettra de répondre aux questions relatives au réseau :

- De quoi est-il constitué ?
- Á quoi est-il utilisé ?
- Par qui est-il utilisé ?
- Comment est-il géré ?
- Que véhicule-t-il ?

La réponse à ces questions nous permettra de dresser un état du réseau du point de vue sécurité et de définir son degré de sécurité.

IV.2 – RESSOURCES INFORMATIQUES DE L'UNIVERSITÉ DE TLEMCEN

IV.2.1 – Infrastructure et architecture du réseau

L'université de Tlemcen possède un réseau essentiellement filaire composés de plus de 1800 prises informatiques aux services des étudiants, enseignants, chercheurs et administrateurs et donc un nombre important d'équipements réseaux en commutateurs et concentrateurs **[18].**

Le but est de pouvoir interconnecter toutes les administrations, laboratoires de recherche, salles de travaux pratiques, bibliothèques, espaces Internet, bureaux enseignants. Ce réseau sert à la connexion à Internet et sert aussi à la mise en place de l'Intranet de l'université.

L'université de Tlemcen dispose aussi d'un réseau sans fil **Wi-Fi** reliant ses sites distants pour lesquels la liaison filaire pose problème ou pour des sites éphémères.

Les deux pôles Imama et Chetouane sont les pôles les plus importants de l'université de Tlemcen regroupant les plus grands nombres de prises informatiques. De ce fait les liaisons sont dupliquées, une par fibres optiques et l'autre par faisceaux hertziens en cas où la liaison filaire serait en panne (voir **FIG** IV.1).

Les pôles Kiffane et le Rectorat sont des sites éphémères et n'exigent pas un nombre important de prises informatiques, leurs trafic n'est pas lourd d'où le choix de mettre des liaisons sans fil pour faciliter l'installation du réseau.

Les réseaux Wi-Fi sont aussi utilisés dans les laboratoires de recherche, soit pour relier des stations entre elles (mode ad hoc) ou pour partager la connexion Internet (mode infrastructure).

La participation des chercheurs aux séminaires et aux journées spéciales organisés au sein de l'université nécessite des salles de conférences équipées d'une infrastructure sans fil pour connecter tous les invités. Ces réseaux là doivent être sécurisés.

La plupart de ces réseaux sont ouverts, aucune mesure de sécurité n'est déployée. Parfois la clé WEP existe mais n'est pas suffisante pour protéger les accès illicites et les attaques des hackers. .

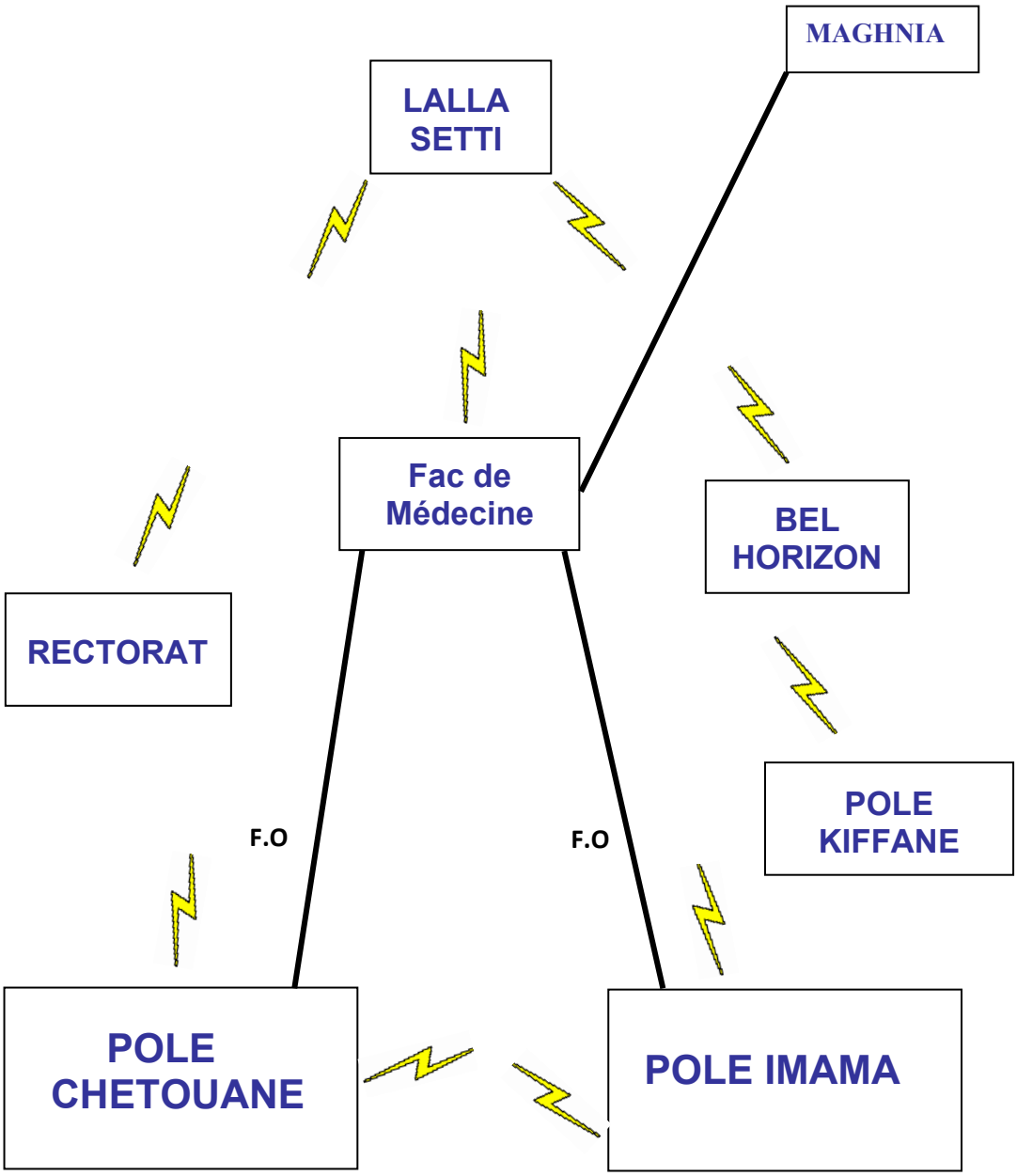


FIG IV.1 **–** *Architecture générale du réseau Informatique de l'université de Tlemcen.*

IV.3 - LES SERVICES

Le réseau informatique de l'université est destiné à plusieurs applications et services. Dans cette partie, nous allons présenter ces services offerts eten mettant l'accent sur leurs vulnérabilités.

IV.3.1 – Accès Internet

L'accès à Internet représente l'un des services importants du réseau. Il constitue 80% de l'exploitation du réseau. La connexion Internet se fait par deux liaisons principales, la première passe par le pôle Tlemcen Centre (Ex caserne Miloud) qui est connectée à Internet par une fibre optique d'un

débit de 8 Mb/s fournit par CERIST, la deuxième connexion utilise une station Vsat située à Chetouane.

Cela pourrait paraître inutile de sécuriser les connexions au réseau Internet, du fait que les contenus qui transitent dans ces réseaux ne sont pas très critiques Mais en fait, des failles de sécurité peuvent compromettre la disponibilité de ce service. Des attaques pourraient rendre les équipements réseaux tels que les routeurs, les serveurs proxy non opérationnels en les submergeant de requêtes (floading). Elles peuvent même être la cause de la détérioration de ces équipements et des postes clients.

En plus de cela, ce service est onéreux pour l'université, donc il serait dommage de donner l'accès à des personnes étrangères à l'institution, pour une utilisation irrationnelle de la bande passante privant ainsi les étudiants et chercheurs de cette ressource

Plus grave, l'utilisation de la connexion Internet d'une façon illégale peut entrainer l'université dans des poursuites juridiques dans le cas où le réseau est utilisé comme passerelle afin d'atteindre et d'attaquer d'autres réseaux extérieurs.

Ces défaillances peuvent mettre à mal la bonne réputation de l'université.

IV.3.2 – Messagerie électronique

Les administrateurs du système d'information de l'université de Tlemcen ont mis à la disposition des utilisateurs réseau un service permettant l'échange de messages et de tout document informatisés. Les messages et documents électroniques nécessitent un besoin fort en sécurité. C'est l'intégrité des données qui est exigée dans ce cas. Une modification du contenu des messages ou leur perte peut avoir des conséquences fâcheuses pour les utilisateurs.

A un degré moindre de gravité, le service peut être rendu indisponible par une attaque de type DoS.

IV.3.3 – Serveur DNS

C'est une machine appelée serveur de nom de domaine permettant d'établir la correspondance entre le nom de domaine et l'adresse IP des machines du réseau de l'université. Cette machine est située au niveau du pôle Tlemcen centre. Les besoins en sécurité pour ce service sont :

- en premier lieu, l'intégrité: une modification des contenus de ce serveurs peut être à l'origine d'attaques
- en second lieu et à un degré moindre la disponibilité: l'arrêt du service rend inaccessible les serveurs du domaine

IV.3.4 – Serveur Web de l'Université et Hébergement des pages Web personnelles

L'université dispose d'un serveur Web pour afficher les informations des activités de l'université.

De même chaque laboratoire de recherche, enseignant et même groupe d'étudiants a la possibilité de développer son propre site Web et de l'héberger sur le serveur Web de l'université.

L'intégrité est l'un des critères les plus importants pour ce service, du fait que tous les enseignants responsables de laboratoires de recherche et les étudiants chercheurs hébergent leurs pages web dans ce serveur. Une modification ou vol de droit de publications nuirait à ce serveur. Puis la disponibilité est recommandée pour répondre à toutes les demandes.

IV.3.5 – E-Learning

Cela repose sur la mise à disposition de contenus pédagogiques via le réseau de type Internet ou Intranet permettant la formation via un PC.

L'authentification est recommandée dans ce cas, puisque n'importe quel étudiant aguerri pourra s'introduire dans le réseau, sniffer les noms et mots de passes des utilisateurs, profiter des cours, occuper la bande passante, d'une façon irrationnelle. Aussi la disponibilité et l'intégrité de ce serveur doit être assurée

IV.3.6 – Inscription

L'université de Tlemcen connaît une croissance remarquable. Chaque année plus de 5000 nouveaux étudiants sont inscrits au niveau de l'université. Pour faciliter cette opération, plus de 60 PC sont mis en réseau chaque année au niveau de la bibliothèque centrale. Les étudiants peuvent effectuer leurs inscriptions et se renseigner sur les différentes filières d'une façon satisfaisante.

Les inscriptions, les acceptations et les recours ne doivent surtout pas être modifiés. Nous devons veiller à ce que cette opération s'effectue en toute confidentialité. Le besoin exigé en termes de sécurité est l'intégrité beaucoup plus que la disponibilité.

IV.3.7 – Documentations

L'université de Tlemcen a plus de 520000 ouvrages. Ils sont classés par spécialités. La recherche bibliographique peut se faire en local au niveau des différentes bibliothèques ou sur toutes les bibliothèques à travers une interface Web.

Ce qui importe dans ce cas là, ce sont la disponibilité, et l'intégrité des serveurs de bases de données qui doivent être assurées

IV.3.8 – Capacité de transmission

La centralisation de serveurs, le déploiement de nouvelles applications telles que les visioconférences, les besoins de sauvegarde et d'archivage exprimés par plusieurs départements, le développement de l'E-Learning qui poussent de plus en plus de scientifiques à manipuler des volumes gigantesques de données mais aussi les nouvelles formes de calcul scientifique vont nécessiter

de plus grandes capacités de transmission. Ces nouvelles applications doivent pouvoir être utilisées et déployées de la même façon sur les sites de l'Université.

IV.4 – GESTION DU RÉSEAU DE L'UNIVERSITÉ

Le centre des ressources informatiques (CRI) de l'université assure la gestion des services informatiques basés sur un réseau informatique et sur des technologies fiables et modernes. Le CRI participe, en collaboration avec les facultés et instituts, ainsi qu'avec des institutions voisines, au développement d'une informatique universitaire moderne au service des usagers.

La gestion d'un réseau informatique universitaire est une tâche ardue. La différence entre la gestion d'un réseau d'entreprise et un réseau universitaire est que dans le cas d'un réseau d'entreprise, l'architecture du réseau est plus ou moins stable, de plus la gestion est centralisée. Par contre au sein du réseau informatique universitaire, les utilisateurs sont libres de configurer leurs postes et d'installer toute application qui les intéresse sans souvent se préoccuper des considérations de sécurité.

De plus, vu le nombre de départements des différents sites, de laboratoires de recherche, d'étudiants, l'utilisation du réseau Internet est vulnérable. L'ajout d'utilisateurs à partir d'une prise informatique en installant un AP pour faire profiter plus de 8 machines de la connexion Internet. Le problème existant est que rares sont les fois où les prises informatiques sont associées à des utilisateurs fixes qu'ils soient enseignants ou chercheurs. La gestion devient alors difficile et le manque de confiance s'installe.

Les administrateurs des départements sont alors sceptiques face à l'utilisation du réseau sans fil pour faire transiter des informations critiques surtout lorsque nous savons que certains sites sont reliés par des liaisons **Wi-Fi** non sécurisées.

IV.5 - ANALYSE

Selon le travail fait par Mr A.Benazza en 2006 concernant « l'audit de sécurité du réseau de l'université » **[18]**, nous pouvons tirer profit de ce travail pour estimer le niveau de sécurité de notre réseau. Il est possible de faire l'audit au niveau du serveur du réseau grâce à des outils tels que « Ethereal », « tcpdump » et « Airsnort ». Les statistiques recensées montrent que le réseau est utilisé en grande partie pour les applications web (page html), ce qui suit est soit des datagrammes UDP ou des segments TCP.

Le résultat de ce travail était de dévoiler les failles de sécurité sur les deux plans architectures et serveurs. Il a aussi proposé des solutions d'architectures sécurisées pour notre système. Le niveau de sécurité des laboratoires de recherche est très bas, puisque le WEP est utilisé seul. Ce mécanisme de sécurité est défaillant plusieurs articles l'ont prouvé **[15]**. D'ailleurs il n'est plus utilisé tout seul, il est couplé à d'autres mécanismes d'authentification robustes. La longueur de la clé joue un rôle

important, mais, elle est crackable. Dans le cadre d'un travail de fin d'études, la clé WEP a été ctackée en 20 minutes, mais la mise en œuvre de la plate forme de crackage n'était pas facile. Il a fallu un pc d'une capacité RAM (512 Mo), une bonne maîtrise de linux et des logiciels de craquage de clé WEP. D'où l'accès au réseau sans fil. Cela pourrait causer un dysfonctionnement du réseau, une utilisation illicite de quelques sites et une utilisation irrationnelle de la bande passante **Wi-Fi**.

IV.6 – PROPOSITION D'UN RÉSEAU SÉCURISÉ POUR LE RÉSEAU DE L'UNIVERSITÉ DE TLEMCEN

La mise en place d'un réseau sécurisé nécessite des moyens matériels conséquents gérés par un personnel qualifié et une stratégie de sécurité adéquate.

La formation du personnel chargé de la maintenance réseau dans ce contexte, a pour objectif une bonne maîtrise de l'architecture réseau, des équipements destinés pour chaque service.

D'autre part, la sensibilisation des utilisateurs du réseau sans fil est sans doute très importante dans la gestion du réseau. L'installation de certaines applications dans des machines individuelles peut nuire au bon fonctionnement du réseau et représenter une menace d'attaque interne contre les serveurs de l'université.

Un recensement des menaces et des attaques dans le système d'information doit être effectué et une étude doit être faite pour proposer les solutions possibles. Les tentatives de sécurisation du réseau auparavant expérimentée peuvent être une bonne source pour cette étude.

IV.6.1 – Expérience de sécurisation d'un réseau au sein d'un laboratoire de recherche de l'université

Le laboratoire STIC dispose d'un réseau local relié au réseau de l'université et à Internet.
Comme chaque laboratoire, nous bénéficions de 3 prises Internet (informatique), dont une d'entre elles est partagée entre dix utilisateurs à travers un AP 7100 (DLink).

Cet AP ne supporte pas le protocole 802.1x. Un mécanisme de sécurité à base de clé WEP statique a été mise en place. Comme cité dans le chapitre1, cette clé a été crackée en 20 mn, dans le cadre d'un projet de fin d'études d'ingénieurs en Informatique. L'utilisation d'une clé WEP dynamique n'aurait pas donné de meilleurs résultats.

Ce niveau de sécurisation aurait pu être amélioré en ne transmettant pas l'ESSID et en réduisant la puissance du signal du point d'accès juste aux limites du laboratoire. Mais ces mesures restent très peu fiables, vu que l'ESSID peut être facilement découvert et qu'il existe des antennes de fort gain qui peuvent capter le signal même à de longues distances.

Cet exemple de tentative de sécurisation de réseau basée sur des techniques non éprouvées, montre l'inefficacité d'une telle approche. Nous pensons qu'après l'analyse des besoins en sécurité, il y a lieu de choisir les mécanismes de sécurité les plus reconnus comme efficaces et de les tester pour en mesurer leur fiabilité et leur conformité à nos besoins. C'est l'approche que nous avons suivie.

IV.6.2 - Sécurité des réseaux Wi-Fi de l'université

Les mesures de sécurité qui seront prises dans une première phase seront choisies en fonction du matériel existant. Elles seront hiérarchiques. Ceci est possible en sécurisant les points d'accès disponibles dans les bibliothèques et des salles de recherche, ainsi que les points d'accès des liaisons point à point. Elles seront basées sur un mécanisme d'authentification des utilisateurs et de chiffrement des données transmises.

Nous avons installé un réseau type que nous avons installé dans notre laboratoire en utilisant les mêmes équipements que ceux utilisés dans le réseau de l'université. Nous avons testé sur ce réseau les mécanismes d'authentification EAP-TLS et EAP-TTLS. Nous avons constaté qu'ils garantissent une forte authentification des machines qui se trouvent dans le réseau, de part les certificats générés par le serveur. L'authentification se fait dans un tunnel protégé, de plus les clés partagées entre le serveur et le client permettent de chiffrer la phase d'authentification. Ceci ne laisse aucune chance à un intrus de se faire passer pour quelqu'un d'autre et de causer par exemple un déni de service.

La méthode EAP-TLS nécessite un certificat serveur à installer coté client. Elle est souple à mettre en œuvre (après une longue maitrise). Néanmoins, l'administrateur réseau doit trouver un compromis sur la durée de validité des certificats. Une durée trop courtes obligerait les clients à ressaisir les certificats fréquemment et peut provoquer un rejet de ce mécanisme. Une durée trop longue augmenterait le risque qu'un intrus puisse s'introduire sur le réseau.

La méthode EAP-TTLS, elle, ne nécessite pas l'installation du certificat serveur sur le poste client. Un logiciel client doit être installé sur les postes clients pour garantir la confidentialité du login/password transmis sur le réseau. Elle est plus pratique à utiliser, mais beaucoup plus difficile à installer, du fait de l'incompatibilité entre les applications clientes et serveur, que nous avons constatée.

Les mécanismes de chiffrement qui accompagnent ces méthodes d'authentifications sont variés. Le plus simple et celui qui est disponible sur les équipements de notre réseau est le mécanisme de chiffrement par clé WEP. Malheureusement, comme nous l'avons noté, ce mécanisme est peu sûr.

Dans une seconde phase, nous préconisons de prévoir l'achat d'équipements Wi-Fi plus sophistiqués supportant des mécanismes de chiffrement plus puissants, tels que WPA ou WPS. D'autres parts,

Ces mécanismes seront couplés par la suite à des mécanismes et protocoles d'authentification plus robustes tels que EAP-SIM. Ce mécanisme très prometteur peut tirer profit du formidable essor de la téléphonie mobile. Les utilisateurs pourront être authentifiés plus sûrement grâce à la carte SIM disponible sur leur téléphone mobile.

IV.7 – CONCLUSION

Les technologies sans fil sont devenues très répandues. Elles couvrent une grande partie des réseaux des télécommunications. L'évolution est vers les réseaux **Wi-Fi.** Leur facilité de déploiement te de connexion sont séduisante. C'est une solution efficace pour relier les sites de l'université néanmoins le manque de sécurité des points d'accès effrayent les utilisateurs. Pour garantir une sécurité acceptable, il faudrait former des équipes d'ingénieurs et de chercheurs pour les spécialiser dans le domaine de la sécurité. La gestion des comptes utilisateurs est une tâche compliquée. Dorénavant, il faudrait prévoir des équipements Wi-Fi au sein desquels sont implémentés des protocoles de sécurité conformes aux nouvelles normes de sécurité.

La proposition de sécurité du réseau sans fil de l'université a été inspirée de quelques universités qui ont opté pour ces mécanismes de sécurité.

Par ce mécanisme de chiffrement et d'authentification, nous souhaitons contribuer à la réalisation d'un réseau **Wi-Fi** universitaire dans lequel règne une sécurité plus ou moins satisfaisante.

5

Mise en œuvre de mécanismes de sécurité pour le réseau sans fil de l'université

Comme annoncé dans le chapitre précédent, notre proposition de sécurisation du réseau sans-fil de l'université de Tlemcen est basée sur les protocoles d'authentification EAP-TLS et EAP-TTLS.

Nous détaillons, dans ce chapitre, leur mise en oeuvre au sein du laboratoire STIC. En plus de l'installation physique des équipements, ceci nécessite la mise en place d'un serveur d'authentification, tel que Radius et d'un mécanisme de génération de certificats. Nous avons opté pour l'installation de ces outils dans un environnement Unix, d'une part parce qu'ils sont en Open Source, et d'autre part, ils sont moins vulnérables aux attaques.

Le réseau sans fil de l'université est un réseau opérationnel. Nous ne pouvions pas utiliser le réseau existant pour ne pas perturber son fonctionnement. Nous avons crée une portion sans fil dans le laboratoire STIC en utilisant le même matériel que ce soit le point d'accès, les antennes **Wi-Fi** ou les serveurs d'authentification (Radius).

V.1 – MISE EN ŒUVRE DE LA PLATEFORME D'ESSAI

La réalisation d'une telle infrastructure d'essai nécessite plusieurs PC munis d'une carte PCIMCIA, de points d'accès et d'un serveur. Les points d'accès sont des Cisco Aironet350, les cartes Wi-Fi utilisées sont des Dlink DWL-AG530.

Les systèmes d'exploitation utilisés :

- Windows XP. Pour les postes clients
- Linux Mandrak 10.0 pour le serveur

Les logiciels :

- Une application cliente SecureW2_312
- Les librairies Openssl-1.9.7 g disponible sur www.openssl.org
- Une application serveur d'authentification : freeradius-1.0.1 et freeradius-Snapshot20042206 disponible sur : www.freeradius.org

Notre plateforme d'essai présente l'architecture exposée sur la figure IV.1.

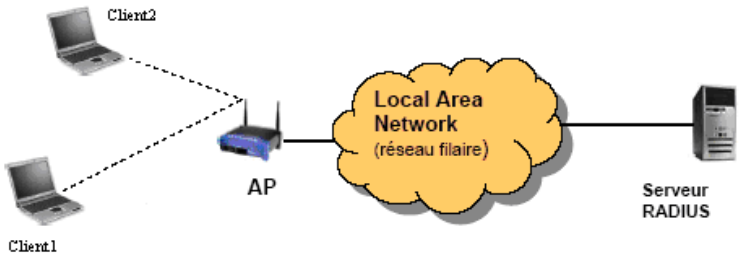


FIG V.1– *Plateforme d'essai.*

V.1.1 – Mise en œuvre de EAP-TLS

La mise en œuvre de cette méthode d'authentification nécessite le passage par des étapes de configuration. Les packages nécessaires pour la configuration du serveur sont disponibles et gratuits.

Néanmoins il faut assurer la compatibilité des packages avec les librairies utilisées. Après plusieurs essais nous avons pu parvenir à une configuration correcte.

Une étape importante de la configuration d'EAP-TLS est la génération des certificats. Ceci est nécessaire du fait que ce protocole utilise un tunnel chiffré pour la phase d'authentification.

Trois entités doivent être configurées.

- Le serveur d'authentification Radius avec OpenSSL pour la génération des certificats.
- Les clients
- Le point d'accès.

V.1.1.1 – Configuration du serveur d'authentification

Le détail des commandes est fourni en Annexe C.

V.1.1.1.1 – Installation d'OpenSSL

Les librairies OpenSSL sont incluses dans toutes les versions Linux. Ce produit est une suite logicielle permettant la manipulation des certificats X509. L'installation et la configuration se fait dans un répertoire bien spécifique pour pouvoir faire appel aux certificats.

Si la licence d'Openssl n'est pas compatible avec la licence de freeradius, les modules EAP/TLS (rlm_eap_tls.so) et EAP/TTLS (rlm_eap_ttls.so) ne sont pas compilés par défaut dans le logiciel freeradius.

La configuration d'OpenSSL se base essentiellement sur la configuration du fichier Opessl.cnf. Ce fichier contient les différentes informations que peut contenir le fichier de génération, comme le nom de l'entreprise, le pays, la ville, l'adresse mail et le nom du propriétaire du certificat.

V.1.1.1.2 – Génération des certificats

Les mécanismes à base de certificats supposent qu'une confiance s'installe entre les utilisateurs et l'entité qui produit les clés privées. Un organisme offrant un service de gestion de clés publique est une autorité de certification appelée tiers de confiance. Cet organisme émet des certificats au sujet de clés permettant à un groupe d'utilisateurs de les utiliser avec confiance. Pour l'université, une personne doit être désignée pour jouer ce rôle d'autorité de certification. Elle générera les certificats en présence des clients. L'idée que le certificat puisse être régénéré par une autre personne n'est pas à écarter, mais les informations confidentielles sont tenues uniquement par l'autorité de certification.

Il faudrait générer trois certificats :

- root pour l'autorité de certification,
- serveur pour le serveur Radius

- et client.

Pour cela, nous avons besoin des fichiers sources CA.root, CA.svr, CA.clt et xpextensions.

Le rôle du CA.root est la génération du certificat de l'autorité de certification. C'est un certificat auto-signé. Une copie de ce certificat nommé root.der est installée sur le poste de l'utilisateur.

Le script CA.srv sert à la génération du certificat du serveur Radius. Ce certificat est stocké sur la machine où tourne le serveur Radius et permet au client d'authentifier le serveur.

Le script CA.clt sert à générer les certificats pour les clients : client.p12.

Pour des raisons de sécurité, les certificats root.der et client.p12 sont fournis à l'utilisateur par une méthode sûre : une clé USB ou une disquette serait l'idéale.

Le fichier xpextensions est très important, il contient les OID pour la génération des certificats.

V.1.1.1.3 – Installation de freeradius

Les certificats par défaut de freeradius sont remplacés par une copie de notre certificat root et serveur.

La configuration de freeradius se base sur 4 fichiers essentiels se trouvant dans /etc/raddb. Ces fichiers sont :

- eap.conf : pour la configuration de EAP et des certificats.
- Clients.conf : pour la configuration des NAS (bornes wifi) autorisés à contacter le Radius.
- Users : pour la configuration des utilisateurs autorisés.
- Radiusd.conf : c'est le fichier principal de configuration de freeradius dans lequel tous les autres fichiers seront appelés.

V.1.1.3 – Configuration du Point d'accès

La configuration du point d'accès se trouve dans **(Annexe D)**.

V.1.1.4 – Configuration du client (sous Windows XP)

La configuration de l'application cliente ne présente pas de difficultés majeures. Elle nécessite juste l'installation des certificats de l'autorité root.der, des clients sofia.p12 et wifi.p12 et la configuration du réseau sans fil.

V.1.1.5 – Notre point de vue sur la mise en œuvre du protocole EAP-TLS

Ce mécanisme d'authentification est souple à mettre en œuvre, il faut juste avoir la bonne documentation pour suivre des étapes qui nous permettent un bon fonctionnement du serveur radius. L'installation de ce mécanisme d'authentification ne pose pas de problèmes au sein d'un réseau sans fil, il est fiable et robuste.

Les certificats installés sur le poste client contiennent tous les renseignements le concernant. De ce fait une connexion confiante est établie entre le client et le serveur.

La mise en œuvre de ce mécanisme est suggérée au sein des laboratoires de recherche et des petits réseaux d'entreprise.

L'architecture sans fil de l'université doit offrir des services sécurisés et confiants aux utilisateurs chercheurs et administrateurs. L'établissement d'une connexion sécurisée permet de faire étendre les réseaux sans fil à un périmètre plus large.

Comme perspective à ajouter à cette première partie, l'ajout d'une base de données Mysql dans le serveur radius, pour faciliter la gestion des clients.

Il est aussi possible de relier plusieurs points d'accès à un seul serveur Radius.

L'inconvénient majeur de ce protocole est, comme cité dans le chapitre 4, la nécessité de regénérer périodiquement les certificats.

V.1.2 – Mise en œuvre d'EAP-TTLS

La procédure de configuration est, sauf pour quelques points, semblable à celle vue précédemment.

V.1.2.1 – Configuration du Serveur d'authentification

Nous préservons l'installation et la configuration d'OpenSSL. La version du serveur freeradius, utilisée pour EAP-TLS n'ayant pas fonctionné pour EAP-TTLS, nous avons remplacé par une autre version `freeradius-snapshot-20042206`, conçue pour ce protocole.

V.1.2.2 – Configuration du poste client

L'application cliente Aegis, conseillée par le fabriquant de la carte DLink utilisée, nous a causé beaucoup de difficultés.

Télechargé du site www.mtghouse.com, ce logiciel libre permet l'authentification par la méthode EAP-TTLS. La version utilisée, AEGIS_Client_v2.1.0, nous a permis de visionner les phases d'authentification et d'association.

Malheureusement, malgré de nombreuses tentatives et modifications de la configuration, il n'a pas été possible de se faire authentifié auprès du serveur à l'aide de cette application cliente. Une inspection du fichier logs, nous a confirmé que la déconnexion était due au manque d'authentification.

```
  rlm_eap_tls: <<< TLS 1.0 Alert [length 0002], fatal certificate_unknown
TLS Alert read:fatal:certificate unknown
    TLS_accept:failed in SSLv3 read client certificate A
2467:error:14094416:SSL routines:SSL3_READ_BYTES:sslv3 alert certificate
unknown:s3_pkt.c:1052:SSL alert number 46
2467:error:140940E5:SSL routines:SSL3_READ_BYTES:ssl handshake
failure:s3_pkt.c:837:
rlm_eap_tls: SSL_read failed in a system call (-1), TLS session fails.
```

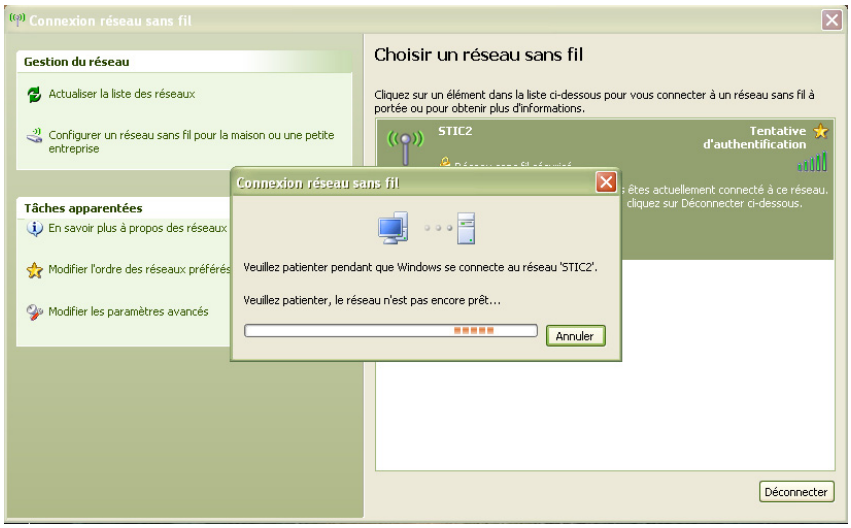
```
In SSL Handshake Phase
In SSL Accept mode
rlm_eap_tls: BIO_read failed in a system call (-1), TLS session fails.
  eaptls_process returned 13
  rlm_eap: Freeing handler
  modcall[authenticate]: module "eap" returns reject for request 9
modcall: group authenticate returns reject for request 9
auth: Failed to validate the user.
Login incorrect: [sofia/<no User-Password attribute>] (from client
aironet350 port 37 cli 001195bc9641)
Delaying request 9 for 1 seconds
Finished request 9
Going to the next request
```

Après une minutieuse prospection, nous en sommes arrivés à la conclusion que ce défaut d'authentification était du à une incompatibilité des longueurs de paquets entre l'application cliente et l'application Radius.

Nous avons résolu ce problème, qui nous a beaucoup freiné en utilisant une autre application logiciel cliente SecureW2_312. Très facile à installer sur le poste client, sa configuration se fait en utilisant les paramètres de connexion de Windows XP.

SecureW2_312.exe

Les certificats déjà installés sur la machine cliente, sont chargés dans le logiciel Secure.



Une fois les certificats chargés dans le client, les username/password correspondant au client sont introduits. Le test de connexion a été concluant.

V.1.2.3 - Notre point de vue sur la mise en œuvre du protocole EAP-TTLS

Cette méthode d'authentification est forte et souple en même temps. Elle permet une authentification des utilisateurs réseau.

Dans le cas où le Login ou le mot de passe de l'utilisateur ne sont pas corrects et ne correspondent pas à ceux donnés par l'administrateur lors de la configuration, l'authentification n'est pas effectuée et l'accès n'est pas possible. Le choix du login/password doit garantir un certain degré de robustesse.
Cette authentification est suggérée pour les points d'accès reliant des sites distants et délicats tels que Rectorat-caserne Miloud ou bien Imama-Chetouane, où nous avons vraiment besoin de garantir une authentification mutuelle lors d'un transfert de fichier et où les risques d'intrusion, sur une telle distance, sont élevés.

V.3 – CONCLUSION

Pour l'instant, les mécanismes d'authentification EAP-TLS et EAP-TTLS sont robustes. D'ailleurs, ils sont utilisés dans les plus grandes universités et dans les HotSpots. Ces serveurs d'authentification permettent d'augmenter le degré de sécurisation du réseau. Mais pour qu'ils soient efficaces, il faudrait le coupler à des mécanismes de chiffrement plus robustes que le WEP tel que WPA non disponible sur les points d'accès de l'université.

Conclusion générale

Durant ce travail, nous avons fait le point sur la sécurité des réseaux sans fil. Nous avons présenté les principales normes utilisées dans ce domaine. Il est clair que beaucoup de problèmes liés à la sécurité des réseaux sans fil restent ouverts.

Cette étude nous a permis de confirmer la vulnérabilité de ces réseaux vis-à-vis de la sécurité.

Leur attrait et les avantages qu'ils apportent dans le déploiement des réseaux font que les travaux sur la sécurité continuent et des solutions commencent à être apportées.

Nous en avons testé quelques unes en vue de leur utilisation dans le réseau **Wi-Fi** de l'université de Tlemcen. Pour mettre en œuvre ces solutions, nous avons étudié les besoins en sécurité du système d'information de l'université et proposé une politique de sécurité qu'il serait urgent de déployer.

Les tests des protocoles EAP-TLS et EAP-TTLS sur une portion de ce réseau sont concluants. Ils augmentent le degré de sécurité de ces connexions sans fil par les mécanismes d'authentification des utilisateurs.

Nous sommes conscients que ces mesures à prendre constituent une charge supplémentaire pour la gestion du réseau, mais elles sont indispensables pour la mise en place des services sécurisés. D'autant plus que la tendance actuelle poussée par les considérations économiques et de flexibilité poussent à une utilisation de plus de plus grande des connexions sans fil.

La normalisation dans ce domaine n'étant pas stable, il est évident qu'une politique de sécurité des réseaux sans fil peut coûter cher, vu que les équipements doivent être souvent mis à jour pour tenir compte des nouvelles spécifications. Ces considérations doivent être prises en compte au moment de la conception du réseau.

Notre travail constitue une contribution à la sensibilisation pour une amélioration de la sécurité du réseau sans fil de l'université et devra être continuée pour tenir compte des évolutions futures des normalisations.

Annexe A

Les formats des paquets PLCP

La couche PLCP écoute le support physique et indique à la couche MAC si le support est occupé ou non via un signal appelé CCA.

Dans la PLCP on trouve la sous-couche PLCP pour la FHSS et la sous-couche PLCP pour la DSSS.

A.1– Pour le cas du FHSS

La trame PLCP est de la forme suivante :

Préambule		En-tete			PSDU blanchi
sync	SFD	PLW	PSF	HEC	
80	16	12	4	16	Nombres variables de bits

Figure A.1 – *La trame FHSS-PLCP.*

Préambule

Il est dépendant de la couche physique et comprend :

- sync : c'est une séquence de 80 bits alternant 0 et 1, qui est utilisée par le circuit physique pour sélectionner l'antenne appropriée (si plusieurs sont utilisées), et pour corriger l'offset (le décalage) de fréquence et de synchronisation.

- SFD : Il consiste en la suite de 16 bits 0000 1100 1011 1101, utilisée pour définir le début de la trame.

En-tête PLCP

L'en-tête PLCP contient des informations logiques utilisées par la couche physique pour décoder la trame :

- PLW : Longueur de mot du PLCP_PDU : il représente le nombre d'octets (de 1 à 4095) que contient le paquet, ce qui est utile à la couche physique pour détecter correctement la fin du paquet.

- ***PSF :*** Fanion de signalisation PLCP :

Bit	Nom du paramètre	Valeurs du paramètre	Description
0	Réservé	Défaut = 0	Réservé
1 : 3	PLCP_BITRATE	b1 b2 b3 = Data Rate 0 0 0 = 1.0 Mbits/s 0 0 1 = 1.5 Mbits/s 0 1 0 = 2.0 Mbits/s 0 1 1 = 2.5 Mbits/s 1 0 0 = 3.0 Mbits/s 1 0 1 = 3.5 Mbits/s 1 1 0 = 4.0 Mbits/s 1 1 1 = 4.5 Mbits/s	Indique le debit du PSDU de 1 à 4.5 par pas de 0.5 Mbits/s

Tableau A.1 – *Fanion de signalisation PLCP.*

- ***HEC :*** Champ de contrôle d'erreur de l'en-tête : champ de détection d'erreur CRC 16 bits.

$G(x) = x^{16} + x^{12} + x^5 + 1.$

PSDU Blanchi

Le blanchisseur de données du PLCP utilises une trame de 127 bits de long pour le brouilleur suivit d'une suppression partielle pour randomiser les données.
La trame du brouilleur est générée par le polynôme : $x^7 + x^4 + 1$.

A.2 – Pour le cas du DSSS

Le PLCP a deux structures, un long et un court préambule. Tous les systèmes compatible **802.11**b doivent supporter le long préambule, le court préambule étant optionnel et servant essentiellement a améliorer l'efficacité du réseau dans la cas où des données *«* spéciales *»* sont transmises comme la voie sur IP ou encore le vidéo *streaming*.

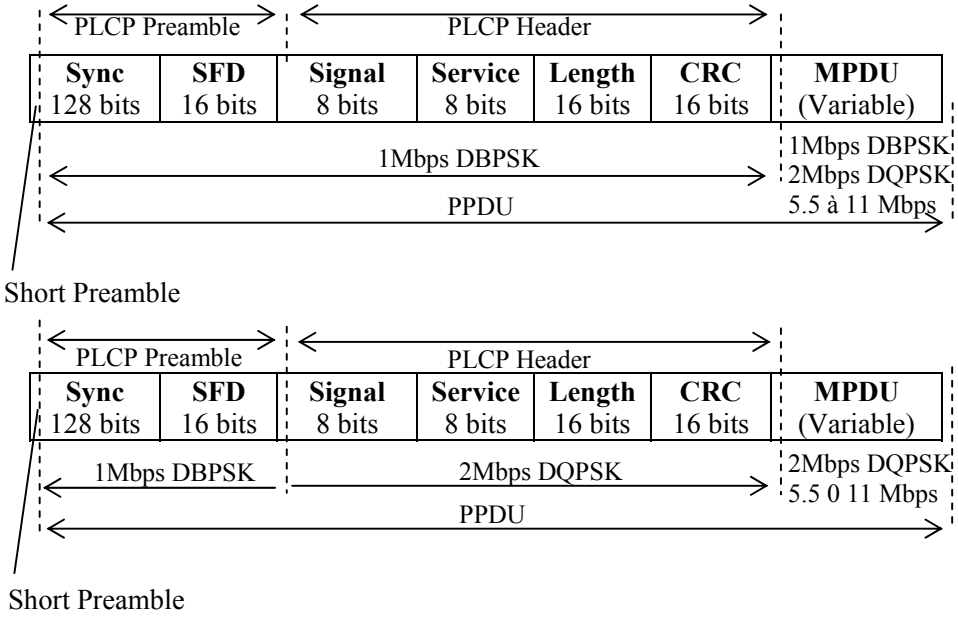
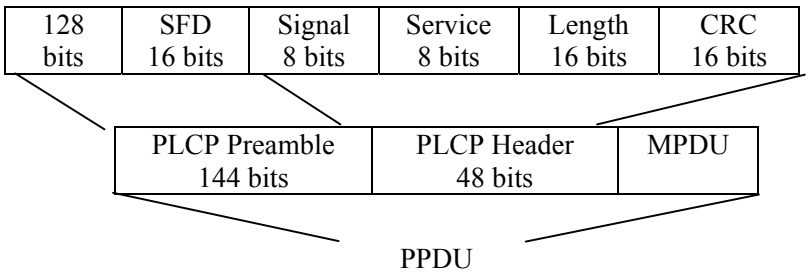


Figure A.2 – *Les deux types de trames DSSS-PLCP.*

La trame par défaut est celle avec un long préambule.



Le PLCP et le header sont toujours à 1 Mbps

Figure A.3 – *La trame DSSS-PLCP à un long préambule en vue éclatée.*

Le préambule est composé de la même manière que dans le cas de la FHSS.

- ***Signal :*** Ce champ indique à la couche physique la modulation qui doit être utilisée pour la transmission et la réception du MPDU.

- ***Service :*** Ce champ est réservé pour des utilisations futures. Il sera protégé par le CRC de fin de trame.

- ***Length :*** Ce champ contient un entier non-signé qui indique le nombre de microsecondes nécessaire pour transmettre le MPDU.

- ***CRC :*** Ce champ contient le complément à un du reste modulo 2 de la division des champs protégé par le polynôme générateur : $x^{16} + x^{12} + x^5 + 1$.

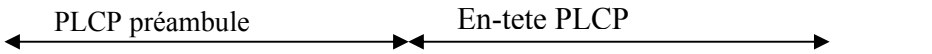
L'**IEEE 802.11** définit quatre types de couches physiques :

- FHSS, avec modulation DBPSK
- DSSS, avec modulation DBPSK ET DQPSK
- OFDM, avec modulation QAM
- Infrarouge, avec une modulation PPM

Les deux premières couches sont utilisées par les réseaux **802.11** et **802.11**b (bande de fréquences des 2.4 GHz), mais ne permettent pas d'obtenir des débits supérieurs à 11 Mbits/s, l'OFDM est utilisé pour les réseaux dont les débits doivent être supérieurs à 11 bits/s, c'est-à-dire pour les réseaux **802.11**a et **802.11**g. Enfin l'infrarouge est destiné à des réseaux à faible portée.

a) – FHSS

Cette technique permet de réduire les interférences générées par des transmissions simultanées de plusieurs stations. Mais, du fait de la faible largeur des sous canaux, limite le débit à 2 Mbits/s. Le format d'une trame PLCP-FHSS est le suivant :



80 bits	16 bits	12 bits	4 bits	16 bits	variable
Synchronisation	SFD	PLW	PSF	HEC	Payload

Figure A.4 – *Trame PLCP-FHSS.*

- Synchronisation : suite de 0 et de 1 mélangés, permettant au récepteur de sélectionner

l'antenne appropriée (s'il en possède plusieurs) et de corriger le décalage de fréquence et de synchronisation.

- SFD (Start Of Frame) : vaut 0000 1100 1011 1101, indique le début de la trame.

- PLW (PLSP_PDU Length Word): indique le débit de transmission de la PLSP_PDU (payload) ; il est toujours inférieur à 4096.

- PSF (PLCP Signaling Field) : indique le débit de transmission de la PLCP_PDU. Le premier bit de poids faible est réservé, les trois autres définissent le débit en une valeur variant de 1 à 5.5 Mbits/s, par pas de 0.5 Mbits/s (0 = 1 Mbits/s, 7 = 4.5 Mbits/s).

- HEC : on utilise un code cyclique CRC sur 16 bits pour vérifier l'intégrité de l'entête.

b) – DSSS

Les trames PLCP-DHSS possèdent deux formats : un format par défaut avec un préambule long de 128 bits, et un format avec préambule court de 56 bits. Le deuxième format est utilisé pour améliorer les performances du réseau dans le cas de données critiques telles que la voix, la VoIP ou le streaming vidéo. Le préambule court est également intéressant lorsque les trames doivent être fragmentées (on transmet moins de bits non utiles). Le format des trames est le suivant :

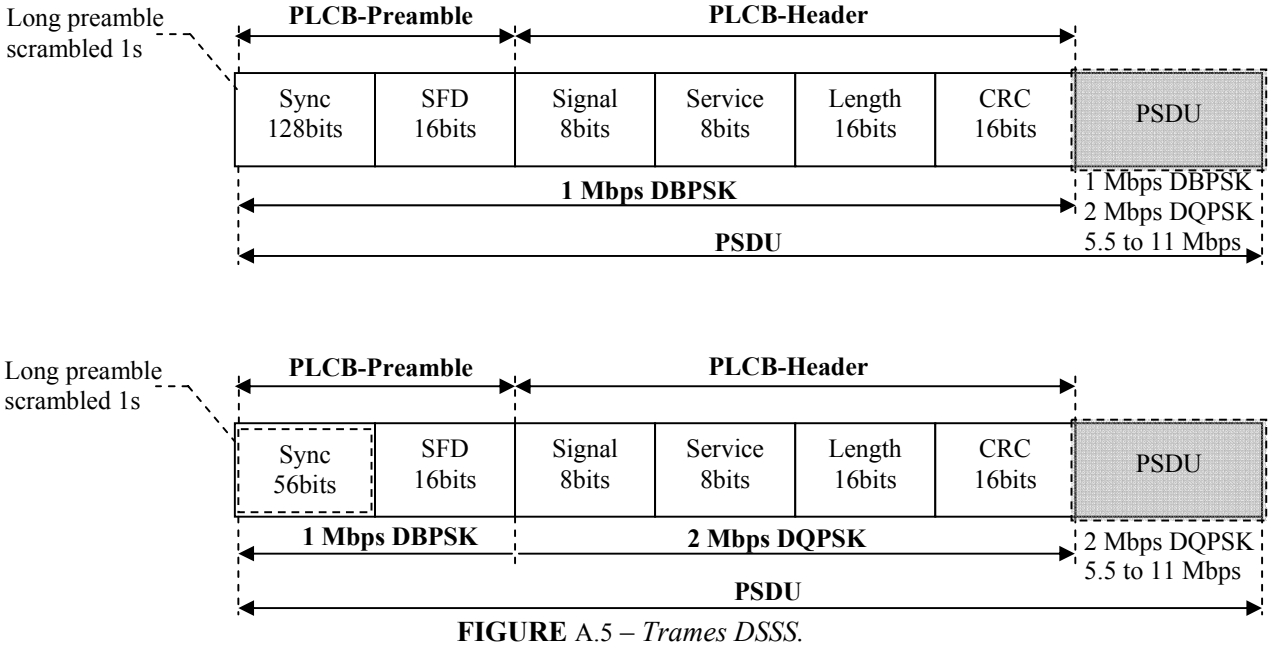


FIGURE A.5 – *Trames DSSS.*

- ***Signal :*** Indique la modulation à utiliser pour l'émission et la réception PSDU.

- ***Service :*** Réservé pour une utilisation future.
- ***Length :*** Indique le nombre de microsecondes nécessaires pour transmettre le PSDU.
- ***CRC :*** Somme de contrôle.

Annexe B

Les autres algorithmes de chiffrement

B.1 – Les algorithmes de chiffrement

Hormis les algorithmes classiques cités ci-dessus, on peut même citer les algorithmes à sens unique où la transformation en sens inverse est quasiment impossible à effectuer dans un laps de temps admissible. Le premier exemple de ce type d'algorithme est constitué par Diffie Hellman.

Principe :

Soit X un émetteur et Y un récepteur. Pour l'établissement d'une communication, ils se mettent d'accord sur 2 valeurs non secrètes, μ et p. L'émetteur X choisit une valeur a secrète et envoie à Y la valeur $x = \mu^b \bmod p$. si les valeur de μ et p sont assez grandes, il serait presque impossible de retrouver a ou b à partir de x ou y. X et Y décident que la clé commune est le produit ab et que le message chiffré est obtenu par $\mu^{ab} \bmod p$.

Le chiffrement permet que l'information ne soit lue que par le destinataire. Les techniques de chiffrement sont toutes à priori violables, mais il faudrait pour cela une machine de calcul puissante et d'une longue durée de vie.

B.2 – Les principaux algorithmes de chiffrement :

- **DES (Data Encryption Standard)**.1977, à clés symétriques, le plus connu des algorithmes de chiffrement. Pour chaque bloc de 64 bits, le DES produit un bloc chiffré de 64 bits. La clé de longueur de 56 bits, est complétée par un octet de détection d'erreur. De cette clé de 56 bits, on extrait de manière déterministe 16 sous clés de 48 bits chacune. À partir de là, la transformation s'effectue par des sommes modulo 2 du bloc à coder et de la sous clé correspondante. Cet algorithme est très utilisé dans les applications financières. Il est également utilisé dans un chaînage dit par bloc CBC (Cipher Block Chaining). Il existe de nombreuses variantes de l'algorithme DES, comme triple DES, ou 3DES, qui utilise trois niveaux de chiffrement, ce qui implique une clé de chiffrement sur 168 bits.
- **RC4, RC5 (Ron's Code #4, #5)**.1987, à clé symétrique, propriété de la société RSA Security Inc. Ils utilisent des clés de longueur variable pouvant atteindre 2048 bits et sont destinés à des applications fortement sécurisées. Ils demandent une forte puissance de calcul, qui ne pourrait être maintenue sur un flot continu à haut débit à des niveaux inférieurs de l'architecture.
- **IDEA**.1992, à clés symétriques, développé en Suisse et surtout pour la messagerie sécurisée PGP.
- **Blowfish**. 1993, à clés symétriques.
- **AES**. 2000, à clés symétriques.
- **RSA**. 1978, à clés asymétriques.
- **Diffie-Hellman**. 1996, à clés asymétriques.
- **El Gamal**. 1997, à clés asymétriques.

La mise en œuvre de ces techniques est difficile lorsque le débit d'une application est important. C'est pour cela que les techniques symétriques et asymétriques sont utilisées conjointement. Cependant, on recourt à des clés de session, qui ne sont valables que pour une communication déterminée. Les informations de la session sont codées grâce à une clé secrète permettant de réaliser un chiffrement avec beaucoup moins de puissance qu'une clé asymétrique. Uniquement la clé secrète est codée par un algorithme de chiffrement asymétrique pour être envoyée au destinataire **[3]**.

Annexe C

Les commandes de Configuration

C.1 – Mise en œuvre de EAP-TLS

C.1.1 – configuration du serveur d'authentification

1- Installation d'Openssl

La version utilisée est OpenSSL-0.9.7g, c'est une version V3. L'installation se fait en suivant les étapes suivantes :

- Décompression du package :

```
tar zxvf openssl-0.9.7g.tar.gz.
cd openssl-0.9.7g
```

- Configuration:

```
./config -prefix=/usr/local/openssl-certgen  shared
```

- Installation :

```
make
make install
```

2 – Génération des certificats

```
mkdir /root/certs
cd /root/certs
```

a – Génération des certificats root

Le lancement de la génération des certificats se fait par :

```
Cd /root/certs
./CA.root
```

En cas de problèmes de droit d'accès :

Chmod 777 –CA.root

b – Génération du certificat serveur

```
Cd /root/certs
./CA.svr –nom-serveur-
```

c – Génération du certificat client

```
Cd /root/certs
. /CA.clt sofia
```

2 – Installation du serveur freeradius

L'installation se fait en suivant les instructions suivantes :

```
cd /radius
tar zxvf freeradius-1.0.1.tar.gz
cd freeradius-1.0.1
```

La configuration et la compilation de freeradius se fait dans `/etc/raddb`.

```
./configure –with-openssl-includes=/usr/local/ssl/include/ -with-opennsl-libraries=/usr/local/ssl/lib/

./configure –sysconfdir=/etc/ --disable –shared
```

En suite :

```
make
make install
```

a – Installation des certificats serveur

```
Cd /etc/raddb/certs
Rm –rf *
Cp /root/certs/root.pem /etc/raddb/certs
Cp /root/certs/serveur.pem /etc/raddb/certs
```

Pour générer ces fichiers nous avons utilisé la fonction `date`. Pour le fichier `dh`, nous avons fait appel à la fonction `dh` (Diffie Hellman) openssl.

```
Date > random
Date > dh

Openssl dhparam –check –text -5 512 –outdh
```

Ceci nous permet la génération d'un fichier de 512 bits, de la forme :

```
Generating DH parameters, 512 bit long safe prime, generator 5
This is going to take a long time
.....+.+.....+.....+
.....+..+.....+.....+....+.....+.....+.....+...+..+.....+..+.....
.....+.....+.+.....+.....+....+.+.....
.....+.....+.....+.....+
.....+.....+.....+..+.....
.....+.....+.....+.....+....+.....+....+.....
.....+.....+.....+.....+....+.+.....+.....
.....+.....+.....+.....+.....+.....
...+.....+..... .....+.....
.....++*++*++*++*++*++*
DH parameters appear to be ok.
```

Pour le fichier random.c, on utilise le morceau de code qu'on enregistre dans /etc/raddb/certs/.

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

}
printf("Random : %s\n", buf);
}
```

La compilation se fait par :

```
Gcc random –c –o random –lcrypto
```

Test :

```
./random
```

Ça donne un truc du genre :

random

```
@þ#@ d@Pp*]býrÎG0jï^÷raåÅ°îc·éPÀåÌ#2 aåàíÇ#n&ØuuiJ@Ê
Tûÿ¿ø×@
```

b – Configuration de Freeradius

b.1 – Fichier eap.conf

Dans ce fichier, il faut spécifier le type EAP utilisé et modifier le chemin des certificats.

```
eap {
     default_eap_type = tls

     md5 {
                 }
```

```
     leap {
                  }
   }
tls {
                        private_key_password = whatever
                        private_key_file = ${raddbdir}/certs/serveur.pem

                        #  If Private key & Certificate are located in
                         # the same file, then private_key_file &
                        #  If Private key & Certificate are located in
                        # the same file, then private_key_file &
                        #  certificate_file must contain the same file
                        #  name.
                        certificate_file = ${raddbdir}/certs/serveur.pem

                        #  Trusted Root CA list
                        CA_file = ${raddbdir}/certs/root.pem

                        dh_file = ${raddbdir}/certs/dh
                        random_file = ${raddbdir}/certs/random
```

private_key_password est le mot de passe du certificat serveur (par défaut la valeur est whatever on peut le modifier en éditant le fichier CA.svr)

private_key_file et **certificate_file** est le chemin vers le certificat serveur.

CA_file est le chemin pour le certificat racine.

dh_file et **random_file** sont les chemins vers les fichiers aléatoires qu'on a générés précédemment.

check_cert_cn permet de vérifier que le nom d'utilisateur fournit par le client est le même que celui dans le certificat (utile car certain driver propose de choisir le nom d'utilisateur et le certificat ex : *Intel Proset* ou *Netgear Utility*).

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

b.2 – Fichier clients.conf

Dans ce fichier, on définit les APs autorisés à accéder au serveur Radius.

Pour communiquer en sécurité, le serveur Radius et l'AP partagent une clé secrète « shared secrete ».

```
client 176.64.0.237   {
        secret        = abc123
        shortname     = aironet350
        nastype       = Cisco
}
client 176.64.0.110   {
        secret       = abc123
        shortname    = wifi
```

b.3 – Fichier users

En bas de ce fichier, les utilisateurs autorisés seront ajoutés.

```
"wifi" Auth-Type := EAP, User-Password =="testing123"
"testing123" Auth-Type:= Local, User-Password =="testing123"
```

b.4 – Fichier radiusd.conf

C'est le fichier le plus long, il faut faire attention, en bref, c'est ce qu'il faut faire.

```
Prefix = /usr/local
exec_prefix = ${prefix}
sysconfdir = /etc

localstatedir = ${prefix}/var

sbindir = ${exec_prefix}/sbin
logdir = ${localstatedir}/log/radius
raddbdir = ${sysconfdir}/raddb
radacctdir = ${logdir}/radacct

confdir = ${raddbdir}
run_dir = ${localstatedir}/run/radiusd
log_file = ${logdir}/radius.log
libdir = ${exec_prefix}/lib

pidfile = ${run_dir}/radiusd.pid
...
user = nobody
group = nogroup

...
max_request_time = 30
...
max_requests = 1024

...
bind_address = *
...
port = 0
...
hostname_lookups = yes
...
log_stripped_names = yes
...
log_auth = yes
...
log_auth_badpass = yes
log_auth_goodpass = yes
...
modules {
..
$INCLUDE ${confdir}/eap.conf
}
authorize {
preprocess
auth_log
eap
files
}
...
authenticate {
unix
eap
}
```

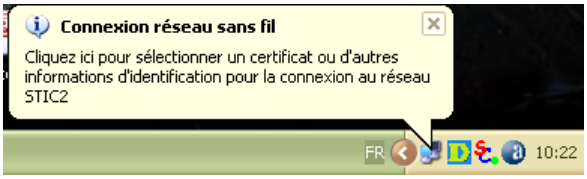
c – Lancement du daemon Freeradius

dans /etc/raddb

radiusd –X -A

C.1.2 – Configuration du poste client

Lorsqu'on dispose de plusieurs certificats sur une machine cliente, on reçoit ce message à fin de faire un choix sur le certificat client.



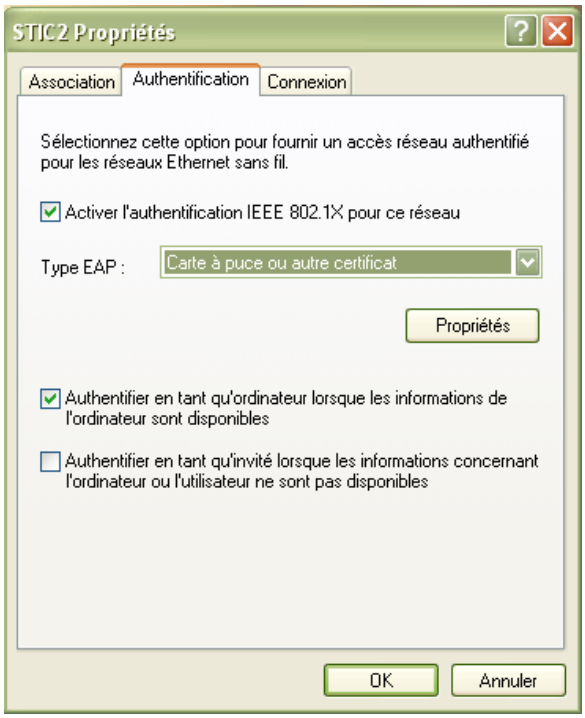
- **Configuration de la connexion sans fil**

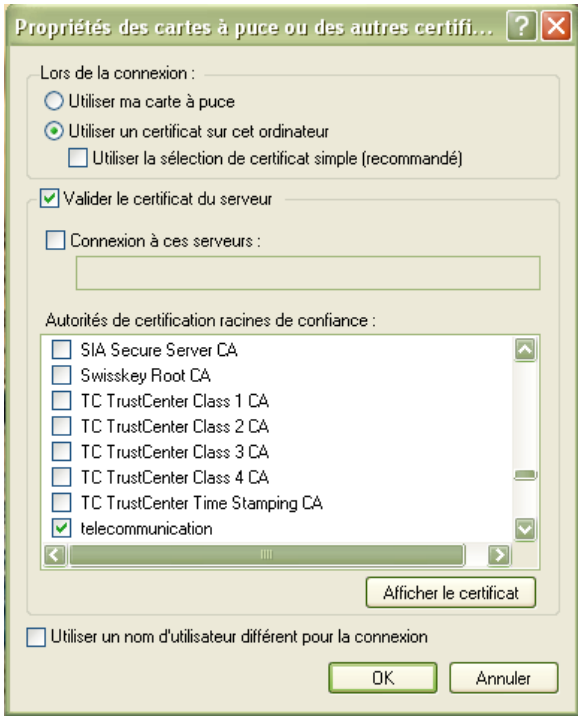
L'étape qui suit consiste à connecter ce client au réseau sans fil.

Le signal STIC2 est reçu, en cliquant sur STIC2 puis sur propriétés, nous obtenons :

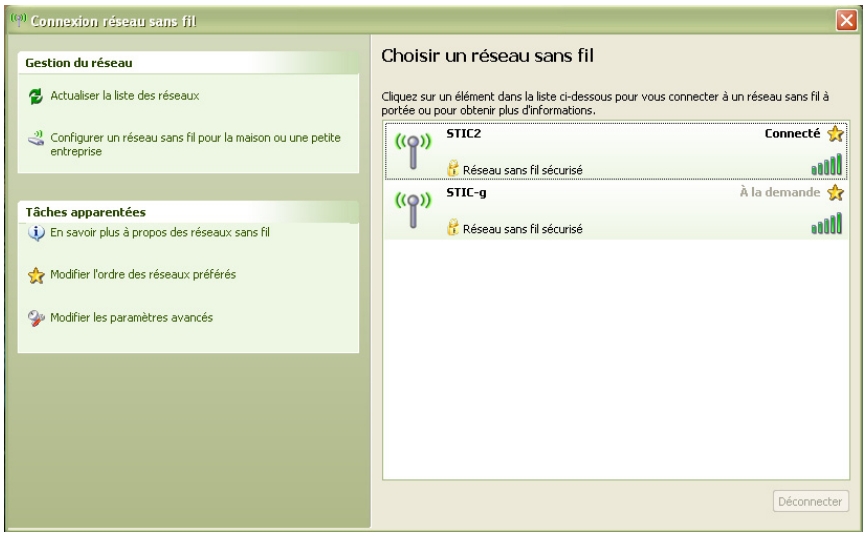
Dans la fenêtre propriété STIC2 le choix entre plusieurs types d'EAP se présente, dans notre cas il faut choisir « carte à puce ou autre certificat », c'est commun.

Dans propriétés, il est possible de choisir dans la liste des certificats le nom de notre certificat déjà installé.





En fin de configuration et d'installation des certificats, le client peut demander l'authentification, suite à une lecture d'adresse IP et des certificats l'accès au réseau devient possible.



Le plus important est :

```
Login OK: [sofia/<no User-Password attribute>] (from client aironet350 port
37 c
li 001195bc9641)
Sending Access-Accept of id 8 to 176.64.0.237:1032
        MS-MPPE-Recv-Key =
0xceef4a547648b7477b9ed32babc72c3e755bd62a5fb2c7c2dab
d56266261241e
        MS-MPPE-Send-Key =
0xbaff4e1bc20078bc61d19807f7d0108db700b4c61c518170662
abde023555ea6
        EAP-Message = 0x030d0004
        Message-Authenticator = 0x00000000000000000000000000000000
        User-Name = "sofia"
Finished request 4
```

C. 2 – Implémentation d'EAP-TTLS

C.2.1 – Configuration du Serveur d'authentification

Après avoir téléchargé le package l'installation se fait en suivant les étapes suivantes :

```
tar xjvf freeradius-snapshot-20042206.tar.tar
cd freeradius
```

Il faut penser à faire un

```
make clean
./configure –sysconfdir = /etc/
make
make install
```

Une fois l'installation terminée, il ne reste plus qu'à configurer les fichiers de freeradius se trouvant dans `/etc/raddb`.

La configuration est identique à celle de EAP-TLS, le fichier principal à modifier est `eap.conf`

Fichier eap.conf

Il faut respecter la configuration suivante :

```
eap {
     default_eap_type = tls

     md5 {
                 }

     leap {
                 }
   }
tls {
                          private_key_password = whatever
                          private_key_file = ${raddbdir}/certs/serveur.pem

                          certificate_file = ${raddbdir}/certs/serveur.pem

                          CA_file = ${raddbdir}/certs/root.pem

                          dh_file = ${raddbdir}/certs/dh
                          random_file = ${raddbdir}/certs/random


ttls {
                          default_eap_type = md5

                          copy_request_to_tunnel = yes

                          use_tunneled_reply = yes

                 }
```

Sauvegarder et quitter.

En ce qui concerne le protocole à utiliser dans le tunnel TTLS, les choix sont multiples : CHAP-V2, CHAP ou même PAP. Dans notre cas nous avons utilisé MD5.

Lancement du serveur :

Dans `/etc/raddb`

Faire `radiusd -X -A`

Juste pour s'assurer que le serveur fonctionne correctement. Dans certaines versions, les modules rlm_eap ne sont pas configurés lors de l'installation, donc ça pose problème lors du lancement du daemon radius. Il faut juste faire :

```
cd /src/modules/rlm_eap/types/rlm_eap_tls ou rlm_eap_ttls
                          ./configure
```

Le test local est obligatoire. Nous utilisons deux shell.

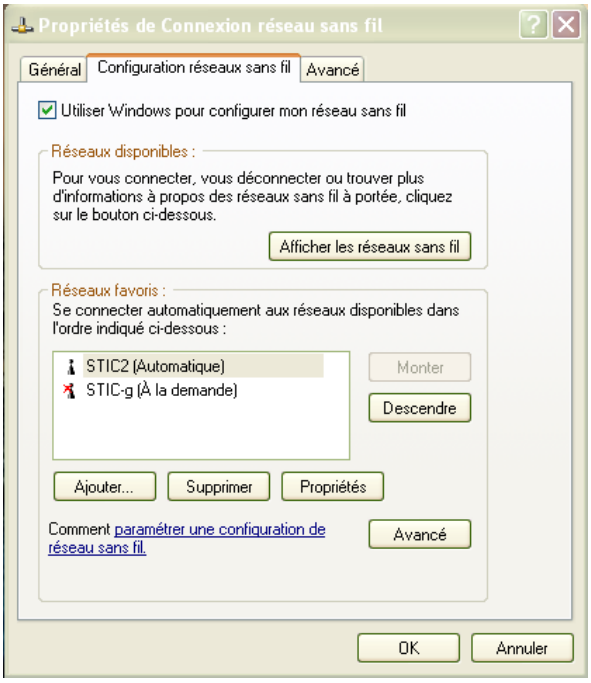
Dans le premier :

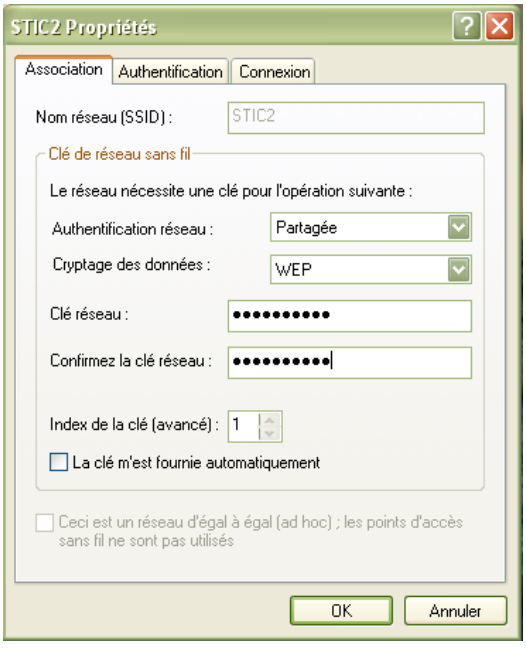
```
Cd /etc/raddb/
Radiusd -X -A
```

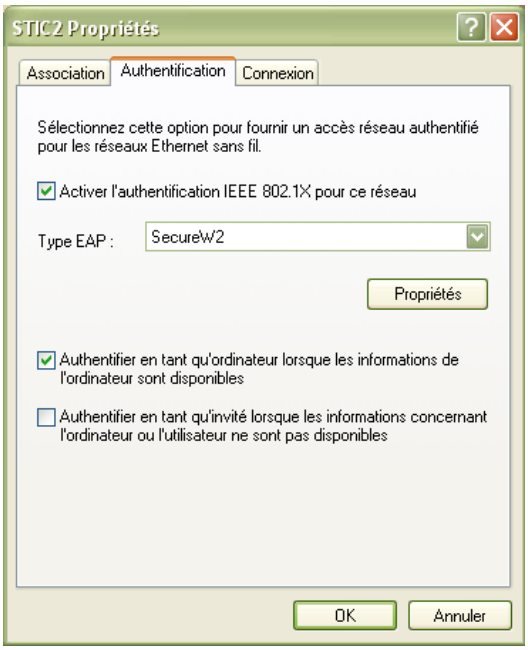
Dans le second :

```
Cd /etc/raddb
Radtest testing123 testing123 localhost 0 testing123
```

C.2.2 – Configuration du poste client







Nous devons spécifier le nom du réseau auquel nous voudrions se connecter, qui est désigné par le SSID de l'AP.

Wifi est le nom du propriétaire du certificat.


SecureW2 Profile: STIC2
Alfa & Ariss
Network Security Solutions
Connection
Certificates
Authentication
User account
Verify server certificate
Trusted Root CA:
telecommunication
Add CA
Remove CA
Verify server name:
Advanced
OK
Cancel


SecureW2 Profile: STIC2
Alfa & Ariss
Network Security Solutions
Connection
Certificates
Authentication
User account
Prompt user for credentials
Username:
wifi
Password:
Domain:
Use this account to logon computer
Advanced
OK
Cancel

Annexe D

Configuration du point d'accès Cisco aironet 350

BR350-53de21 **Summary Status**

Cisco 350 Series Bridge 12.00T

Home | Map | Network | Associations | Setup | Logs | Help

Uptime: 00:33:09

Current Associations			
Clients: 0 of 0	Repeaters: 0 of 1	Bridges: 0 of 0	APs: 0

Recent Events		
Time	Severity	Description
00:19:59	Warning	Ethernet Link Lost. Attempting to re-establish link to primary network.
00:19:44	Warning	Ethernet Link Lost. Attempting to re-establish link to primary network.
00:19:29	Warning	Ethernet Link Lost. Attempting to re-establish link to primary network.
00:19:14	Warning	Ethernet Link Lost. Attempting to re-establish link to primary network.
00:18:59	Warning	Ethernet Link Lost. Attempting to re-establish link to primary network.

Network Ports				Diagnostics
Device	Status	Mb/s	IP Addr.	MAC Addr.
Ethernet	Up	100.0	176.64.0.237	00409653de21
Bridge Radio	No Link	11.0	176.64.0.237	00409653de21

Figure C.1

Cliquer sur l'icône setup :

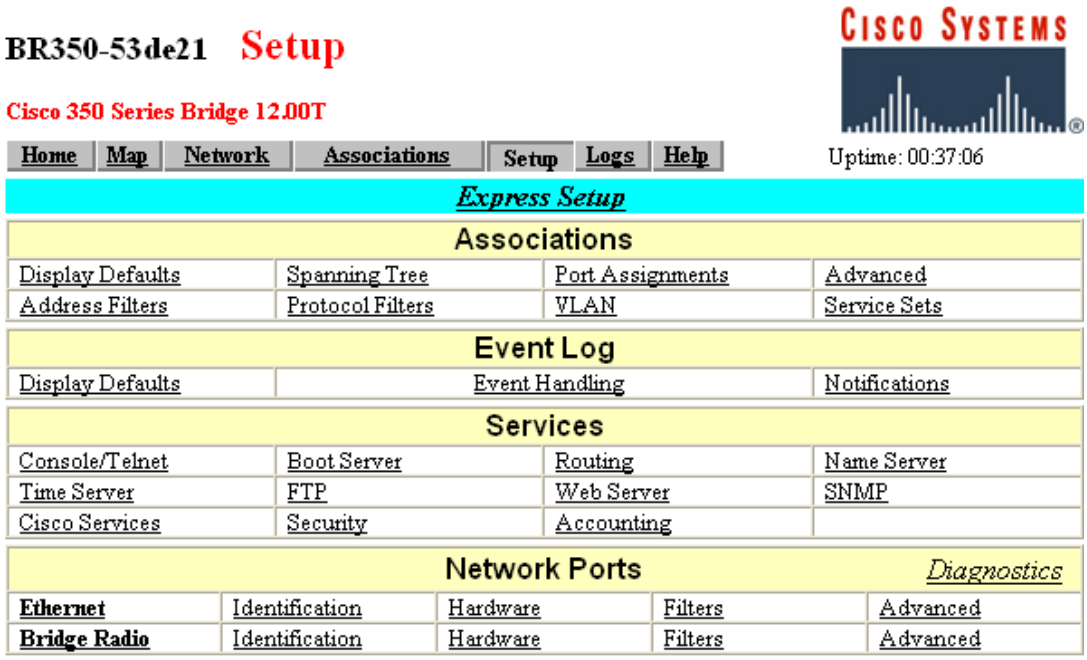


Figure C.2

Puis sur sécurity :

Figure C.3

Puis authentification Server :

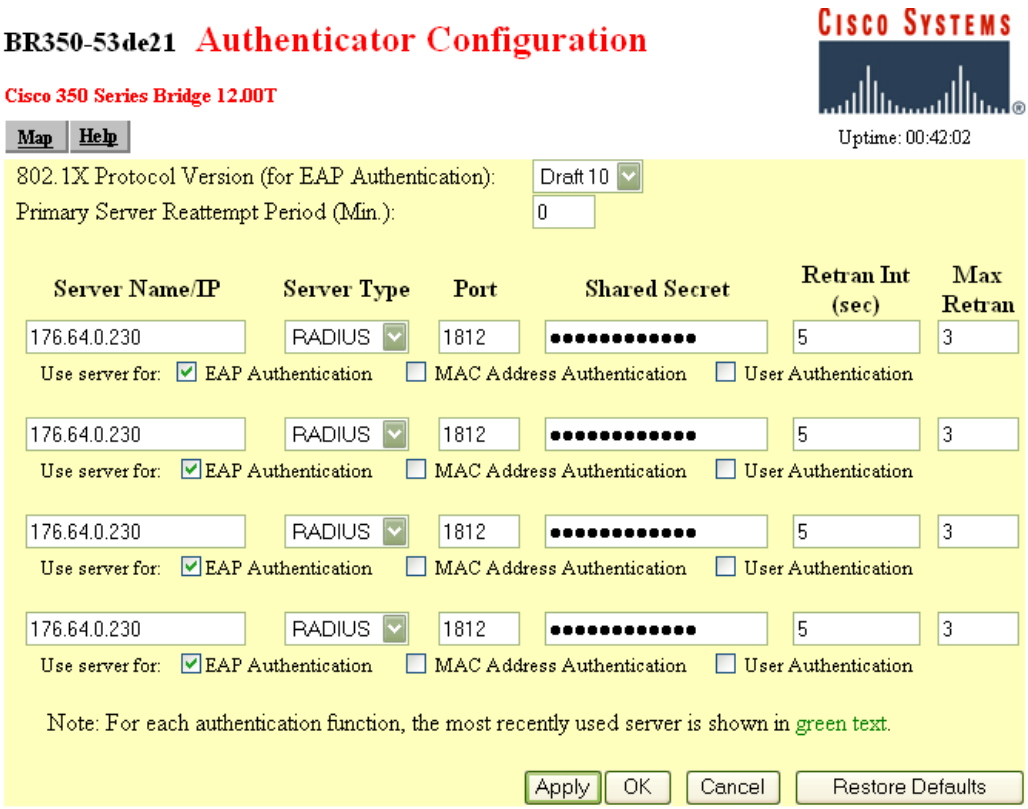


Figure C.4

On configure l'@ IP du serveur RADIUS, pui on fait entrer les clés wep :

Figure C.5

On choisi l'espace Radio Data Encryptions :

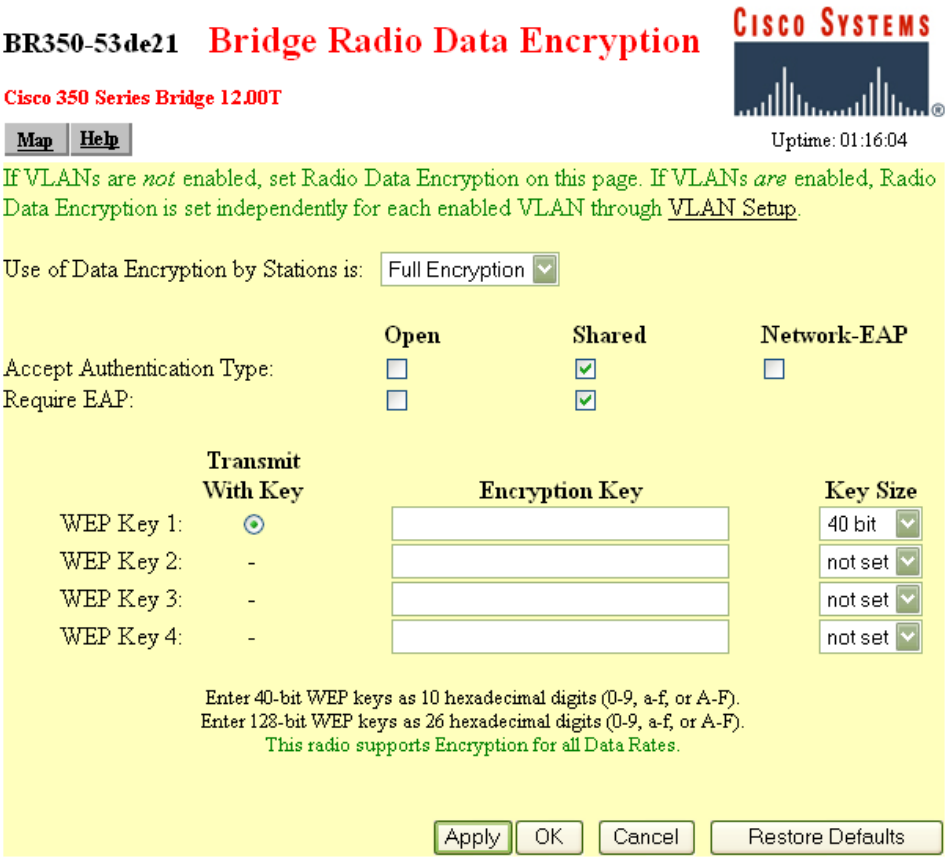


Figure C.6

On retrouve toutes les spécifications sur le bridge au niveau de cette page.

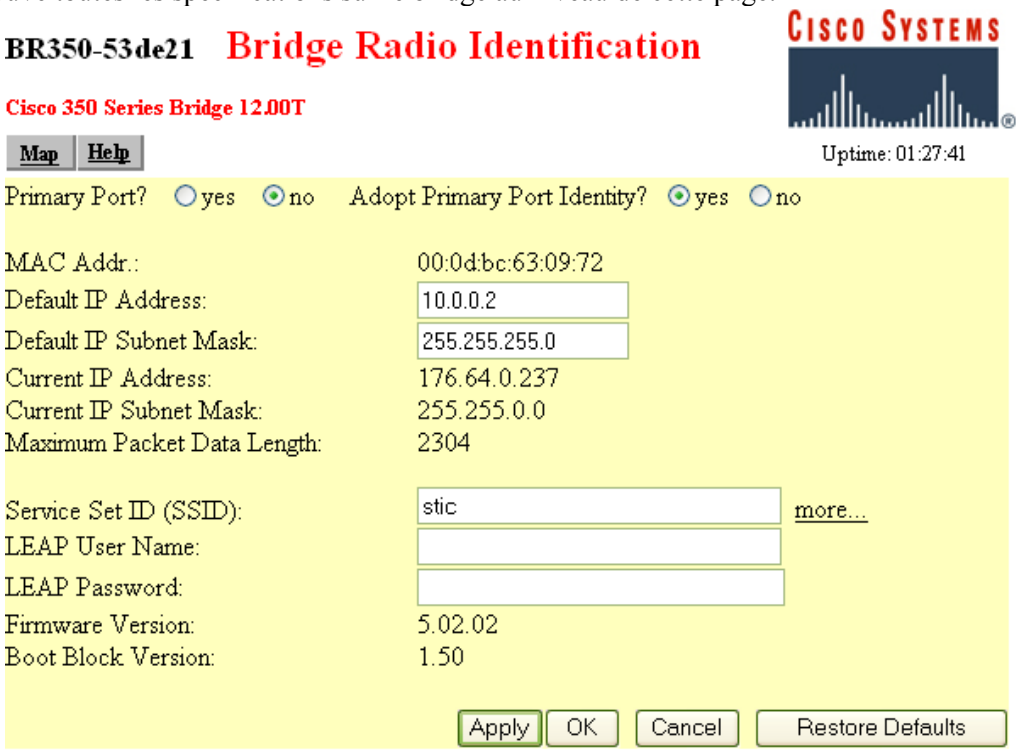


Figure C.7

Bibliographie

Chapitre I

[1] « Historique du WiFi »,

http://www.coopwifi.com/technologie.html visité janvier 2007

[2] « Le WIFI- L'Internet sans fil » 2003,

http://www.artezia.net/technologies/wifi/wifi.htm

[3] Guy Pujolle « Sécurité Wi-Fi ». Edition Eyrolles, Octobre 2004

[4] **Jean-François Pillou** « Introduction au Wi-Fi (802.11) », **2007**

http://www.commentcamarche.net/wifi/wifiintro.php3

[5] Jean louis Lacoche « Le réseau Wifi (Wireless FIdelity) » 20.01.2007

http://locoche.net/wifi.php

[6] Leila Cherid « Le développement de la technologie Wimax. Situation et perspectives » Direction de l'interconnexion des nouvelles technologies, ARPT. Alger 19-22 juin 2006.

[7] Pierre-Olivier Bourgeois, Alexis MARCOU « La Sécurité dans IEEE802.11 » Université de Nantes. 26 juillet 2004

[8] Bruno Cormier «50 sociétés néo-zélandaises ont un réseau WiFi ouvert » 14 juillet 2005

http://www.pcinpact.com/actu/news/50_societes_neozelandaises_ont_un_reseau_WiFi_ouve.htm

[9] Alexander Gostev (**Analyste Virus Senior, Kaspersky Lab**) «Sécurité des réseaux sans fil et wardriving à Paris » **20.12.2006.**

http://www.viruslist.com/fr/analysis?pubid=200676066

[10] « Encore-un-quart-de-reseaux-Wifi- dentreprises »

http://www.pcinpact.com/actu/news/29083-Encore-un-quart-de-reseaux-Wifi-dentreprises.htm

[11] « Le réseau sans fil WiFi Université Henri Poincaré Nancy 1 »,

http://www.cri.uhpnancy.fr/wuhp/index.php?id_rub=102&PHPSESSID=83293fb52f6a57a7fd9af4261bdc3a31#1

[12] « Le WiFi à l'Université de Limoges, Nouveau service sur le réseau Wi-Fi (SMTPS) »
19 Juin 2006

http://wifi.unilim.fr/article.php3?id_article=106

[13] « Présentation et configuration de votre connexion à CanalIP-UPMC »

http://www.canalip.upmc.fr/doc/Default.htm

[14] Christophe Saillard « 802.1X : Solution d'authentification sécurisée pour le futur réseau sans fil de l'Université Louis Pasteur » Centre Réseau Communication, Université Louis Pasteur, Strasbourg 2002.

[15] Houda Labiod « **WiFi et WiFi5 »** Ecole Nationale Supérieure des Télécommunications

www-rp.lip6.fr/dnac/4.3-labiod-article.pdf

[16] :T. Sekkal & S. Djaziri « Les failles du protocole Web dans les réseaux sans fil ». Mémoire d'ingénieurs en Informatique, université de Tlemcen. Décembre 2005.

[17]: H. **Sebbagh** & A. **khebichat** « sécurité des réseaux sans fil ». Mémoire d'ingénieurs en informatique, université de Tlemcen. octobre 2005.

[18]: A. **Benazza** « audit de sécurité du réseau informatique de l'université de Tlemcen ». Mémoire d'ingénieurs en informatque, université de Tlemcen. Juin 2006.

[19] Alex « WPS : certification pour un Wi-Fi sécurisé par défaut », **8 janvier 2007.** http://www.clubic.com/actualite-67922-wps-certifcation-wifi-securise-defaut.html

Chapitre II

[20] Houda Labiod & Hossam Affifi. « De Bluetooth à Wi-Fi ». Lavoisier 2004.

[21] « Wifi : Matériel nécessaire »
http://www.clubic.com/wiki/Wifi_:_Mat%E9riel_n%E9cessaire

[22] « Antenne Wifi Neodiscount_ Antenne wifi ainsi que ses accessoires » 2003

http://www.neodiscount.com/antenne-wifi.htm

[23] Balmokoun Bruno « SECURITE DANS LE MONDE WIFI » **:** Ingénieur Maître en Informatique et Mathématiques, université des Antilles et de la Guyane, 2005.

[24] « Le Direct Le Frequency-Hopping Spread Spectrum[] (FHSS) » 2004-08-25
http://www.pouf.org/documentation/securite/html/node9.html

[25] « Sequence Spread Spectrum[] (DSSS) » 2004-08-25
http://www.pouf.org/documentation/securite/html/node10.html

[26] « Techniques de transmission de données »
http://www.commentcamarche.net/wifi/wifitech.php3

[27] « Les techniques de Modulation »
http://www.commentcamarche.net/s/les-techniques-de-modulation

[28] John Bellardo & Stefan Savage « 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions » Department of Computer Science and Engineering University of California at San Diego
www.cs.ucsd.edu/~savage/papers/UsenixSec03.pdf

[29] « Etude des réseaux 802.11. Déploiement et Architecture »
http://brett2078.free.fr/images/TOWifi/wlan-1.0.pdf

Chapitre III

[30] Anonyme. « Sécurité Maximale des systémes et réseaux». Edition CompusPress 4émé édition 2003

[31] Guy Pujolle « Les Réseaux ». Edition Eyrolles, 2003.

[32] Ibrahim HAJJEH « Sécurité des échanges. Conception et validation d'un nouveau protocole pour la sécurisation des Echanges ». Thèse de doctorat Spécialité informatique et réseaux. ENST Paris. 7 décembre 2004

[33] Guillaume Desgeorge « La sécurité des réseaux » **2000**
www.wireless-lyon.org/docs/base/Securite.pdf

[34] « Attaques - Analyseurs réseau (sniffers) »
http://www.epsic.ch/Branches/info/ccm/attaques/sniffers.htm

[35] « Attaques - Spoofing IP »
http://www.commentcamarche.net/attaques/usurpation-ip-spoofing.php3

[36] « Attaques - Man in the middle » 2007
http://www.commentcamarche.net/attaques/man-in-the-middle.php3

[37] Hani Raghab Hassan « Sécurité des Réseaux d'Ordinateurs Sans-fil » Laboratoire HeuDiaSyC UMR-CNRS 6599. Université de Technologie de Compiègne, France

[38] Mohamed Badra « Le transport et la sécurisation des échanges sur les réseaux sans fil » Thèse de Doctorat en Informatique et Réseaux**,** ENST PARIS. 2005

[39] Nicole Dausque, « Infrastructures de gestion de clefs » 09/05/2000
www.urec.cnrs.fr/IMG/**pdf**/IGC.**pdf**

Chapitre IV

[40] Cédric Llrens & Laurent Levier « Tableaux de bord de la sécurité Wi-Fi ». Edition Eyrolles. Octobre 2004.

Chapitre V

[41] Goutte Alexis. « Guide d'installation de Freeradius avec EAP-TLS+Mysql »

[42] Florian. « Installation de Freeradius en mode EAP-TLS » **24/05/2004**
http://www.alphacore.net/spip/spip.php?article33

[43] Florian. 02/05/2004 « Installation de Freeradius en mode EAP-TTLS »
http://www.alphacore.net/spip/spip.php?article45

[44] « **CanalIP-UPMC** »
http://www.canalip.upmc.fr

Glossaire

A

AAA : Authentication Authorization Accounting.
ACK : Acknowlegement.
ACL : Access Control List.
AES : Advanced Encryption Standard.
ARP : Address Resolution Protocol.
ARPT : Autorité de Régulation des Postes et Télécommunications.
ART : Autorité de Régulation des Télécommunications.
AT: Algérie Télecom.

B

BEB : Binary Exponential Backoff
BLR : Boucle Locale Radio
BPSK : Binary Phase Switch Keying.
BSS : Besic Service Set
BSSID : BSS Identifier

C

CA : Certificate authority.
CAM : Continuous Aware Mode.
CCA : Clear Channel Assessment.
CCK : Complementary Code Keying.
CCMP : Counter-Mode/CBC-Mac protocol.
CFP : Contention Free Period.
CHAP : Challenge Handshake Authentication Protocol
CHU : Centre Hospitalier Universitaire.
CP : Contention Period.
CRC : Control Redondancy Check.
CRL : Certificate Revocation List.
CS : Carrier Sense.
CSMA/CA : Carrier Sense Multiple Access/Collision Detection.
CSMA/CD : Carrier Sense Multiple Access/Collision Detection.

CTS : Clear To Send.

D

DBPSK : Differential Binary Phase Shift Keying.
DCF : Distributed Coordination Function.
DES : Data Encryption Standard.
DIFS : Distributed Inter Frame Space.
DMZ : De-Militarized Zone.
DN : Distinguished Name.
DQPSK : Different Quadrature Phase Dhift Keying.
DoS : Deni Of Service.
DS : Distribution System.
DSSS : Direct Sequence Spread Spectrum.

E

EAP : Extensible Authentication Protocol.
EIFS : Extended Inter Frame Space.
ESS : Extended Service Set.
ESSID : Extended SSID.
ETSI : European Telecommunications Standards Institute.

F

FAI : Fournisseurs d'accès Internet.
FCC : Federal Communications Commission.
FCS : Frame Check Sequence.
FEC : Forward Error Correction.
FHSS : Fréquency Hopping Spread Spectrum.

G

GFSK : Gaussian Frequency Shift Keying.

H

HCF : Hybrid Coordination Function.
HEC : Header Error Check.
HiperLAN : Hiper Local Area Network.
HMAC : Hashed Message Authentication Code.
HTTPS : HyperText Transport Protocol Security.

I

IAPRP : Inter Access Point roaming Protocol.
IBSS : Independant Basic Service Set.
ICMP : Internet Control Message Protocol.
ICV : Integrity Check Value.

IDS : Intrusion Detection System.
IEEE : Institute for Electrical and Electronic Engineers.
IFS : Inter Frame Space.
IGC : Infrastructure de Gestion des Clés.
IP : Internet Protocol.
IPsec : IP Security.
ISP : Internet service provider.
IV : Vecteur d'Initialisation.

K

KSA : key Sheduling Algorithm.

L

LAN : Local Area Network.
LDAP : Lightweight Directory Access Protocol.
LEAP : Lightweight Extensible Authentication Protocol.
LLC : Logical Link Control.
LSAP : Logical Service Access Point.

M

MAC : Medium Access Control.
MAN : Metropolitan Area Network.
MD5 : Message Digest 5.
MIB : Management Information Base.
MIC: Michael Integrity Check.
MIC : Message Integrity Check.
MitM : Man in the Middle.
MK : Master Key.
MKK : Kensa kentei Kyokai.

N

NAS : Network Attached Storage.
NAV : Network AllocationVector.

O

OFDM : Orthogonal Frequency Division Multiplexing.
OSI : Open Source Inder
OTP : One Time Password.

P

PAE : Port Access Entity.
PBCC : Packet Binary Convolutionnary Code.
PC : Point of Coordination.

PCF : Point Coordination Function.
PCMCIA : Personal Computer Memory Card International Association
PCS : Physical Carrier Sense.
PDA : Personal Digital Assistant.
PEAP : Protected Extensible Authentication Protocol.
PGP : Pretty Good Privacy.
PH : Couche Physique.
PIFS : Point Inter Frame Space
PIN : Personal Identification Number.
PKCS : Public-Key Cryptography Standard.
PKI : Private Key Infrastructure.
PLCP : Physical Layer Convergence Protocol.
PLW : PSDU Length Word.
PMD : Physical Medium Dependent.
PMK : Paire Master Key.
PPDU : PLCP Protocol Data Unit.
PPM : Pulse Position Modulation.
PPP : Point to Point Protocol.
PR : Polling Request.
PRF : Probe Request Frame.
PSDU : PLCP Service Data Unit.
PSF : PCLP Signaling Field.
PSPM : Power Save Polling Mode.
PSK : Phase Shift Keying.

Q

QAM : Quadrature Amplitude Modulation.
QoS : Quality of Service.
QPSK : Quadrature Phase Switch Keying.

R

RA : Receiver Address.
RADIUS : Remote Authentification Dial-In User Service.
RC4 : Ron's Code #4.
RFC : Request For Comments.
RSA : Rivest shamir Adleman.
RSN : Robust Security Network.
RSSI : Received Signal Strength Indicator.
RTS : Request To Send.

S

SFD : Star Frame Delimiter.
SIFS : Short Inter Frame Space.
SIM : Subscriber Identity Module.
SK : Shared Key.
S-MIME : Secure / Multipurpose Internet Mail Extensions.
SNMP : Simple Network Management Protocol
SSID : Service Set Identity.
SSL: Secure Socket Layer.

STIC : Systéme & Technologies de l'Information & de la Communication.
SYN : Synchronize.

T

TA : Transmitter Address.
TCP : Transport Control Protocol.
TIM : Traffic Information Map.
TKIP : Temporary Key Integrity Protocol.
TLS : Transport Layer Security.
TSF : Timing Synchronization Function.
TTLS : Tunneled Transport Layer Security.

U

UDP : User Datagram Protocol.
UPMC : Université de Pierre et Marie Currie.
USB : Universal Serial Bus.
USM : User Security Model.

V

VCS : Virtual Carrier Sense.
VPN : Virtual Private Network.

W

WAN : Wide Area Network.
WEP : Wired Equivalent Privacy.
Wi-Fi : Wireless Fedelity.
WLAN : Wireless Local Area Network.
WLL : Wireless Local Loupe
WMAN : Wireless Metropolitan Area Network.
WPA : Wi-Fi Protected Access.
WPA : Wireless Protocol Access.
WPS : WiFi Protected Setup.
WWAN : Wireless Wide Area Network.