WhitePaper :

Les réseaux sans fils et le 802.11b

Réalisé par :

FreeLink® Networking

1. Introduction

En fait la communication numérique sans fil n'a rien d'une idée neuve. En 1901, déjà, le physicien Gugliemo Marconi fit sur un bateau la démonstration d'une liaison télégraphique sans fil avec la côte en utilisant le code Morse (les points et les traits forment bien un système binaire). Les systèmes numériques d'aujourd'hui ont certes de meilleures performances, mais l'idée reste la même.

Les technologies sans fil représentent actuellement ce qu'on appelle la 2ème révolution internet. Grâce au **802.11x**, à **Bluetooth** et tous les autres protocoles passant par ondes radio ou infrarouge, l'informatique circule sans entrave. Le sans fil sonne le glas de tous ces câbles qui enchaînent les ordinateurs et vous empêchent de profiter d'une connexion en tous lieux et en tous moments. La communication nomade se développe si vite et sous tellement de formes différentes que nous n'avons que l'embarras du choix pour nous connecter (téléphones portables, ordinateurs avec **WiFi** intégré, **PDA** et même talkies-walkies).

A l'endroit même où vous vous trouvez en ce moment, des douzaines de réseaux de données sans fil distribuent des informations aux quatre coins de la planète. Un de vos voisins fait ses courses tandis que quelqu'un de l'autre coté de la rue discute (gratuitement) de vive voix avec l'une de ses connaissances située à Hong Kong, tout cela pendant qu'une autre personne télécharge l'album de son groupe de musique favoris depuis un site hébergé à San Francisco. Le sans fil constitue donc probablement la technologie la plus merveilleuse qui soit, après internet.

2. Les différentes catégories

2.1. Wireless Personal Area Network (WPAN)

Le réseau personnel sans fils concerne les réseaux d'une faible portée : de l'ordre de quelques dizaines mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques, ...) ou un assistant personnel (PDA) à un ordinateur sans liaison filaire ou bien à permettre la liaison sans fils entre deux machines très peu distantes. Il existe plusieurs technologies utilisées pour les WPAN :

Bluetooth, lancée par Ericsson en 1994, propose un débit théorique de 1 Mbps pour une portée maximale d'une trentaine de mètre. Bluetooth possède l'avantage d'être très peu gourmand en énergie, ce qui le rend particulièrement adapté à une utilisation au sein de petits périphériques. C'est sans aucun doute le leader dans le domaine des réseaux personnel.

HomeRF (*Home Radio Frequency*), lancée en 1998 par le HomeRF Working Group (formé notamment par les constructeurs Compaq, HP, Intel, Siemens, Motorola et Microsoft) propose un débit théorique de 10 Mbps. Cette norme a été abandonnée en Janvier 2003.

La technologie **ZigBee** permet d'obtenir des liaisons sans fil à très bas prix et avec une très faible consommation d'énergie, ce qui la rend particulièrement adaptée pour être directement intégré dans de petits appareils électroniques (appareils électroménagers, hifi, jouets, ...).

Enfin les liaisons **infrarouges** permettent de créer des liaisons sans fils de quelques mètres avec des débits pouvant monter à quelques mégabits par seconde.

2.2. Wireless Local Area Network (WLAN)

Le réseau local sans fils est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre-eux les terminaux présents dans la zone de couverture. Il existe plusieurs technologies concurrentes :

Le **Wifi** (ou IEEE 802.11), soutenu par l'alliance **WECA** (Wireless Ethernet Compatibility Alliance) offre des débits allant jusqu'à 54Mbps sur une distance de plusieurs centaines de mètres. Cette technologie sera étudiée plus en détail dans la suite du dossier.

hiperLAN2 (*HIgh Performance Radio LAN 2.0*), norme européenne élaborée par l'**ETSI** (*European Telecommunications Standards Institute*). HiperLAN 2 permet d'obtenir un débit théorique de 54 Mbps sur une zone d'une centaine de mètres dans la gamme de fréquence comprise entre 5 150 et 5 300 MHz.

2.3. Wireless Metropolitan Area Network (WMAN)

Le réseau métropolitain sans fils est connu sous le nom de **BLR** *(Boucle Locale Radio)*. Les WMAN sont basés sur la norme *IEEE 802.16*. La boucle locale radio offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres, ce qui destine principalement cette technologie aux opérateurs de télécommunication.

2.4. Wireless Wide Area Network (WWAN)

Le réseau étendu sans fils est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fils les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fils. Les principales technologies sont les suivantes :

- **GSM et GPRS: GPRS** (*General Packet Radio Service*) est un service de données disponible sur les réseaux GSM (*Global System for Mobile Communication*). Il offre un débit de 20 à 30kbps et est un protocole basé sur les paquets signifiant que le GPRS ne transmet que lorsque des données doivent être envoyées. La plus grosse partie du monde est entièrement couverte par le réseau GSM.
- **CDPD et TDMA : CDPD** (Cellular Digital Packet Data) fonctionne sur le très populaire réseau mobile TDMA (Time Division Multiple Access), qui est aisément le réseau mobile le plus déployé aux Etats-Unis. Il offre des vitesses jusqu'à 19,2kbps.
- **1xRTT et CDMA : CDMA** (Code Division Multiple Access) est la 2ème technologie mobile la plus utilisée aux Etats-Unis. 1xRTT est une mise à jour qui permet des débits de 144kbps.
- **UMTS** (Universal Mobile Telecommunication System)**: UMTS** est la nouvelle norme pour les téléphones portables ou PDA (Portable Digital Agenda), elle permettra d'augmenter le débit de données entre le portable et le relais, avec un débit allant jusqu'à 2 M bits/seconde. L'endroit sera aussi insignifiant pour les données qu'il est actuellement pour la voix.

3. La Norme 802.11b

3.1. Introduction

Cela fait une bonne quinzaine d'années que l'on parle des réseaux de transmission de données sans fil ouverts au public sans qu'une technologie n'ait permis de faire émerger un modèle économique parvenant d'en faire véritablement décoller l'usage.
Pourtant nombreuses ont été les technologies candidates : CT2, Tétra, 3RD, DECT, ERMES, WAP/GPRS, sans compter les protocoles propriétaires. Les spéculations financières que la future technologie **UMTS** avait suscitées, avaient même failli, à tort, faire de l'Internet mobile un mythe inaccessible. Et pourtant, aujourd'hui, avec l'arrivée du **WiFi**, et le renouveau de l'**UMTS**, tout semble possible de nouveau.

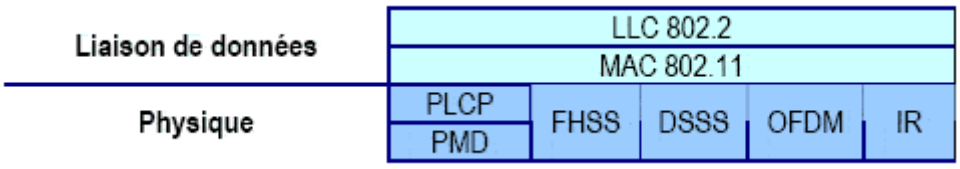
La norme IEEE 802.11 *(ISO/IEC 8802-11)* est un standard international décrivant les caractéristiques d'un réseau local sans fil datant d'une dizaine d'années. Le nom **WiFi** *(contraction de Wireless Fidelity)* correspond initialement au nom donné à la certification délivrée par la **WECA** *(Wireless Ethernet Compatibility Alliance)*, l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11. Par abus de langage le nom de la norme se confond aujourd'hui avec le nom de la certification. Ainsi un réseau **WiFi** est en réalité un réseau répondant à la norme 802.11.

Le **WiFi** s'est est tout d'abord développée pour des usages privés, principalement dans le monde des réseaux d'entreprises. Sous l'impulsion donnée en 1999 par une alliance entre industriels - la WiFi Alliance - le **WiFi** est parvenu à s'imposer dans un nombre croissant d'équipements informatiques nomades. La création du label **WiFi** qui garantit la compatibilité des terminaux et des infrastructures de tous les constructeurs, a en effet entraîné une adhésion massive des acteurs qui commercialisent dorénavant des milliers de produits différents labellisés **WiFi**. L'intégration du standard 802.11 dans le système d'exploitation Microsoft Windows XP, les microprocesseurs Centrino d'Intel, la présence de carte **WiFi** intégrées directement sur les ordinateurs portables et PDA, illustre à quel point **WiFi** est désormais incontournable.

Fort de son irrésistible ascension dans les usages privés, entreprise et grand public, le **WiFi** ambitionne également de s'imposer comme le standard qui permettra l'essor des réseaux de transmission de données ouverts au public (aéroports, hôtels, gares, universités, etc.).

3.2. Méthode d'accès

La norme 802.11 couvre les deux premières couches du modèle **OSI** *(Open Systems Interconnexion)* : la couche physique et la couche liaison de données. Le tableau suivant résume l'ensemble des protocoles utilisés :



3.2.1. Couche Physique (Couche 1)

La couche physique définit la modulation des ondes radio électriques et les caractéristiques de la signalisation pour la transmission de données. Elle se décompose en deux sous-couches :

- **PLCP** *(Physical Layer Convergence Protocol)* : s'occupe de l'écoute du support et de la signalisation en fournissant un **CCA** *(Clear Channel Assessment)* à la couche MAC.
- **PMD** *(Physical Medium Dependent)*: traite la modulation et l'encodage des données à transmettre sur le support.

L'IEEE 802.11 définit quatre types de couche physique :

- **FHSS** *(Frequency Hopping Spread Spectrum)*, avec modulation DBPSK : étalement du spectre par saut de fréquence.
- **DSSS** *(Direct Sequence Spread Spectrum)*, avec modulations DBPSK et DQPSK : étalement du spectre par séquence directe.
- **OFDM** *(Orthogonal Frequency Division Multiplexing)*, avec modulation QAM : Effectue un multiplexage fréquentiel de sous porteuses orthogonales.
- **Infrarouge**, avec une modulation **PPM**

Les deux premières couches sont utilisées par les réseaux 802.11 et 802.11b (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 Mbits/s, c'est-à-dire pour les réseaux 802.11a et 802.11g.

Enfin, l'infrarouge est destiné aux réseaux à faible portée.

3.2.2. Couche Liaison de Données (Couche 2)

a. LLC (Logical Link Control)

Son rôle est d'adapter les données venant des couches supérieures à la couche physique. Cette couche normalisée 802.2 permet de relier un **WLAN** 802.11 à tout autre Réseau respectant l'une des normes de la famille 802.*x*.

b. MAC (Medium Access Control)

Son rôle est d'écouter le canal, attendre s'il est occupé, puis transmettre lorsqu'il se libère.

En plus des fonctions habituellement rendues par la couche **MAC**, la couche **MAC** 802.11 offre d'autres fonctions qui sont normalement confiées aux protocoles supérieurs, comme la retransmission, l'acquittement ou la fragmentation de trames.

Les trames 802.11 sont du type suivant:

Préambule	Entête PLCP	Données MAC	CRC

Nous ne détaillerons que le champ « Données MAC » :

Contrôle de trame 2 octets	durée/Id 2 octets	adresse1 6 octets	adresse2 6 octets	adresse3 6 octets	Contrôle de séquence 2 octets	adresse4 6 octets	Corps de la trame 0-2312 octets	CRC 4 oct.

Ensuite le champ « Contrôle de Trame » :

Ver. Proto	Type	Sous - Type	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order

Et finalement le champ ToDS et FromDS. Ces champs sont significatifs en ce qui concerne la sécurité 802.11. En effet, ils permettent de connaître le **BSSID** qui permet d'identifier un réseau sans fil. Le chapitre 3.x.x explique le principe de l'ssid et le chapitre 3.5.2 fait référence à la sécurité le concernant.

La norme 802.11 introduit, de plus, deux méthodes d'accès au support physique fondamentalement différentes, le **DCF** *(Distributed Coordination Function)* et le **PCF** *(Point Coordination Function).*

DCF, équivaut à la méthode d'accès au support des réseaux filaires traditionnels supportant le best effort, c'est-à-dire des réseaux dans lesquels tous les utilisateurs ont une chance d'accéder au support. La seconde, appelé **PCF**, se base l'interrogation des terminaux, ou polling, contrôlée par le point d'accès. Elle est utilisée pour la transmission de données temps réel, telles que la voix ou la vidéo. Un réseau de type ad hoc supporte uniquement le **DCF**, tandis qu'un réseau infrastructure peut supporter à la fois le **DCF** et **PCF**. Cependant très peu de points d'accès supportent la combinaison **DC**/**PCF**.

Méthode d'accès DCF :

Le **DCF** est fondée sur la méthode **CSMA**/**CA** *(Carrier Sense Multiple access/Collision Avoidance, accès multiple à détection de porteuse/esquive de collision)*, elle-même dérivée de la méthode **CSMA**/**CD** *(Carrier Sense Multiple Access/Collision Detection, accès multiple à détection de porteuse /détection de collision)* utilisée par des réseaux filaires traditionnels, et notamment par Ethernet.

La norme 802.11 n'est cependant pas capable de détecter les collisions comme le fait la méthode **CSMA**/**CD**. Elle va donc essayer d'éviter ces collisions grâce à la méthode **CSMA**/**CA**.

Pour cela, le 802.11 va en fait utiliser plusieurs techniques complémentaires :

Positif Acknowledge	C'est un mécanisme d'acquittement qui envoi un ACK lorsqu'une trame est reçue.	
IFS *(Inter Frame Spacing)*	Les espaces inter trames : Définit un intervalle de temps entre l'émission de deux trames. La norme 802.11 définit quatre types d'**IFS** :	
	SIFS	Le plus court, représente le plus court des IFS et permet de séparer deux trames d'un même dialogue (envoie de données, ACK, etc.).
	PIFS	Utilisé par le point d'accès pour bénéficier d'une

		priorité supérieure, dans le cas de réseaux à accès au support mixte **DCF**/**PCF**.
	DIFS	Utilisé lorsqu'une station veut commencer une nouvelle transmission.
	EIFS	Le plus long, utilisé par une station quand la couche physique indique à la couche MAC qu'une transmission de trame a débuté mais qu'aucun **FCS** correct n'a été reçu. L'**EIFS** évite que la station ne provoque de collision avec une future trame du dialogue en cours.
NAV *(Network Allocation Vector)*	C'est une temporisation d'émission qui permet d'éviter les collisions en retardant les émissions de toutes les stations qui détectent que le support est occupé.	

Le principe de fonctionnement est donc le suivant : Lorsque deux stations communiquent, la station réceptrice envoie une trame ACK à la station émettrice pour lui signifier qu'elle a reçu correctement sa trame de données (c'est-à-dire reçue et sans erreur). Si la station émettrice ne reçoit pas cette trame ACK, cela signifie que, soit la station émettrice n'a pas reçue la trame, soit que la trame ACK s'est perdue. La station émettrice en déduit donc qu'il y a eu collision, et la trame de données est retransmise. Pour réduire la probabilité de collision et pour permettre aux stations de se synchroniser plus facilement, les émissions de trames sont séparées par des intervalles **IFS**. Le temporisateur **NAV** est le premier élément qui permet concrètement d'éviter les collisions.

Lorsqu'une station émet sur le réseau, les autres stations détectent la transmission et doivent donc attendre avant d'émettre à leur tour. Pour cela, elle déclenche le temporisateur **NAV**, avec une valeur calculée en fonction de la valeur du champ Durée/ID de la trame **MAC**. La valeur du temporisateur est mis à jour à chaque fois qu'une autre trame d'un même dialogue est reçue ; ainsi, lorsque le **NAV** arrive à zéro, les stations savent qu'elles peuvent émettre à leur tour.
Lorsque le **NAV** arrive à zéro, les stations attendent pendant un **DIFS**, puis déroulent l'algorithme du back off avant d'émettre. Cet algorithme permet d'éviter que deux stations émettent en même temps. Pour cela, chaque station calcule initialement et aléatoirement la valeur d'un temporisateur appelé timer back off, avec une valeur comprise entre 0 et 7. Lorsque une station détecte qu'elle peut émettre (**NAV** à zéro), elle commence à décrémenter le timer. Quand celui-ci arrive à zéro, la station émet. Si une station émet avant que le timer arrive à zéro, ce dernier est bloqué jusqu'à la prochaine exécution du back off. Si les timers de deux stations arrivent à zéro en même temps, on considère qu'il y a collision, et chaque station recalcule son timer avec une valeur comprise entre 0 et 15. Lorsqu'une station a réussi à émettre une trame, elle réinitialise son timer.

Méthode d'accès PCF :

La **PCF** est une méthode d'accès basée sur l'interrogation des terminaux, ou polling, et selon laquelle les échanges sur le réseau sont contrôlés par un **PC** (*Point of Coordination)*, généralement représenté par le point d'accès. Cette méthode est particulièrement adaptée à la transmission de données temps réel, telles que la voix ou la vidéo. Concrètement, les stations envoient des trames spéciales appelées **PR** *(Polling Request)*, 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 court 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** *(Contention Free Period)* pour la **PCF**, et une période dite **CP** *(Contention Period)* 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.

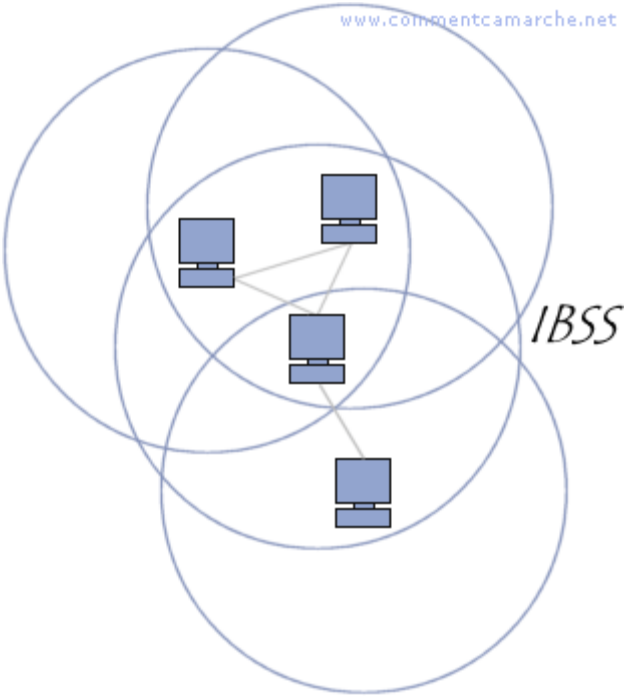
3.3. Mode de fonctionnement

3.3.1. Introduction

La topologie d'un réseau sans fil est très différente de celle d'un réseau local traditionnel. La connectivité est limitée par la portée, nous n'avons habituellement pas une complète couverture (certains nœuds ne peuvent pas se voir). Pour résoudre ce problème, soit le réseau est divisé en cellules contrôlées par un **PA** *(Point d'Accès)* et plusieurs clients peuvent se trouver dans 1 cellule, le réseau ne forme qu'un et chaque station agit en tant que **PA** et client en même temps.

3.3.2. Réseau Ad-hoc

Un réseau ad hoc est la plus simple forme de réseau sans fil composée de quelques nœuds sans aucune possibilité de redirection ou pontage. Tous les nœuds sont égaux et peuvent joindre ou partir à n'importe quel moment. C'est un peu comme un réseau local, on peut ajouter ou supprimer un nœud quand on veut. C'est le genre de réseau développé dans des petits bureaux ou à la maison.

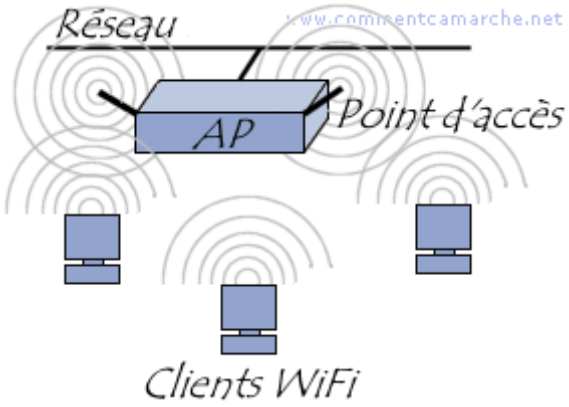


Evidement pour que ceci marche, il faut que chaque nœud puisse voir tous les autres nœuds du réseau. Quand un nœud est hors portée, il perd tout simplement la connexion avec le reste du réseau ad-hoc. Il n'y aura donc plus qu'une seule cellule.

Un des noeuds peut apporter des options de redirection et de routage pour communiquer avec le reste du réseau, mais les noeuds sont toujours renfermés dans la zone de cette cellule. Les stations se trouvant à portée radio forment un **IBSS** *(Independant Basic Service Set)*.

3.3.3. Infrastructure

Le mode infrastructure se base sur une station spéciale appelée **PA**. Ce mode permet à des clients **WiFi** de se connecter à un réseau (généralement Ethernet) via un point d'accès. Elle permet à un client **WiFi** de se connecter à un autre client **WiFi** via leur **PA** commun. Une station **WiFi** associée à un autre **PA** peut aussi s'interconnecter. L'ensemble des stations à portée radio du **PA** forme un **BSS** *(Basic Service Set)*. Chaque **BBS** est identifié par un **BSSID** *(BSS Identifier)* de 6 octets qui correspond à l'adresse MAC du **PA**.



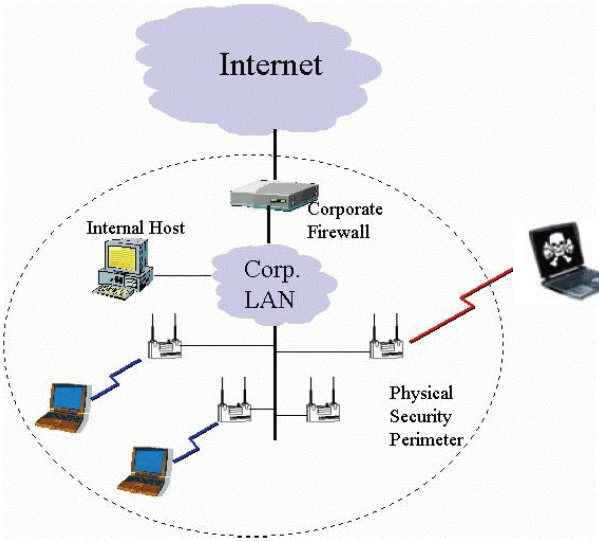
3.3.4. Interconnexion

On peut composer un réseau avec plusieurs **BSS**. Ceux-ci sont reliés entre eux par un **DS** *(Distribution System)* connecté à leurs points d'accès. Ce **DS** est généralement le réseau Ethernet sur lequel le **PA** se connecte mais il peut correspondre à du token ring, FDDI ou un autre réseau 802.11. Ces différents **BSS** interconnectés via un DS forme un **ESS** *(Extended Service Set)*. Un **ESS** est identifié par un **ESSID** (abrégé en SSID) qui est constitué d'un mot de 32 caractères qui représente le nom du réseau. Le **SSID** permet donc la séparation logique de plusieurs réseaux sans fil. On peut associer un **IBSS** au sein d'un **ESS**.

4. Sécurité 802.11b

4.1. Introduction

Les réseaux sans fils 802.11 introduisent un nouveau challenge pour les administrateurs réseaux et administrateurs pour la sécurité de l'information. Contrairement aux traditionnels réseaux Ethernet câblés, les réseaux sans fil émettent des données par fréquences radio pour que les stations clientes puissent les réceptionner. Pour avoir une similitude avec un réseau câblé on pourrait imaginer que toutes les stations clientes soient reliées entre elles par un simple HUB et non un SWITCH. Ce qui implique des nouveaux et complexes enjeux de sécurité (voir schema).



La sécurité des réseaux 802.11 a été minutieusement étudiée par de nombreuses universités. Des chercheurs ont exposé différentes vulnérabilités dans l'authentification, la confidentialité des données et les mécanismes d'intégrité de données.

A cause de leurs problèmes d'émissions par fréquences radio, les réseaux sans fils doivent présentés les propriétés suivantes :

- Authentification des utilisateurs pour prévenir des accès non autorisé.
- Confidentialité et intégrité des données qui sont transmises par fréquences pour éviter toute écoute (sniff) par un tiers.

La norme 802.11b spécifie des techniques de sécurité de base (implémentée directement). Il existe, fort heureusement, d'autres techniques qui permettent de mieux sécuriser l'authentification, la confidentialité et l'intégrité des données.

4.2. Techniques de base

4.2.1. SSID *(Service Set Identifier)*

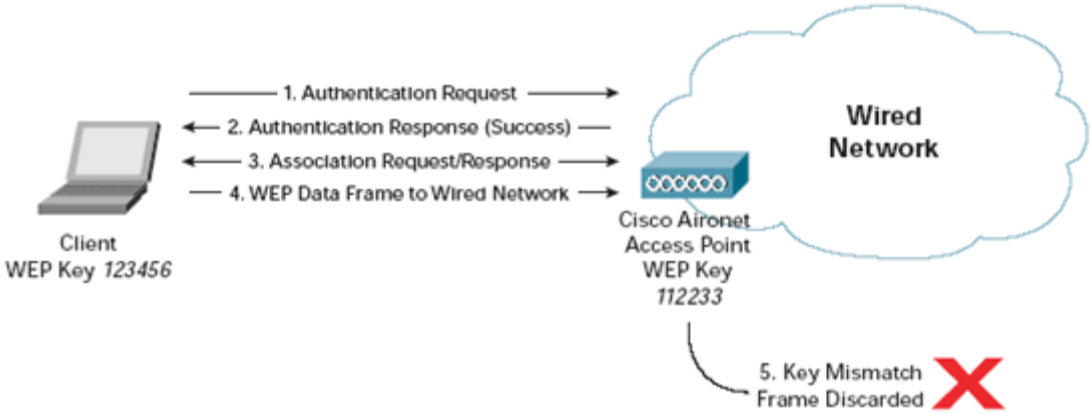
L'**ssid** permet la séparation logique de plusieurs réseaux sans fil. Un client doit donc être configuré avec un **ssid** valide pour avoir accès au réseau sans fil. Toutefois, l'**ssid** n'apporte ni la confidentialité des données ni l'authentification par client.
De plus, l'**ssid** peut être sniffé très facilement même si certains **PA** permettent de désactiver le broadcast des **ssid**, il est possible de le retrouver dans certains paquets.
(La trame et les champs visés sont définis dans le chapitre 3.2.2.2 au point b.)

4.2.2. Authentification

a. Authentification Ouverte

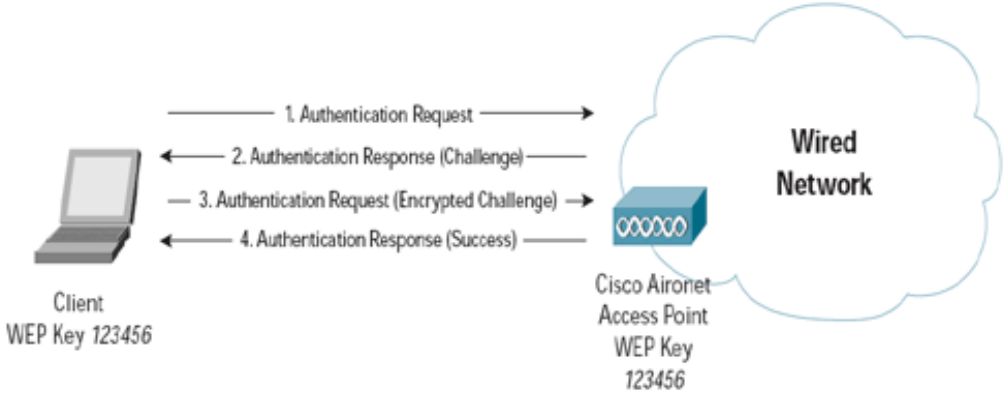
L’authentification ouverte est un algorithme d’authentification nul. Le **PA** donnera l’accès à n’importe quel requête d’authentification. Ca semble peut être inutile mais ceci avait été développé il y a longtemps et les besoins étaient fort différents. Il fallait une authentification rapide qui demande le moins de ressources possibles au **PA**.

L'authentification ouverte permet l’accès à n'importe quel dispositif réseau. Si aucun chiffrage n'est permis sur le réseau, n'importe quel dispositif connaissant le **SSID** du **PA** pourra accéder au réseau. Avec l’encryptions **WEP** activée sur un **PA**, la clef **WEP** devient elle-même un moyen d’authentification. Si un dispositif client n'a pas la clef **WEP** correcte, même si l'authentification est réussie, le dispositif client ne pourra pas transmettre des données à travers le **PA**. Ni l'un ni l'autre ne pourront déchiffrer les données.



b. Authentification par clés partagées (shared key)

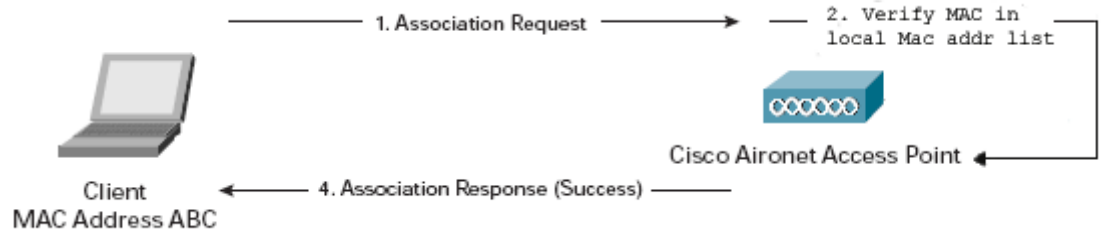
Ce mode de fonctionnement se base sur l'utilisation d'une clé secrète de 40 bits échangée au préalable par un chemin de confiance et l'utilisation de l'algorithme **WEP**. L'objectif de ce dernier est d'offrir une sécurité équivalente à celle offerte par un réseau filaire traditionnel.
L'authentification se fait en 4 étapes :
1 - Demande d'authentification de l'émetteur
2 - Réponse contenant un message aléatoire de 128 octets
3 - 2e message de l'émetteur contenant le message aléatoire précédent et encrypté par l'algorithme **WEP**
4-Vérification de l'intégrité de la trame reçue et du message de 128 octets qu'elle contient.



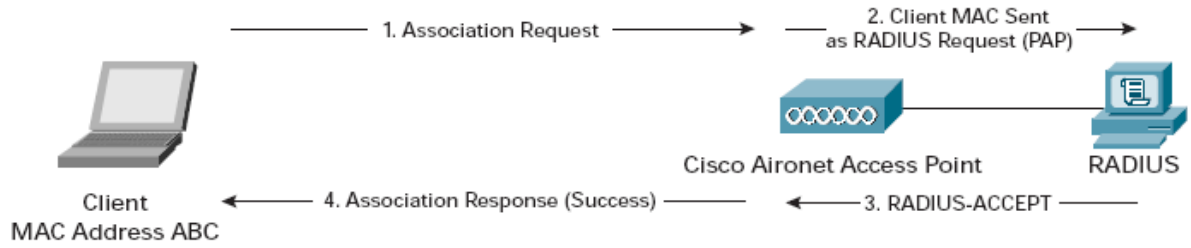
L'authentification à clé partagée exige au client d'utiliser une clé **WEP** partagée pour chiffrer le texte envoyé par le point d'accès. Le point d'accès authentifie le client en déchiffrant la réponse et en regardant si le texte est identique au message de départ. Le processus d'échange de message se fait sur le réseau sans fil et est donc vulnérable aux attaques de types « man-in-the-middle ». Il suffira à un attaquant de sniffer le message non crypté et la réponse cryptée du client. Il pourra ensuite appliquer la fonction XOR sur le texte non crypté et sur la réponse cryptée pour obtenir la clé secrète. Cette solution est par conséquent, peu fiable.

c. Authentification avec adresse MAC

L'authentification avec l'adresse mac se fait au sein même du **PA**. Le **PA** a une liste statique d'adresse mac mise à jour par l'administrateur ou dans le cas des **PA** Cisco par mise à jours automatique (network update). En imaginant qu'un client dont l'adresse figure dans la liste essaye de s'authentifier, le PA renverra un paquet « Association Response » avec le flag Success positionné.



Il est aussi possible d'avoir une liste d'adresse mac sur un autre support que sur le **PA**. Habituellement Freeradius (détaillé au point XXXX) sert de serveur d'authentification. L'authentification avec l'adresse MAC sert à augmenter la sécurité des authentifications à clés ouvertes et partagées pour tenter de réduire les accès non autorisés au réseau.



Ce type d'authentification reste très peu sécurisé. Un simple sniffer pourra récupérer l'adresse MAC. Il suffira à l'attaquant de changer son adresse MAC pour être successivement authentifié.

4.2.3. WEP

Par défaut la norme 802.11 dispose d'un cryptage nul, en option on dispose d'un cryptage des échanges appelé **WEP** *(Wired Equivalent Privacy ou Intimité Equivalente à celle d'un cable)* implémenté au niveau de la couche MAC et qui est disponible sur la plupart des cartes clientes et **PA**.

WEP est basé sur l'algorithme RC4, qui est un algorithme de chiffrement symétrique. Comme expliqué plus haut, les clés de cryptages doivent être les mêmes sur les stations clientes que sur le PA. Le chiffrement se fait sur 40bits et plusieurs constructeurs porposent 128bits.

Cet algorithme est censé renforcer la sécurité au niveau de la confidentialité et intégrité des données. Cependant le protocole WEP a été rapidement "cassé" et il est aujourd'hui admis que cette technique de chiffrement n'est pas sûre, on trouve désormais de multiples outils sur Internet permettant de trouver automatiquement les clés **WEP**.

Voici les principales failles :

- Attaques passives pour décrypter le trafic basé sur des analyses statistiques.
- Attaque active en injectant du nouveau trafic provenant de stations non autorisées.
- Attaques actives pour déchiffrer le trafic en trompant le **PA**.
- Attaque avec un dictionnaire qui, après plus ou moins 1 jour de trafic, permet de déchiffrer automatiquement tout le trafic en temps réel.

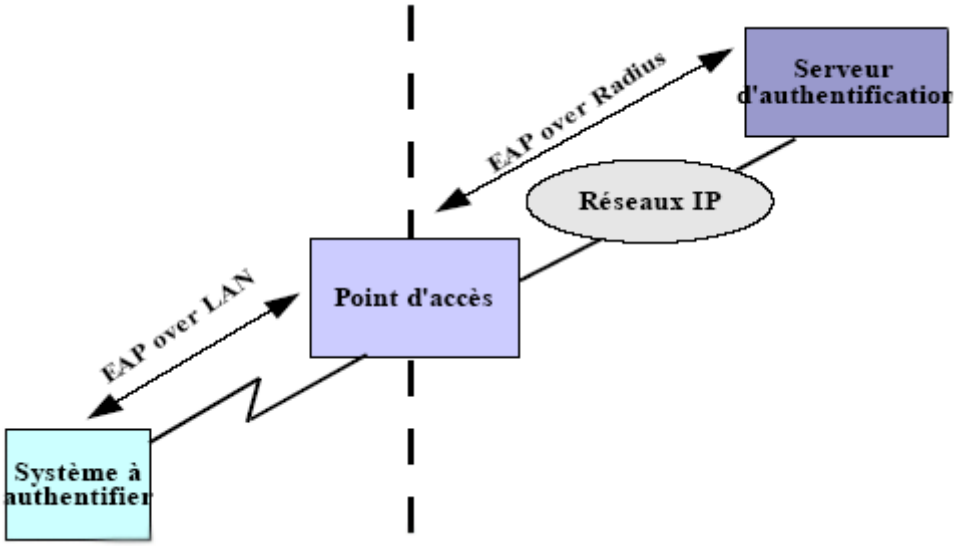
Ce protocole présente des trous de sécurité à considérer et est déconseillé par de nombreuses firme (Cisco, WiFi-Alliance, WiFi-Security, …).

4.3. Techniques Complémentaires

Après avoir constaté les faiblesses de la sécurité du 802.11b, plusieurs autres techniques on vu le jour. Certaines ont été développées à la va-vite pour combler le manque de sécurité du 802.11b et sont par conséquent temporaires. D'autres sont développées et étudiées depuis plusieurs années et tendent à devenir des standards.

4.3.1. Protocole EAP

Le protocole **EAP** *(Extensible Authentication Protocol)* est une extension du protocole **PPP** *(Point-to-Point Protocol).* Le protocole **EAP** a été développé pour répondre à la demande croissante pour une authentification des utilisateurs d'accès distant employant d'autres périphériques de sécurité.



EAP agit comme un mécanisme d'authentification arbitraire permettant de valider une connexion d'accès distant. Le modèle d'authentification utilisé est négocié par le client d'accès distant et le responsable de l'authentification (soit le serveur **IAS** *(Internet Authentication Service))*. Vous pouvez utiliser **EAP** pour prendre en charge les modèles d'authentification tels que Generic Token Card, **MD5**-Challenge, **TLS** *(Transport Level Security)* pour la gestion des cartes à puce, S/Key, ainsi que toutes les autres et futures technologies d'authentification.

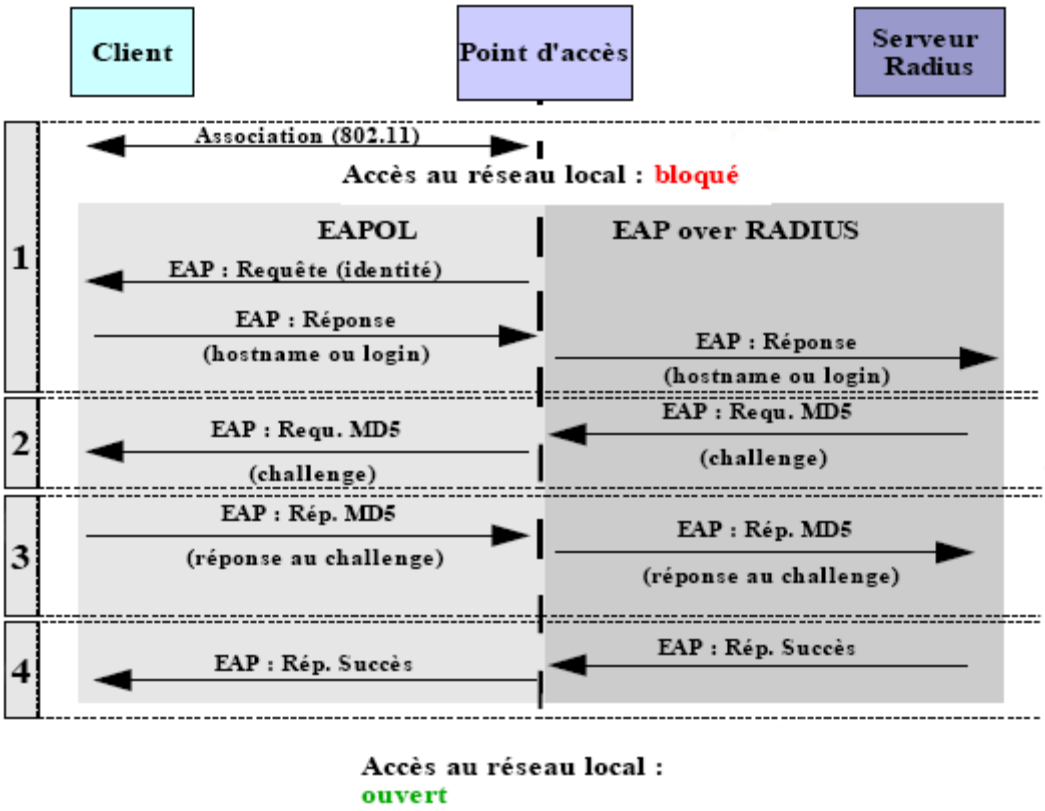
EAP permet une conversation évolutive entre le client d'accès distant et le responsable de l'authentification. La conversation est composée de demandes en informations d'authentification, émanant du responsable de l'authentification, et de réponses provenant du client d'accès distant. Par exemple, lorsque **EAP** est utilisé avec des cartes à jeton de sécurité, le responsable de l'authentification peut demander au client d'accès un nom, un code confidentiel et un jeton de carte pris individuellement. Après chaque question et réponse, le client d'accès distant passe au niveau suivant d'authentification. Lorsque toutes les questions ont fait l'objet d'une réponse satisfaisante, le client d'accès distant est authentifié.
Un modèle d'authentification **EAP** spécifique s'appelle un type **EAP**. Le client d'accès distant et le responsable de l'authentification doivent tous les deux prendre en charge le même type **EAP** pour que l'authentification soit réussie.

a. EAP-MD5 CHAP

Le protocole **EAP-MD5 CHAP** *(EAP-Message Digest 5 Challenge Handshake Authentication Protocol)* est un type **EAP** obligatoire qui utilise le même protocole de défi/réponse que **CHAP PPP**, mais les défis et les réponses sont envoyées sous forme de messages **EAP**.

EAP-MD5 CHAP est généralement utilisé pour authentifier les informations d'identification des clients d'accès distant, à l'aide d'un système de sécurité basé sur le nom d'utilisateur et le mot de passe. Vous pouvez également utiliser **EAP-MD5 CHAP** pour tester l'interopérabilité de **EAP**.

*** voir page suivante pour schéma**



1. Après l'association et la phase **EAP** standard de demande d'identification, le serveur émet une requête **EAP-MD5** sous forme d'un texte de défi ou *challenge text* (2).

3) Le client doit répondre à cette requête en chiffrant le défi avec son mot de passe.

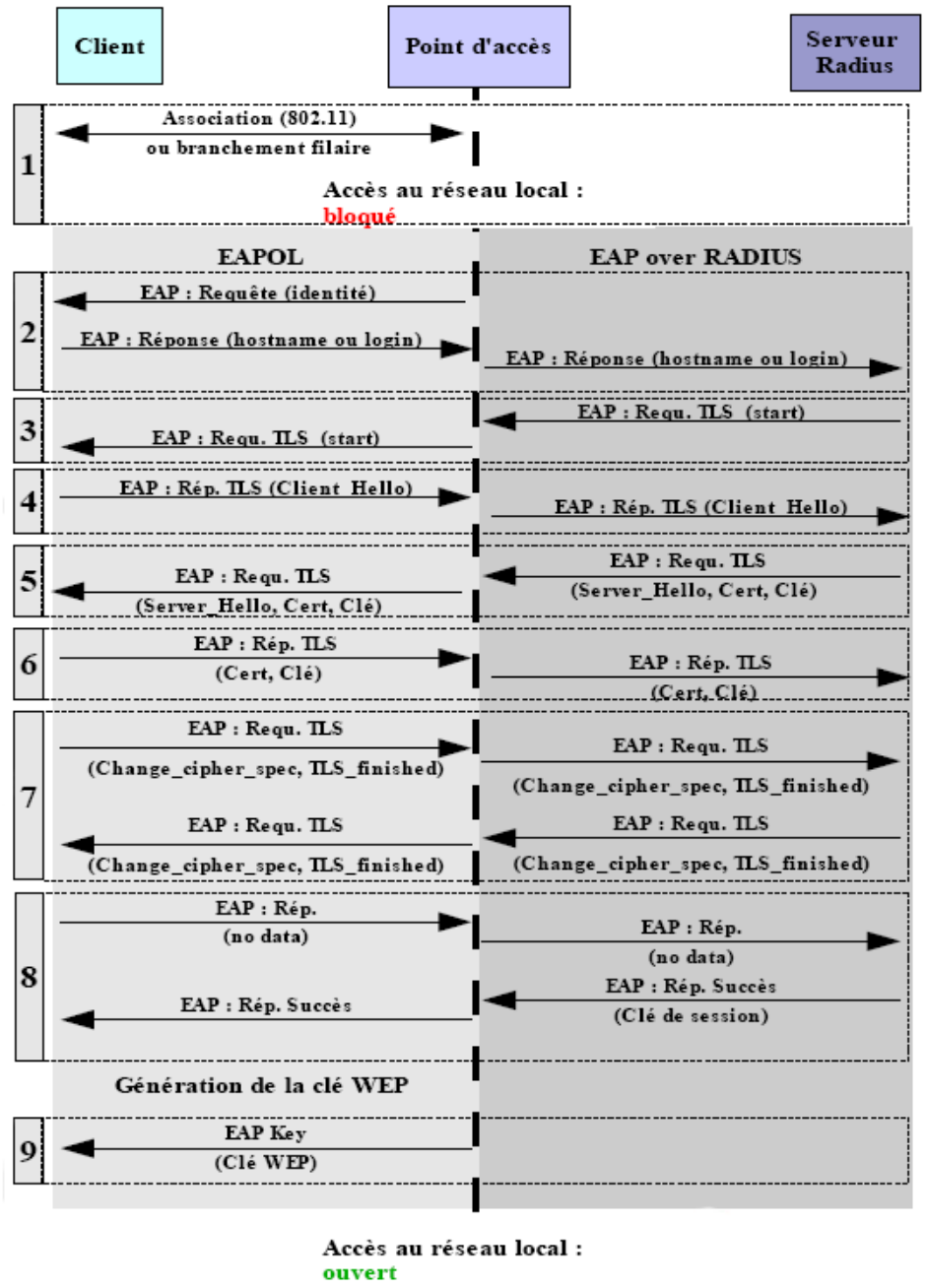
4) Le serveur chiffre le défi de son côté en utilisant le mot de passe du client stocké dans sa base. Si le résultat coïncide, le client est authentifié.

Il est très important de noter que les échanges sont non chiffrés. Le *challenge text* et son résultat chiffré transitent en clair sur le réseau.

Ce protocole est vulnérable aux attaques du type dictionnaires, « man-in-the-middle » et usurpation de session. Il est cependant facile à implémenter ce qui en fait probablement son seul avantage. Il est habituellement utilisé pour des réseaux filaires où la contrainte liée au chiffrage des échanges est moins forte que pour les réseaux **Wifi**.

b. EAP-TLS

EAP-TLS (**EAP**-Transport Level Security) est un type **EAP** utilisé dans les environnements de sécurité reposant sur les certificats. Si vous utilisez des cartes à puce pour l'authentification d'accès distant, vous devez utiliser la méthode d'authentification **EAP-TLS**. L'échange de messages **EAP-TLS** offre une authentification mutuelle, une négociation commune de la méthode de cryptage, et un échange sécurisé des clés privées entre le client d'accès distant et le responsable de l'authentification. **EAP-TLS** offre la méthode d'authentification et d'échange de clés la plus sûre.



1. Le client s'associe physiquement au point d'accès.

2. Le point d'accès envoie une requête d'authentification au client. Le client répond avec son identifiant (nom de machine ou login), ce message est relayé par le point d'accès vers le serveur Radius.

3. Le serveur Radius initie le processus d'authentification **TLS** par le message *TLS start*.

4. Le client répond avec un message *client_hello*, qui contient des spécifications de chiffrement vides en attendant qu'elles soient négociées entre client et serveur, la version **TLS** du client, un nombre aléatoire (défi ou *challenge*), un identifiant de session et les types d'algorithmes de chiffrement supportés par le client.

5. Le serveur renvoie une requête contenant un message *server_hello* suivi de son certificat (*x509*) et de sa clé publique, de la demande du certificat du client, d'un nombre aléatoire (défi ou *challenge*) et d'un identifiant de session (en fonction de celui proposé par le client).
Le serveur choisit un algorithme de chiffrement parmi ceux qui lui ont été proposés par le client.

6) Le client vérifie le certificat du serveur et répond avec son propre certificat et sa clé publique.

7) Le serveur et le client, chacun de son côté, définissent une clé de chiffrement principale utilisée pour la session. Cette clé est dérivée des valeurs aléatoires que se sont échangées le client et le serveur. Les messages *change_cipher_spec* indiquent la prise en compte du changement de clé. Le message *TLS_finished* termine la phase d'authentification **TLS** (*TLS handshake*), dans le cas **d'EAP-TLS** la clé de session ne sert pas à chiffrer les échanges suivants.

8) Si le client a pu vérifier l'identité du serveur (avec le certificat et la clé publique), il renvoie une réponse EAP sans donnée. Le serveur retourne une réponse *EAP success*.

9) La clé de session générée en (8) est réutilisée par le point d'accès pour créer une clé **WEP** qui est transmise au client, dans le cas où il s'agit d'une station **Wifi**. La clé de session est valide jusqu'à ce que le client se déconnecte ou que son authentification expire, auquel cas il doit s'identifier à nouveau.

Cette méthode offre une sécurité robuste pour l'authentification. Mais requiert des certificats client et (à mon expérience) beaucoup de maintenance.

c. EAP-TTLS et EAP-PEAP

EAP-TTLS *(Tunneled Transport Layer Security)* est la version **EAP** signée par l'éditeur Funk ; elle est prise en charge sur ses produits Odyssey ou Steel-Belted **RADIUS** Server, ainsi que sur des logiciels clients tiers, tels que ceux proposés par **MDC**.

EAP-PEAP *(Protected Extensible Authentication Protocol)* est un protocol développé en collaboration par Microsoft, RSA Security et Cisco pour la transmission de données d'authentification (utilisateur et mot de passe) sur un réseau 802.11.

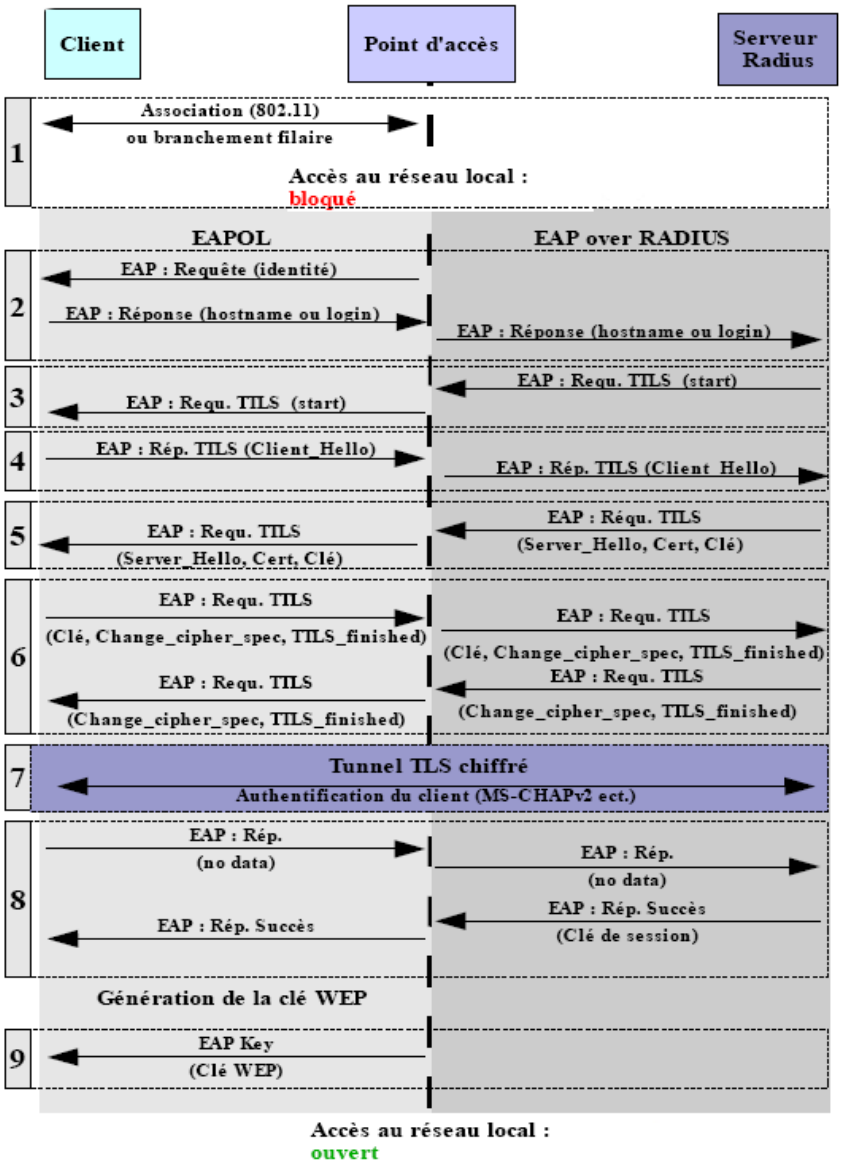
Tout comme **TTLS**, **PEAP** authentifie les clients en utilisant uniquement des certificats **PKI** du côté serveur et non sur les postes clients.

Ces deux méthodes s'appuient sur la confidentialité proposée par l'encapsulation dans un tunnel pour réaliser une authentification via login/mot de passe ou *token-card*.
On distingue deux phases d'authentification :

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

À l'issue de la première phase, le tunnel **TLS** chiffré s'établit, garantissant une grande confidentialité des échanges pour la phase 2 où le client transmet ses éléments d'authentification (login/password) via ***CHAP***, ***PAP***, ***MS-CHAP*** ou ***MS-CHAPv2***.

La différence principale entre **EAP-PEAP** et **EAP-TTLS** vient de la manière d'encapsuler les échanges lors de la deuxième phase. Pour **EAP-PEAP**, les données échangées entre le client et le serveur au travers du tunnel **TLS** sont encapsulées dans des paquets **EAP**. **EAP-TTLS** utilise des **AVP** *(Attribute-Values Pairs)* encapsulées dans des paquets **EAP-TTLS**, le format **AVP d'EAP-TTLS** est compatible avec le format **AVP** de Radius, ce qui simplifie les échanges entre le serveur **EAP-TTLS** et le serveur Radius qui contient les informations relatives aux utilisateurs, dans le cas où les informations ne sont pas directement stockées sur le serveur **EAP-TTLS**. La méthode **EAP-PEAP** ne peut-être utilisée qu'avec un serveur Radius supportant **EAP** (figure 5). **EAP-TTLS** est plus souple, il est toujours nécessaire de dialoguer avec un serveur **EAP**, cependant ce serveur peut retransmettre directement la requête auprès d'un serveur Radius ne gérant pas **EAP**.



1. à 5. Les échanges sont presque similaires à **EAP-TLS**. Le client authentifie le serveur par l'intermédiaire d'un certificat (étape 5).

6. Cette étape diffère légèrement **d'EAP-TLS** car le client n'a pas besoin de fournir de certificat, la clé qui sert à chiffrer la session peut donc être créée directement. À la fin de cette étape, le ***TLS** handshake* est terminé, les échanges suivants seront donc chiffrés par la clé de session.

7. L'établissement d'un tunnel **TLS** permet de chiffrer les échanges, le client fournit donc ses identifiants (login/mot de passe) au serveur en utilisant par exemple ***MS-CHAPv2*.**

8. et 9. Similaires à EAP-TLS

Cette solution est généralement considérée comme presque aussi sûre qu'**EAP-TLS**, tout en simplifiant le déploiement (pas de certificats client). . **EAP-PEAP** présente l'avantage d'être supporté nativement par Windows XP et 2000.

d. EAP-LEAP

Cisco a été l'un des premiers fournisseurs à proposer, en décembre 2000, un produit doté de son "standard" **LEAP** *(Lightweight EAP)*. Il s'agit d'une solution propriétaire qui ne fonctionnait initialement qu'avec les cartes Cisco clients 802.11, les serveurs **RADIUS** et les points d'accès Cisco. L'équipementier s'est récemment associé à d'autres fournisseurs pour assurer la compatibilité avec **LEAP** des équipements et logiciels. L'éventail de cartes PC clients 802.11 est désormais plus large, et au moins quatre autres solutions **RADIUS** prennent en charge **LEAP**. Certains fabricants d'ordinateurs portables supportent même cette solution en mode natif avec leurs adaptateurs intégrés 802.11. Heureusement, il existe des logiciels clients permettant de s'authentifier en utilisant **LEAP** avec des cartes d'autres constructeurs.

L'implémentation de **LEAP** est relativement simple. Des serveurs **ACS**/AR **RADIUS** de Cisco peuvent être aisément reliés à un domaine **LDAP** ou Active Directory et l'authentification des utilisateurs est transparente.

Par ailleurs, **LEAP** présente quelques défaillances. Tout d'abord, la clé utilisée entre le client et le point d'accès est dérivée du login et du mot de passe stockés sur le serveur Radius. La méthode utilisée dans ce cas est ***MS-CHAPv1***, connue pour être vulnérable. Ensuite, Les échanges **EAP** ne sont pas chiffrés, le login passe en clair, seul le mot de passe est protégé par le hachage ***MS-CHAPv1***. Et finalement, **LEAP** est vulnérable à des attaques de types dictionnaires.

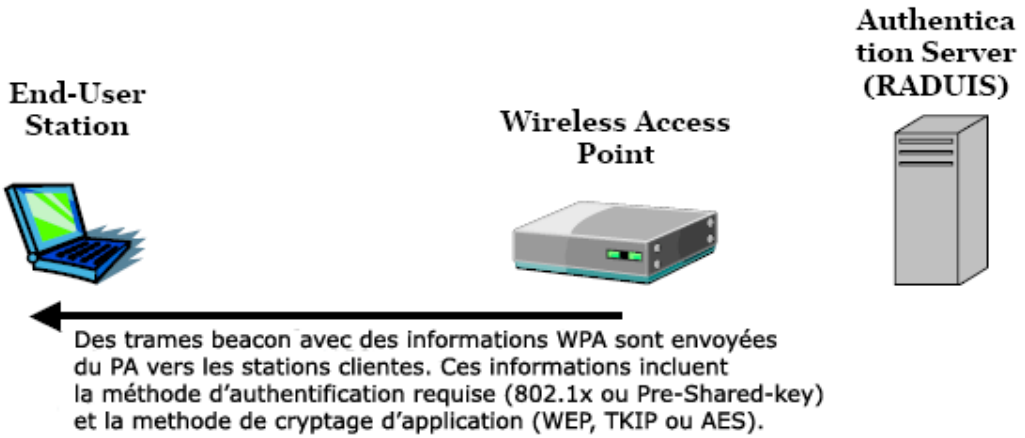
e. Autres type EAP

Il existe bien d’autres types EAP à savoir, EAP-SRP, EAP-SIM, EAP-AKA, etc. Cependant, ils n’ont aucun rapport avec le 802.11.

4.3.2. WPA

C'est en Octobre 2002 que la Wi-Fi Alliance annonçait une solution de sécurité contre les failles du **WEP** appelée **WPA** *(Wi-Fi Protected Access)*. **WPA** a été développé pour être compatible avec la norme 802.11 existante et avec la future norme 802.11i. **WPA** utilise le protocole de cryptage de données **TKIP** *(Temporal Key Integrity Protocol)* en plus de l'authentification par utilisateur avec 802.1x (voir chapitre 3.6.3.3. pour détails sur 802.1x) et **EAP**.

TKIP consiste à régénérer de nouvelles clés pour chaque paquet de 10Ko de données alors que le **WEP** lui utilisait un système basé sur une clé fixe. Cependant, l'algorithme de chiffrement des données reste le même (RC4), seul la gestion dynamique de clé a été implémentée. **TKIP** inclus aussi la gestion de l'intégrité des messages grâce au **MIC** *(Message Integrity Code)* qui est placé à la fin de chaque message pour éviter toutes possibilités de spoofing.



WPA peut être implémenté chez soi ou dans de petite entreprises qui n'ont pas de serveur Radius. Toutefois, **WPA** est bien plus puissant quand il est déployé en suivant le modèle que décrit la norme 802.1x/**EAP** qui implique des stations clientes, un ou plusieurs **PA** et un serveur d'authentification (radius).

4.3.3. 802.1x

Le 802.1x est une norme **IEEE** *(Std 802.1X-2001 Port-Based Network Access Control)* qui concerne tous les réseaux 802 et pas uniquement les réseaux sans fil.

Les réseaux locaux sont souvent déployés dans un environnement qui pourrait permettre à un équipement non autorisés de s'attacher à l'infrastructure réseau, ou de permettre à des utilisateurs non autorisés d'accéder au réseau à travers des équipements déjà présents.

Elle spécifie donc une méthode de déploiement pour garantir l'authentification et l'autorisation grâce au protocole **EAP** (définit aussi les différentes types) et un protocole d'administration **SNMP** *(Simple Network Management Protocol)*