Exposé :

Sécurité des réseaux Sans Fil

Standard WiFi

Promotion 2010-2011

1. Introduction :

Aujourd’hui, la majorité des ordinateurs et la quasi-totalité des appareils « mobiles » (tel que les téléphones portables, agendas électroniques, etc.) disposent de moyens de connexion ou plusieurs types de réseaux sans fil comme le Wifi, le Bluetooth ou l’Infrarouge. Ainsi, il est tr facile de créer en quelques minutes un réseau « sans fil » permettant à tous ces appareils de communiquer entre eux.

Or, avant de déployer ces technologies, il est nécessaire de s’informer sur les technologi utilisées et sur les mesures de sécurité indispensables à respecter. En effet, sans ce savoir faire sans prendre les mesures de protection utiles, le risque est grand d’ouvrir sans s’en rendre com son réseau à des personnes malintentionnées.

Dans le cadre de cet exposé, nous allons nous intéressés au type de réseaux Wi-Fi et principalement à sa sécurité, Nous aborderons ainsi les différentes normes de Wi-Fi existantes, équipements utilisés, la technologie employée et les précautions nécessaires à prendre pour sécuriser son réseau.

2. Présentation du Wifi :

Qu’est ce que le Wi-Fi ?

Pratiquement inconnu, il y a encore quelques années, les réseaux sans fil (Wi-Fi™) sont, aujourd’hui, omniprésents dans notre société.

Wi-Fi est l'abréviation de Wireless Fidelity. Wi-Fi correspond initialement au nom donnée à certification délivrée par la Wi-Fi Alliance, anciennement WECA (Wireless Ethernet Compatibilit Alliance), l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la 802.11. Par abus de langage (et pour des raisons de marketing) le nom de la norme se confond aujourd'hui avec le nom de la certification. Ainsi un réseau Wifi est en réalité un réseau répond la norme 802.11 qui permet de supprimer les câbles et de résoudre les problèmes de distances d’obstacles.

Cependant, pour communiquer sur ces réseaux, les ordinateurs, les modems et les périphériques doivent être équipés de récepteurs/émetteurs Wi-Fi. Ils se présentent sous plusi formes : carte PCI Wifi, ou PCMCIA Wifi pour les ordinateurs portables.

Le mot « Wi-Fi », avec le W et le F majuscules, signifie la compatibilité avec les spécifica d’interopérabilité 802.11 de la WECA (on le trouve aussi écrit tout en majuscule). Il est représe par le logo

Sur un équipement que l’on souhaite acheter, le logo Wi-Fi blanc et noir, ou la mention d standard « IEEE 802.11 », garantit que le matériel est compatible avec la technique de réseau « IEEE 802.11 ».

Aujourd’hui, compte-tenu de l’évolution de la norme 802.11, il est prudent de vérifier qu standard respecte un équipement : 802.11b, 802.11g ou bien 802.11n. Le logo Wi-Fi avec un ro noir en arrière plan

ZONE

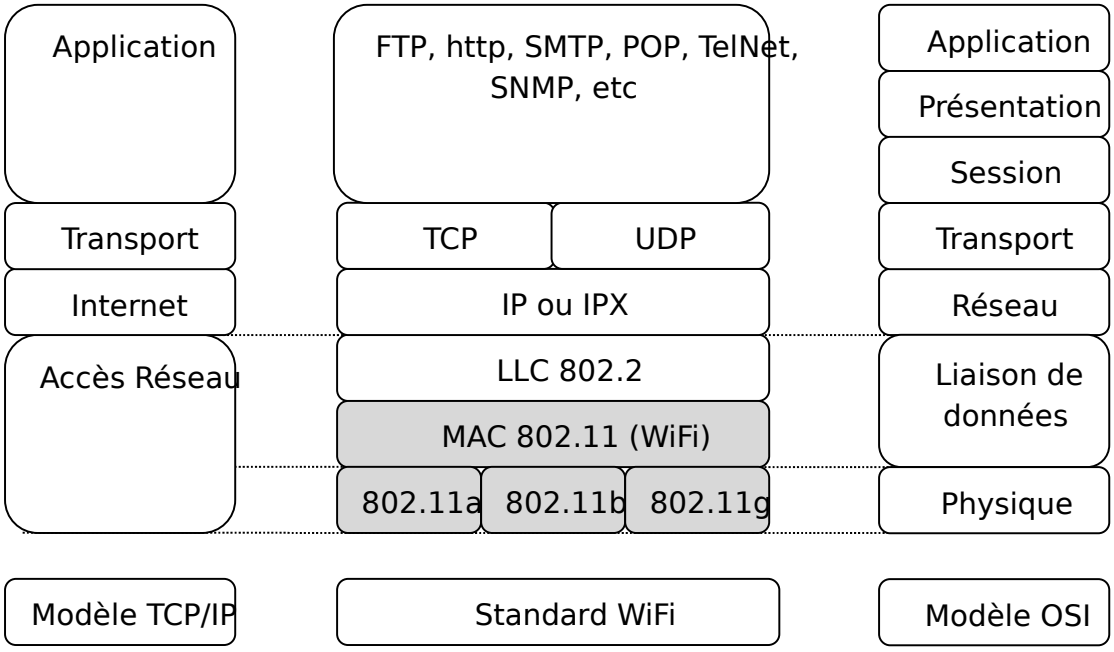
Signifie que l’on se trouve dans une zone de réseau Wi-Fi « IEEE 802.11 ».

La premier version du 802.11, publiée en 1997, s'appelée simplement 802.11, aujourd'h
appelée 802.11Legacy (802.11Hérité) définie 3 couches physiques :

- Une sur infrarouge. (elle n'a pas connue le succès, car de meilleurs produits bas
  sur l'infrarouge est standardisés par IrDA existaient déjà)
- Deux sur les ondes Radio (2.4Ghz de fréquence). Une sur DSSS et l'autre sur FH

Et il définit une couche MAC (Couche 2 du modèle OSI) Media Access Control :

3. Analogie au modèle OSI et TCP/IP et situation du standard Wifi



Les couches réseaux

4. Fonctionnement du Wifi :

4.1. Introduction

Si vous prenez le temps de bien maîtriser les aspects les plus techniques du WiFi, vous pourrez plus facilement choisir le matériel le mieux adapté à vos besoins, optimiser votre réseau résoudre certains problèmes qui pourraient survenir dans la vie de votre réseau sans fil. Et surt vous pourrez localiser les aspects liés à la sécurité du votre réseau WiFi.

4.2. La norme 802.11 : couches physiques.

Cette couche correspond à la physique du modèle OSI, elle se charge de coordonner l'acc la couche physique. Elle définit en particulier comment plusieurs périphériques devront partag temps de parole sur les ondes radios, comment un périphérique doit se connecter (on dit « s'associer ») à un réseau sans fil et également comment sécuriser les donnes échangées.

4.2.1. La modulation du Wifi

Pour échanger des informations, les équipements WiFi génèrent des ondes Radios qui transportent des informations. Ces ondes sont générées (**modulées**) d'une station et aboutiss dans les antennes des autres Radio qui finira par les **démodulées** pour extraire les informatio modulation de la norme Wifi repose sur les modulations suivantes : FHSS, DSSS et OFDM.

Toutes ces variations du Wifi découpent la bande de fréquence sur laquelle elles reposent (2.4Ghz ou 5Ghz) en canaux.

4.2.2. Sécurité et droit d'utilisation d'une fréquence en Algérie :

La régulation des fréquences est nécessaire pour éviter les brouilleurs et l'anarchie ou la pollution des ondes électromagnétiques dans un territoire, et permettre le partage équitable d ondes radios et de limiter leur impact sur la santé. Un organisme, souvent étatique, gère l'attri de ces fréquences.

En Algérie, Ces ondes Electromagnétiques sont gérées par l'organisme ARPT (Autorité de Régulation de la Poste et de Télécommunications)[1]. Si vous voulez exploiter une bande de fréquence pour élaborer votre réseau vous devez procurer une « autorisation d'exploitation ».

a. Conditions d'exploitation telles que défini par ARPT :

Les conditions techniques et d'exploitation du réseau radioélectrique privé sont définies par un "Autorisation d'exploitation" délivrée au permissionnaire.

- L'organisme demandeur ne peut procéder à l'exploitation de son réseau radioélectrique qu'a obtention de l'autorisation d'exploitation.

[1] http://www.arpt.dz/4Auto_reseau_radio.htm

- Seules les fréquences assignées par l'Autorité de Régulation de la Poste et des Télécommuni
sont autorisées à l'exploitation de réseau(x) radioélectrique(s).

b. Acquittement des redevances

- L'assignation des fréquences radioélectriques est soumise au paiement des redevances déterminées par voie réglementaire.
- Les redevances d'assignation des fréquences radioélectriques sont annuelles et sont due pendant toute la durée de validité de l'autorisation. La période d'exigibilité commence à date d'établissement de l'autorisation d'exploitation.

c. Lois de réglementation :

Extrait du:

Décret exécutif n° 09-410 du 23 Dhou El Hidja 1430 correspondant au 10 décembre 2009 fixan
règles de sécurité applicables aux activités portant sur les équipements sensibles.

CHAPITRE I
DISPOSITIONS GENERALES

Article 1er : Le présent décret a pour objet de fixer les règles de sécurité applicables aux activités portant sur les équipements sensibles, ainsi que les conditions et modalités d'exercice ces activités.

Art. 2 : Au sens du présent décret, on entend par «équipements sensibles» tous matériel dont l'utilisation illicite peut porter atteinte à la sécurité nationale et à l'ordre public.

La liste des équipements sensibles est fixée à l'**annexe I** du présent décret. Elle peut être actualisée par arrêté conjoint des ministres chargés de la défense nationale, de l.intérieur, des transports et des technologies de l'information et de la communication.

ANNEXE I
I. - SECTION « A » : Les équipements sensibles de télécommunications.
Sous-section 1 : Les équipements de télécommunications nécessitant l'assignation ou l'attrib gammes de fréquences :

Paragraphe 2- Tout équipement pouvant rayonner de l'énergie électromagnétique dans l'espa libre des spectres des fréquences radioélectriques, y compris les appareils de faible puissance faible portée (**Wifi**) et notamment les prolongateurs de lignes téléphoniques dits « Cordless ».

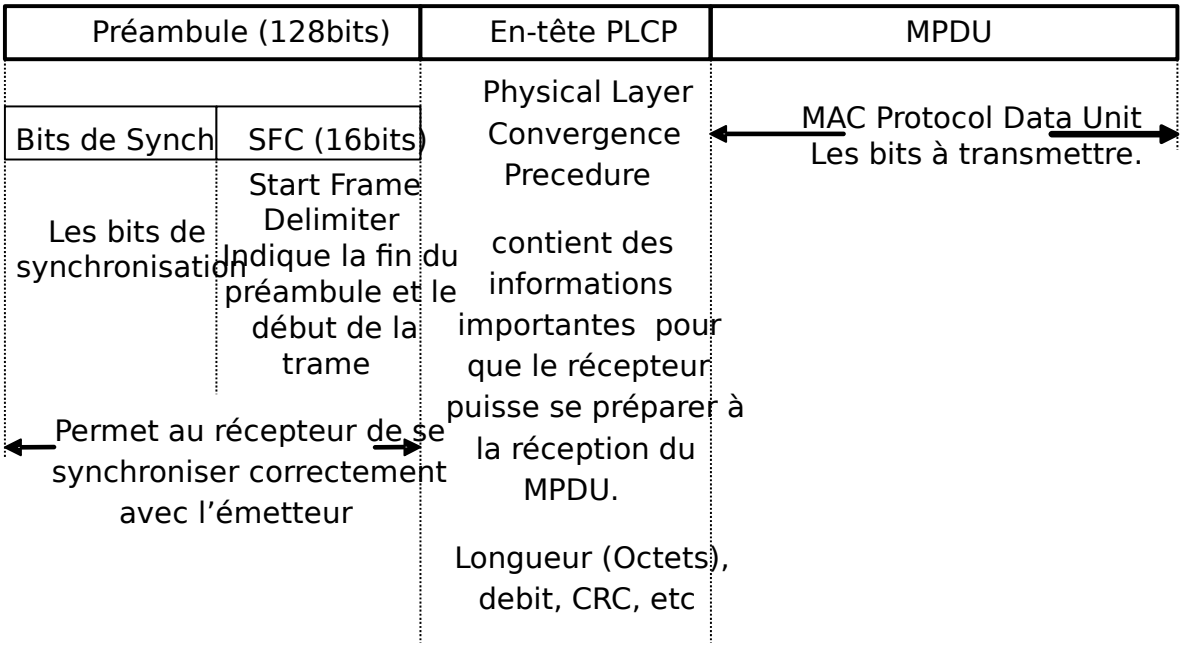
Pour plus de renseignements consulter le site :

http://www.joradp.dz/FTP/Jo-Francais/2009/F2009073.zip

4.2.3. Les trames 802.11 :

Les données à transmettre sur les ondes sont encapsulées dans une Trame. Cette trame e
générée au niveau de la couche MAC.

Format Trame 802.11 :



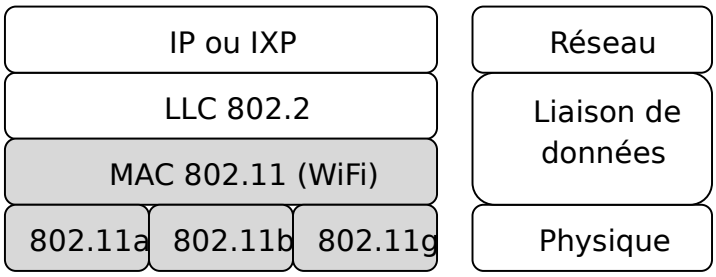
NB L'en-tête PLCP est toujours transmis à 1Mb/s, quelle que soit la couche physique utili
et le débit peut augmenter pour la transmission du MPDU.

NB 802.11 a défini un format de synchronisation plus court (56 bits), préambule court (Sh
Preamble) certains produits sont configurés avec le préambule court par défaut ! Donc si vous
comprenez pas pourquoi votre adaptateur ne détecte pas votre point d'accès (AP), vérifié bien
utilisent le même préambule : ce sera souvent la réponse à votre problème.

Configurer votre matériel Wifi qu'il utilise un préambule court peut améliorer la performance d
votre réseau. Toutefois, il faut vous assurer que tous les équipements sachent le gérer.

4.3. La norme 802.11 : couche MAC.

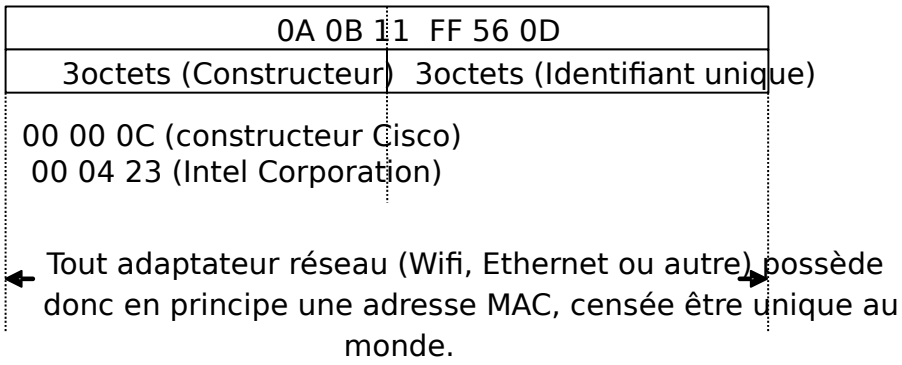
4.3.1 Présentation de la couche LLC et MAC :



L'IEEE a divisé la couche **liaison de données du modèle OSI** en deux couches : la couc
contrôle de la liaison logique (**Logical Link Control, LLC**) et la couche de contrôle d'accès au
(MAC).La couche LLC permet aux protocoles réseaux de niveau 3 (Par exemple IP) de reposer s
couche unique (la couche LLC) quel que soit le protocole sous-jacent utilisé, dont le Wifi, Ethern
le TokenRing, par exemple. L'en-tête d'un paquet LLC indique le type du protocole IP, mais cela
pourrait être un autre protocole, comme IPX (Internet Packet Exchange) par exemple.

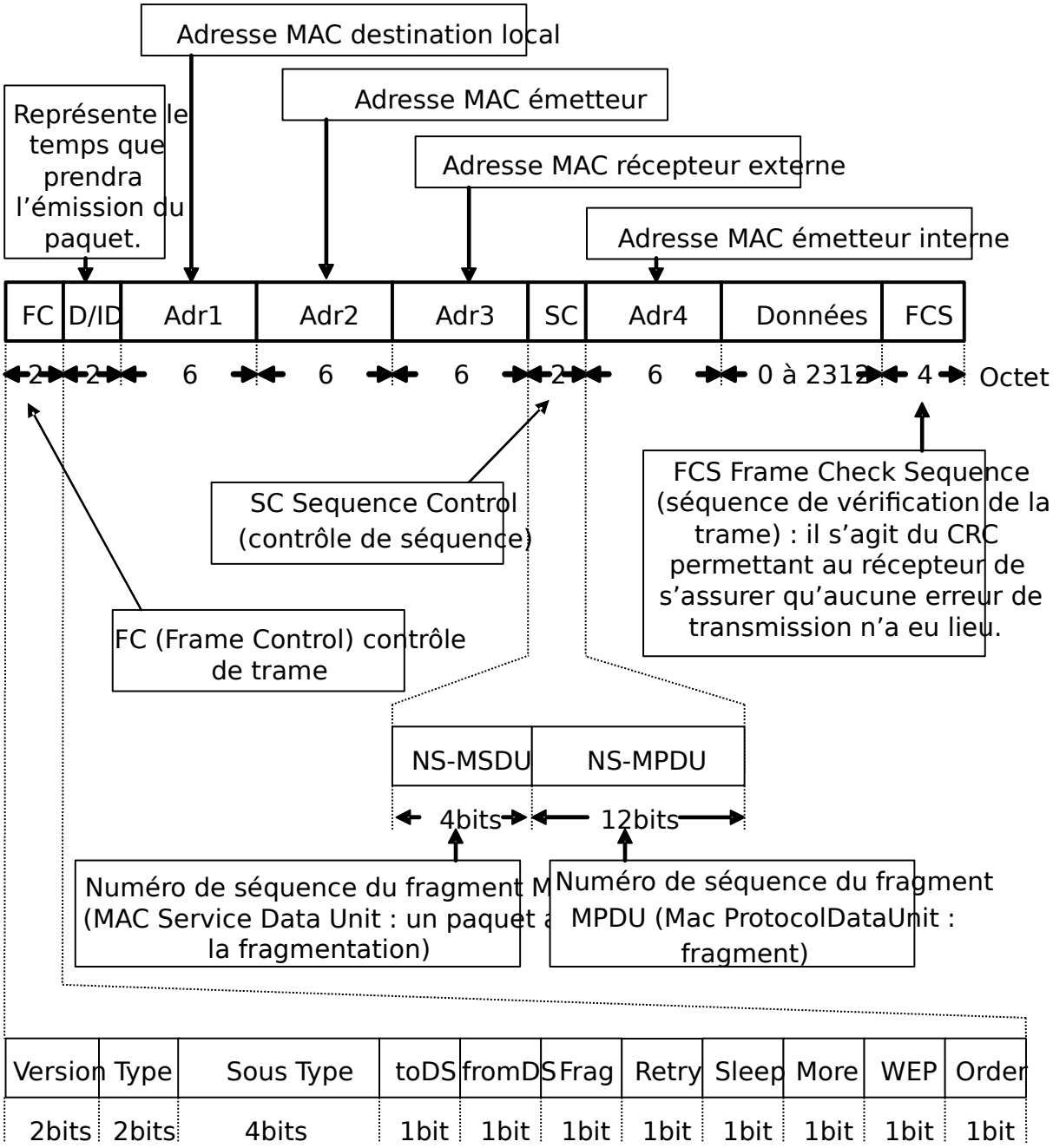
La couche de contrôle d'accès au media (MAC Media Access Control) permet de définir comment différents utilisateurs doivent se partager la parole, le format des paquets échangés, topologies possibles, les modalités exactes de connexions à un réseau sans fil (on parle d'asso et elle va même plus loin en définissant des fonctionnalités avancés telles que la sécurité des communications, l'économie d'énergie, le contrôle d'erreur ou encore comment assurer une bo qualité de service, en particulier pour les communications multimédias. La couche MAC est do quelque sorte le cerveau du Wifi.

La couche MAC définit les adresses du réseau MAC (48bits = 6Octets)



4.3.2Les paquets Wifi :

La couche MAC du 802.11 définit le paquet WiFi comme suit :



Version Le premier champ est la version du 802.11 utilisée.

Type indique le type du paquet. Il en existe troie : paquet de gestion (association authentification,...), paquet de contrôle (RTS,CTS, ACK,CF-End,...) ou opaquet de données (donn simples, données +CF-Poll ...)

Sous-type du paquet : association, RTS, données simple, etc.

toDS , fromDS : ils servent à indiquer si le paquet s'adresse au système de distribution (t et s'il provient (fromDS).

Frag : indique s’il en reste encore des fragments après ce paquet.

Retry (nouvel essai) indique que ce paquet est une nouvelle tentative d’émission d’un paquet dejà envoyer précédemment, mais qui n’a pas reçu d’ACK en réponse.

Sleep : (Sommeil) indique si la station sera en mode économique d’énergie (PSM) ou non après ce paquet.

More (Plus): est utilisé par un AP lorsqu’il communique avec une station en mode PSM et qu’il souhaite la prévenir que d’autres paquets seront envoyés après celui-ci. Ceci permet d’évi que la station ne s’endorme trop tôt et permet également de lui indiquer quand elle peut se rendormir.

Le champ WEP indique si ce paquet est crypté avec WEP ou non.

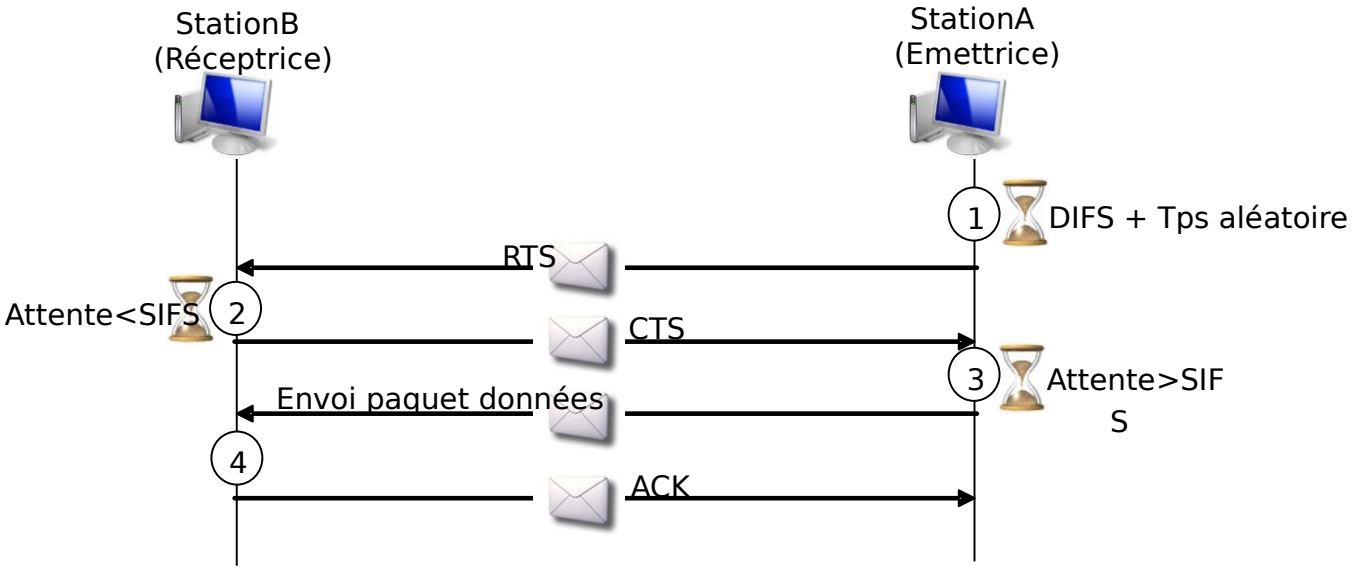
Le champ ordre indique que l’émetteur souhaite que ce paquet appartienne à la « classe service strictement ordonnée ». Les paquets appartenant à cette classe doivent toujours être r dans le même ordre qu’ils ont été reçus.

4.3.3Le partage des ondes en Wifi :

A l'instar de l'Ethernet, la couche MAC du 802.11 définit comment partager le média de communication entre plusieurs stations et la méthode la plus fréquente est très semblable au CSMA/CD de l'Ethernet. Mais contrairement à l'Ethernet, le Wifi propose plusieurs autres straté possibles.

Le mode DCF :

La première stratégie s'appelle la fonction de coordination distribuée (Distributed Coordination Function, DCF). Il s'agit d'une version améliorée du protocole CSMA with Collision Avoidance (CSMA/CA), qui est elle-même une variation du CSMA/CD.



1. La station émettrice attend un temps de silence DIFS (Distributer Inter Frame Space) suiv d'un délai d'attente supplémentaire aléatoire puis envoie un RTS (Request To Send)

2. La station réceptrice répond au RTS par un CTS (Clear To Send) pour donner son autorisation en moins du délai SIFS (Short Inter Frame Space)

3. La station émettrice attend un délai SIFS avant d'émettre le paquet.

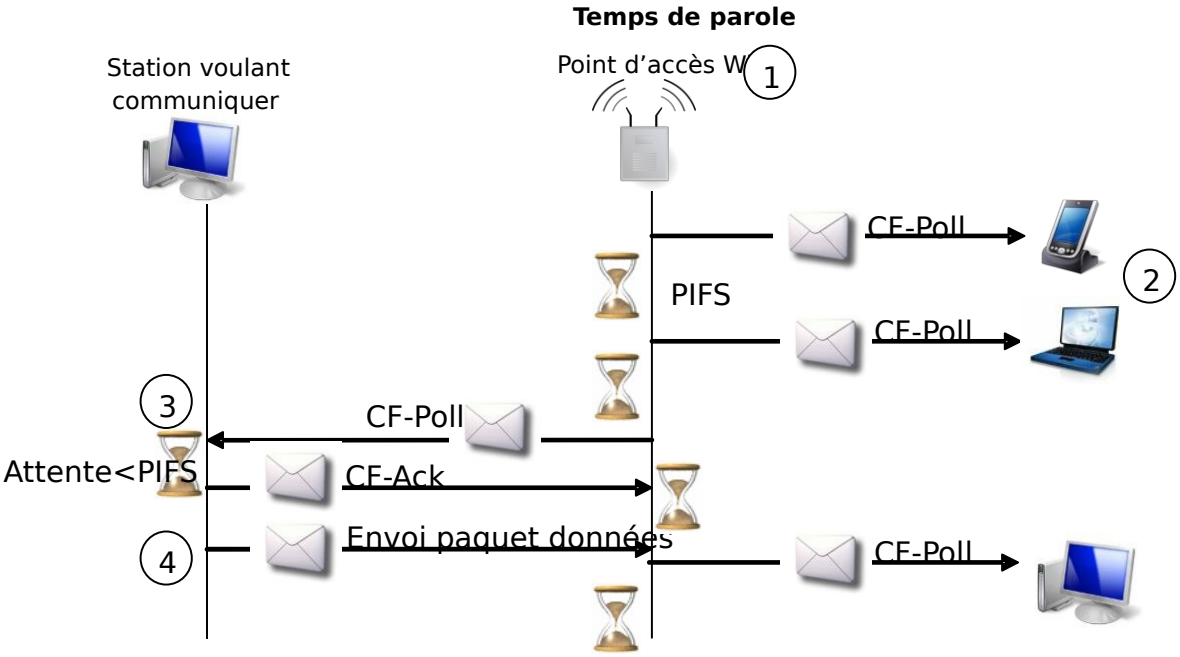
4. La station réceptrice acquitte le paquet Ack (acknowledgment).

Notons que ce mécanisme n'est valable que pour le trafic unicast : les paquets de broadc de multicast sont envoyés sans le RTS, sans CTS et sans ACK.

Avec le mécanisme RST/CTS, on peut éviter la majorité des collisions plutôt que de les dé après qu'elles aient lieu. En contrepartie, on perd une part de la bande passante avec les paqu contrôles RTS/CTS et ACK. C'est une des raisons pour lesquelles le débit réel en 802.11 est infé au débit théorique.

Le mode PCF :

La deuxième stratégie de partages des ondes d'appelle la fonction de coordination par po
(Point Coordination Function PCF). Toutes les stations sont reliées (sans fil) à un point d'accès (A
qui s'occupe de distribuer la parole à chacun. Par nature, cette stratégie n'est donc pas possibl
mode Ad Hoc. Puisqu'un AP s'occupe de distribuer la parole, il n y'a plus de collision possible et
temps de latence est donc garanti. En anglais, on dit que ce système est Contention Free (CF),
dire libre de toute dispute.



1 L'AP génère des paquets CF-Poll pour chaque station tous les PIFS (PCF Inter Frame Spac

2 La station qui ne veut pas prendre la parole il ne réponde pas au message.

3 La station qui veut prendre la parole renvoie un paquet CF-ACK. Avant la fin du PIFS.

4 La station commence à émettre ces données (1 ou plusieurs paquets) dans ce temps de

Le mode PCF permet ainsi de diviser le temps de parole plus équitablement ente les stati
et surtout de façon pus fluide et déterministe : ce mode est donc intéressant pour transférer de
données synchrones, telles que des communications multimédias. En contrepartie, une portion
importante de la bande passante peut être gâchée si de nombreuses stations n'ont rien à émet
lorsque la parole leur est donnée, les autres stations attendent, en définitive, pour rien.

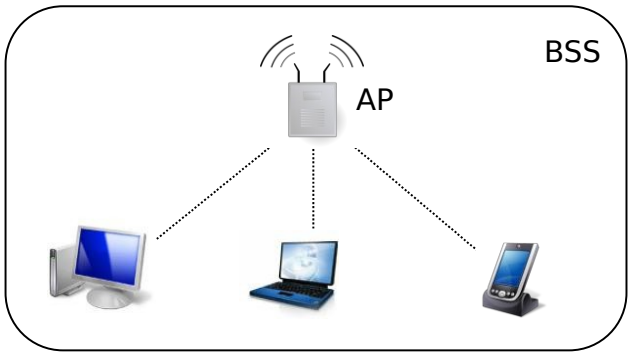
Pour limiter cela, mais aussi pour permettre aux stations incompatibles avec le PCF de
communiquer, la norme 802.11 impose que le PCF soit toujours accompagné du DCF. Pendant
quelques instants, toutes les stations sont en mode PCF et ne parlent que si l'AP auquel elles s
associées leur donne la parole, puis, pendant quelques instants, les stations prennent la parole
le mode DCF, puis on revient au mode PCF.

4.3.4Le réseau ad hoc ou infrastructure :

La couche MAC autorise l'établissement de deux types de réseaux : Les réseaux de type Infrastructure et les réseaux de type Ad hoc.

4.3.4.1. Le mode infrastructure :

Dans les réseaux de type Infrastructure, chaque périphérique est relié au réseau via un po d'accès (AP) Wifi. On dit que le périphérique est le « client » et l'AP le « maître ». Un réseau de type s'appelle un **Basic Service Set** (BSS) Et couvre un espace qu'on appelle une « cellule » c Service Area (BSA). Chaque BSS est identifié par un nombre composé de 48bits : c'est BSSID. mode Infrastructure, ce BSSID correspond tout simplement à l'adresse MAC du point d'accès.

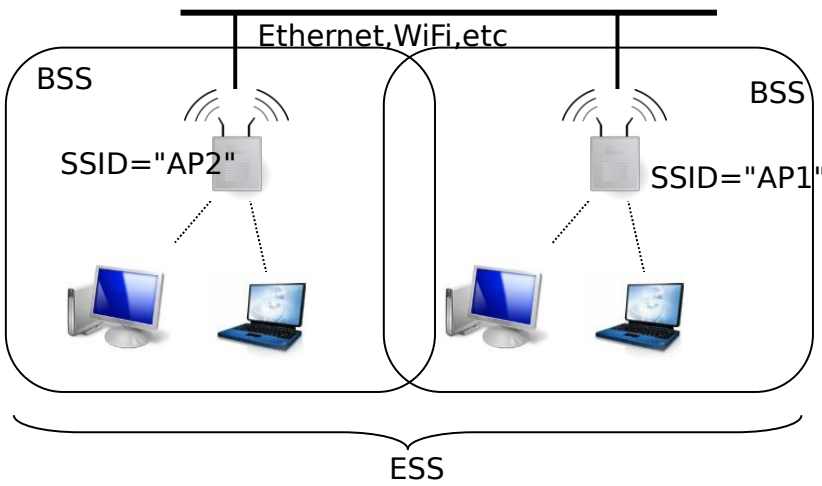


Un réseau Infrastructure composé d'une seule cellule (BSS)

Plusieurs points d'accès peuvent être déployés pour éteindre une plus large couverture W Ces BSS multiples peuvent être reliés par un système de distribution (Distribution System, DS) façon à former un unique réseau sans fil.

Le DSS peut être un réseau filaire Ethernet (cas le plus fréquent), ou une liaison sans fil ! I alors possible à un utilisateur de se déplacer dans l'ensemble de la zone de couverture sans so de ralentissement ou d'interruption de sa connexion : en cas de besoin, la liaison bascule automatiquement c'est le « hand-over » vers le point d'accès offrant la meilleure connexion.

On parle dans ce cas d'Extented Service Set (ESS) qui couvre naturellement un espace ap l'Extented Service Area (ESA), composé de plusieurs cellules. Chaque ESS est identifié par un n 32 caractères maximum qui s'appelle l'ESSID (ou simplement SSID). Il faut faire attention à ce deux ESS distincts dont les cellules se superposent aient toujours des noms (SSID) différents, s observera des problèmes de connexion importants dans les zones de superposition.

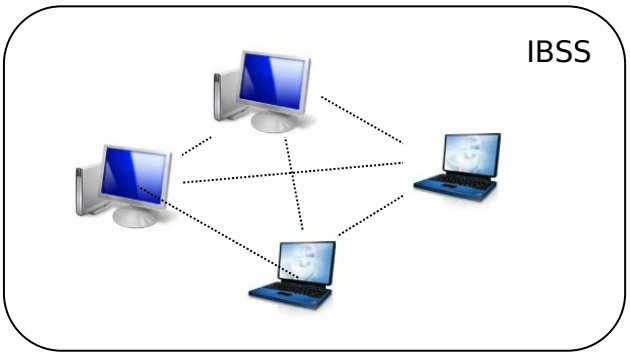


Un réseau Infrastructure composant plusieurs cellules (ESS)

4.3.4.2. Le mode Ad Hoc et les réseaux maillés :

Dans les réseaux de type Ad hoc, chaque périphérique communique directement avec les périphériques situés à sa porté, sans passer par un intermédiaire.

Ce mode est pratique pour l'échange de données entre quelques stations en l'absence d'u quelconque infrastructure réseau (aucun point d'accès). Le réseau ainsi constitué s'appelle un Independent Basic Service set(IBSS)



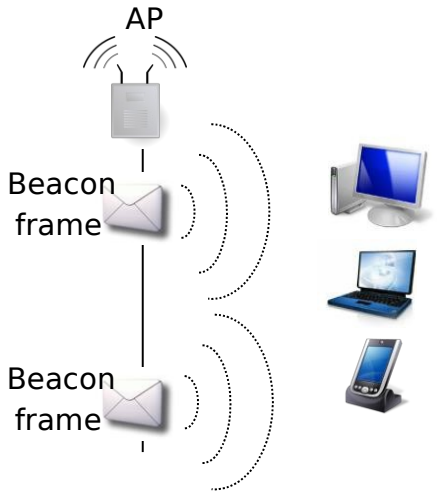
Un réseau AD Hod

4.3.5 Processus d'association

4.3.5.1. Les trames balises : Beacon frame

En mode Infrastructure, AP émet à intervalles réguliers (≈100ms) une trame balise (Beacon frame) qui contient des informations concernant l'AP (BSSID, débits, SSID).

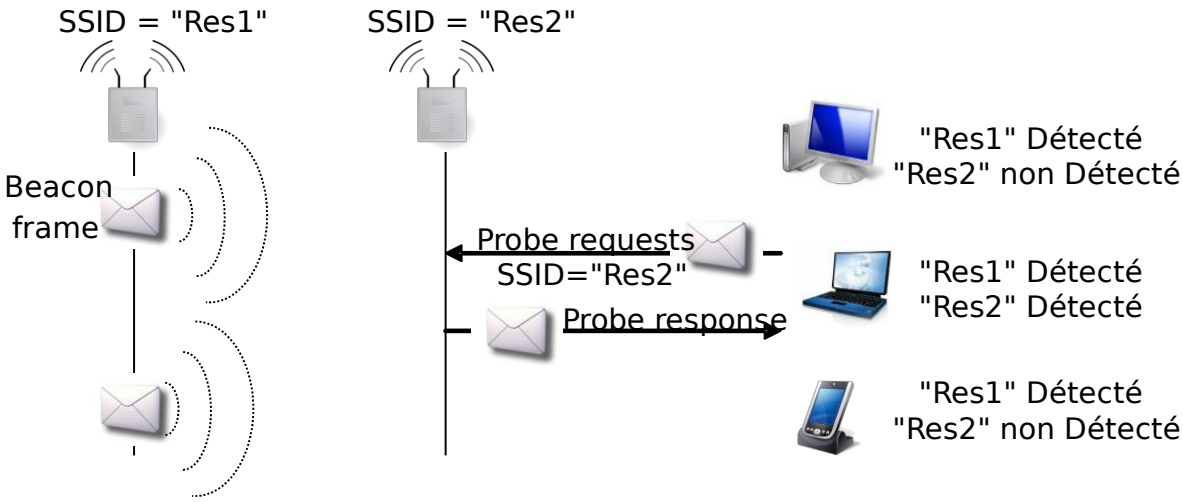
Un rôle important des trames balises est de garantir la synchronisation entre toutes les stations qui lui sont associées.



4.3.5.2. Détecter les réseaux présents :

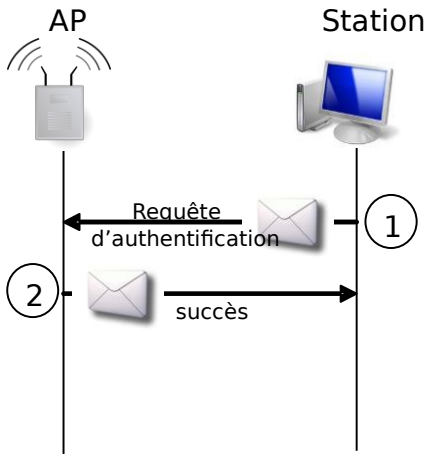
Le réseau peut être détecté seulement en recevant des Trames Balise qui contiennent le S
Ou il peut être détecté en envoyant une requête de sondage (**probe requests**) contenant le S
souhaité et les débits que le périphérique est capable de gérer.

Si un point d'accès se situe à proximité et reçoit la requête, il commence par vérifier que
SSID correspond au sien et si c'est le cas il répond avec un paquet (**probe response**) contena
près la même chose que la trame balise.

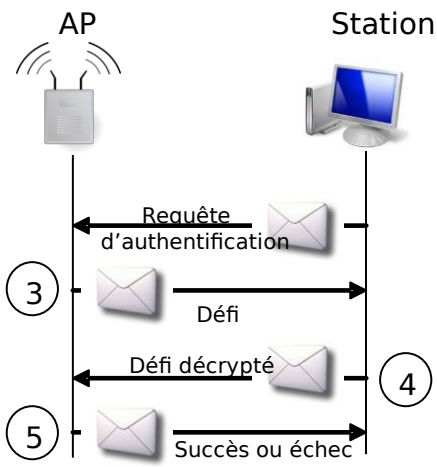


4.3.6Authentification :

Pour pouvoir communiquer sur un réseau sans fil de type Infrastructure, une station doit d'abord d'identi
auprès d'un AP avant d'y être associée. L'authentification peut être ouverte ou peut être sécurisée.



Authentification ouverte
« Open Authentication »



Authentification WEP
« Wired Equivalent Privacy »

1. La station d'identifie en envoyant une requête d'authentification contenu le SSID.
2. L'AP répond toujours positivement à ces requêtes d'authentification
3. L'AP répond en envoyant un défi (Message de 128bits crypté avec la clé WEP)
4. La station décrypte le message (si elle la clé WEP) et renvoie le Message + Message crypté
5. L'AP vérifie si le message a été décrypté avec la même clé, si c'est le cas, il accorde l'authentification.

Vulnérabilité du processus d'authentification :

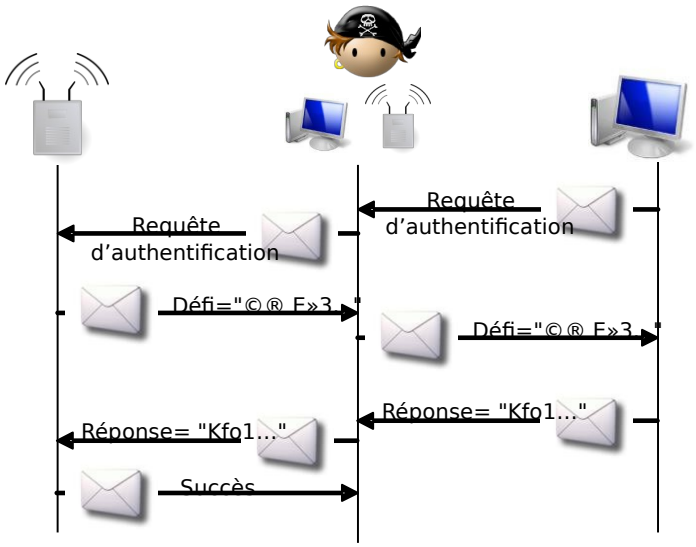
Ce précédé possède de graves défauts :

1. tout d'abord, il permet à l'AP d'identifier que la station est légitime, mais l'inverse n'est pas vrai. Au cours de l'authentification, rien ne garantit à la station qu'elle a bien affaire à un AP du réseau auquel elle souhaite s'associer.

2. Une fois l'authentification terminée, on se retrouve plus ou moins au point de départ : l'AP sait que la station dont l'adresse MAC est « x » est légitime, c'est tou Or, une adresse MAC peut facilement être imitée. « Présentation d'EtherChange »

Il suffit donc à un pirate de « sniffer » le réseau sans fil, d'attendre qu'un utilisateur légitime s'authentifie, puis de noter son adresse MAC et de configurer son adaptateur Wifi pour qu'il util cette adresse, ce que permettent certains adaptateurs.

Une autre attaque possible consiste pour le pirate à s'intercaler entre la station et l'AP : on par d'attaque MIM (Man in the Middle). Il intercepte la demande d'authentification de la station, la remplace par la sienne et l'envoie à l'AP ; ensuite il intercepte le défi de l'AP, le redirige vers la station ; enfin, il intercepte la réponse et la station et la redirige vers l'AP : de cette façon, il es authentifié sans même avoir à changer d'adresse MAC !



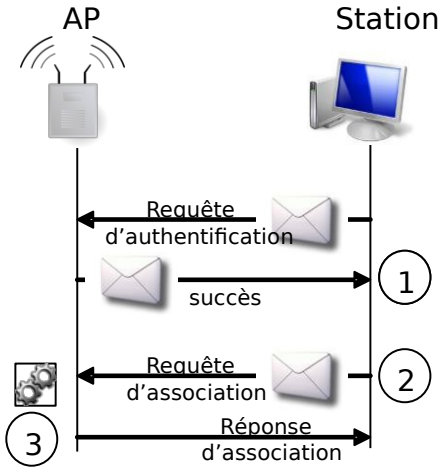
Attaque MIM

En deux mots, l'authentification 802.11 n'apporte rien. Pire, elle fournit à un pirate un exemple message en clair et sa version codée (le défi et la réponse au défi). C'est un indice de plus pou trouver la clé WEP ! Bref, malgré le fait que l'authentification WEP soit spécifiée par le standard 802.11, elle été bannie des spécifications Wifi définies par la Wi-Fi Alliance[2] (authentification ouverte).

[2] attention : seule l'authentification WEP a été éliminée. Le cryptage WEP peut être utilisé par la suite, un la station associée. Dans ce cas, il y aura une authentification implicite par la station et par l'AP.

4.3.7L’association

La station a bien été identifiée, elle peut alors s’associer à l’AP pour avoir accès aux services d
réseau. Pour cela, elle doit envoyer une requête d’association à l’AP.



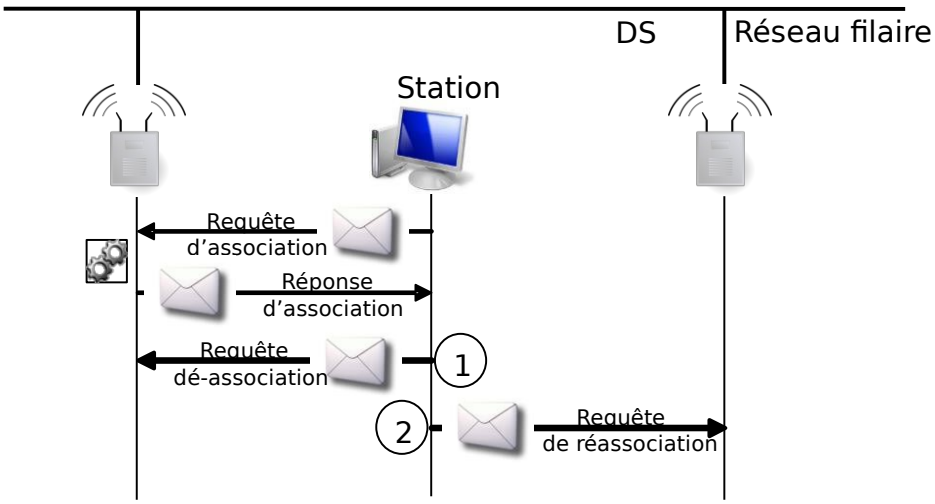
Processus d’association

1. La station a bien été identifiée (Authentification ouverte ou avec WEP)
2. La station envoie une requête d’association contenant la liste des débits qu’elle peut gé
3. L’AP alloue un identifiant d’association à la station, elle enregistre les informations de l
requêtes dans sa table des associations, enfin elle renvoie une réponse d’association p
confirmer association.

4.3.8la réassociation

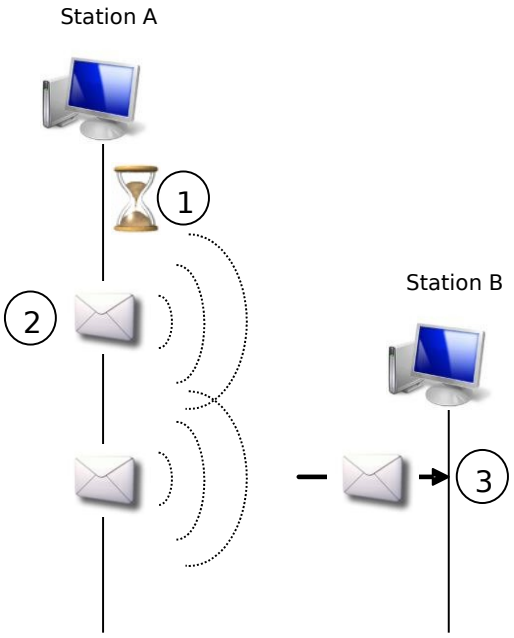
Malgré son association avec un AP donné, la station vérifie régulièrement (passivement ou activement) la présence d'autres AP ayant le même SSID. Ainsi, lorsqu'un AP s'avère plus intér (plus proche ou plus disponible), la station envoie d'abord une **requête de désassociassions** auprès de l'AP actuel suivie d'une **requête de réassociation** vers le nouvel AP.

La requête de réassociation indique entre autres l'identité de l'AP précédent. Ceci permet aux AP de se mettre en relation au travers du système de distribution (DS) pour se transmettre des informations concernant la station et pour distribuer d'éventuels paquets en attente pour la sta Tout ce processus de réassociation se déroule automatiquement, de façon complètement transparente pour les couches réseaux supérieures et pour l'utilisateur : on peut ainsi changer cellule tout en poursuivant un téléchargement, par exemple.



Processus de réassociation

4.3.9En mode Ad hoc ?



1. La station attend un certain temps et si elle ne détecte pas de balise, elle l'émet elle-même, à intervalles régu
2. Emission à intervalles réguliers.
3. La station B se joint au réseau, et elle le détecte (elle n'a pas besoin d'émettre des balises).

Pour communiquer sur le réseau, il n'est pas nécessaire de s'authentifier ou de s'associer. On p
communiquer directement, sans autre forme de procès. Le cryptage WEP peut être activé pour
crypter les échanges.

5. Mécanisme de sécurité

5.1. Masquer le SSID

Puisque toute requête d'authentification doit contenir le bon SSID, on voit qu'un premier niveau de sécurité pour un réseau WiFi consiste à simplement configurer les points d'accès pou qu'ils ne diffusent pas leur SSID. Si quelqu'un ne connait pas le SSID du réseau, il ne parviendra s'y associer. Pour un réseau d'entreprise, c'est très recommandé : il s'agit d'une action très sim qui offre déjà un premier niveau de sécurité élémentaire.

Toutefois, cette sécurité est assez faible car il suffit de sniffer les paquets de sondage env par les stations « légitimes » du réseau pour pouvoir lire « en clair » (c-à-d sans cryptage) le SS réseau. Il existe des outils très simples disponibles gratuitement (Netstumbler, Vistumbler, Poc Warrior) pour faire cela.

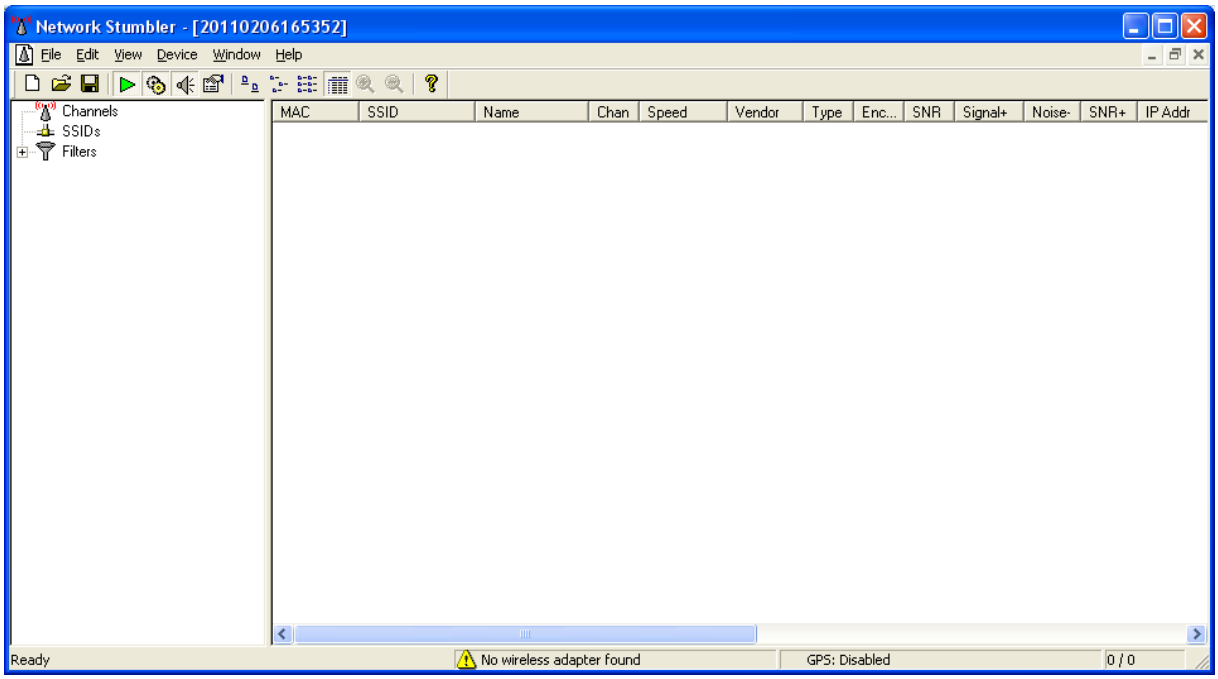
Solution(s) possible(s):

Aucune vraie solution n'existe à ce probleme, cependant une petie astuce simple à mettre place et peut en bluffer plus d'un. Elle consiste à renommer votre SSID par des « espaces », ain lieu de voir un réseau SSID de type « NomSSID », le logiciel affichera « » .

Une autre possibilité également consiste à remplacer les « » éventuellement par des astérisques (ex : « ****** »), le SSID de votre réseau sans fil sera affiché, mais donnera l'impres d'être masqué tel un mot de passe.

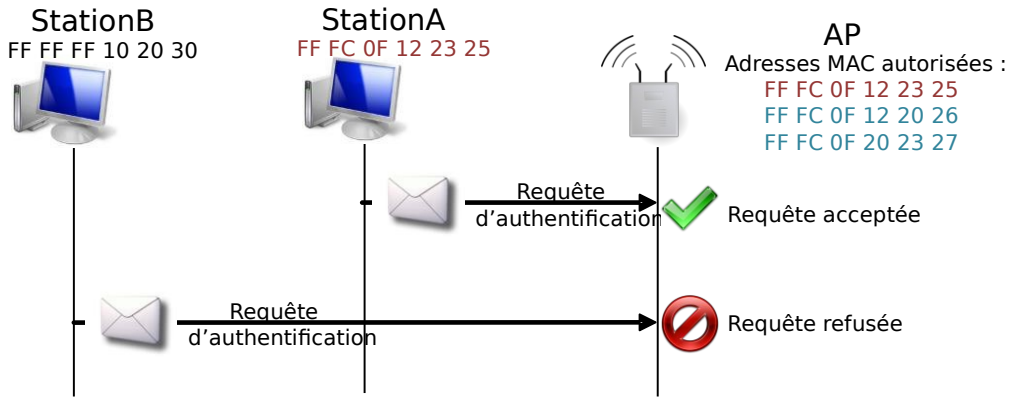
Exemple :

NetStumbler permet d'identifier et de qualifier les réseaux Wifi environnants. Chaque rése est détaillé avec un numéro du canal, un SSID, un débit, le type de périphérique Wifi (point d'a routeur...), le SNR, l'adresse IP (si elle est disponible), la force du signal et le bruit. Un graphe m en temps réel la force du signal. Un système de filtrage permet d'identifier les points d'accès a sans Encryption. NetStumbler peut être relié à un système GPS pour localiser le point d'accès (parlé de gadget).



5.2. Filtrage par adresse MAC

Bien que cela ne soit pas officiellement dans la norme 802.11, rien n'empêche à un AP de vérifier si l'adresse MAC de la station qui cherche à s'authentifier se trouve bien dans une liste d'adresses MAC autorisées.



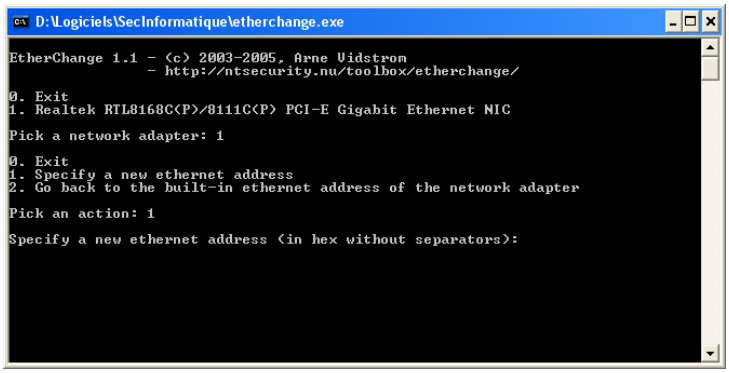
Authentification par adresse MAC

Ce type d'authentification peut être employé en complément d'un autre type d'authentification (WEP, WPA, WPA2,...)

Vulnérabilité :

Il n'est pas difficile pour un pirate de modifier l'adresse MAC de sa carte Wifi pour se faire passer pour l'un des périphériques autorisés : cela s'appelle le MAC Spoofing. Par ailleurs, si le nombre de machines autorisées est important ou change souvent, cette méthode devient assez lourde à gérer. Dans la pratique, le filtrage par adresse MAC est donc plutôt adapté pour un usage familial ou dans une très petite entreprise : il offre peu de sécurité et est rapidement lourd à ge

Logiciel de changement d'adresse MAC EtherChange :



6. Sécurité du WiFi

Malgré toutes ces failles, il existe des solutions robustes qui rendent un réseau sans fil a
sur qu'un réseau filaire, toutefois, ces solutions sont loin d'être triviales. Nous allons vous expli
leur fonctionnement dans cette partie.

6.1. Les attaques d'un réseau Wifi :

6.1.1. Le WarDriving (la guerre en voiture)

A la recherche des réseaux Wifi

Lorsque les réseaux Wifi ont commencé à connaitre le succès, plus de 50% d'entre eux
n'étaient absolument pas sécurisés. Cela peut paraitre aberrant, mais voici ce que pensaient le
propriétaires :

Le signal ne porte pas très loin, donc le risque qu'un pirate trouve le réseau est faible ;

Il y a peu de pirates et beaucoup de réseaux Wifi, donc pourquoi un pirate s'attaquerait-i
mien plutôt qu'à un autre ?

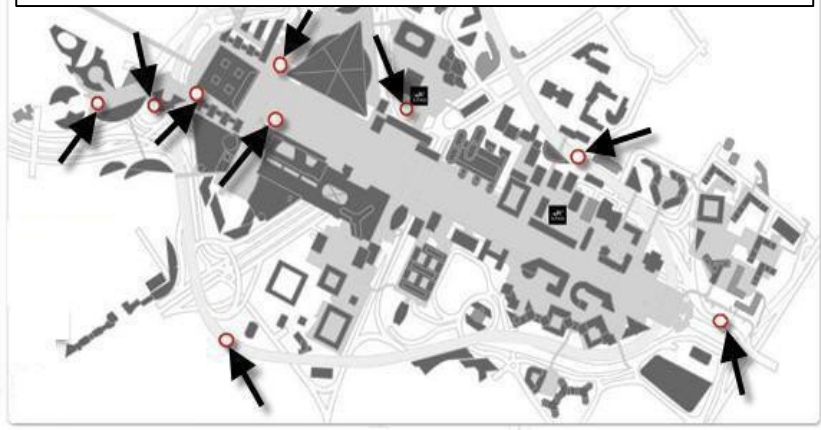
Je ne suis qu'un simple particulier (ou une petite société), donc un pirate n'aurait aucun
intérêt à me causer du tort.

Je n'ai pas de données confidentielles, donc je ne risque rien ?

Toutes ces excuses sont à proscrire ! Voici pourquoi : des lors que l'on su que de nombre
réseaux WiFi n'étaient pas sécurisé, un nouveau sport est né : le WarDriving. Le plus souvent
pratiqué par des groupes de passionnés de la radio, il consiste à se promener en voiture avec u
antenne WiFi et à noter la position et les caractéristiques de tous les AP que l'on puisse trouver

Des logiciels tels que NetSTUMBLER permettent même d'automatiser la tâche, et ils peu
être reliés à un module GPS pour que la position exacte soit enregistrée. La carte des AP ainsi
obtenue est souvent publiée sur Internet, de sorte que n'importe qui peut savoir où se situent
réseaux non sécurisés !

Exemple d'une carte mettant en évidant le positionnement des points accès



6.1.2. Espionnage :

Pour espionner un réseau WiFi sans fil, vous n'avez cas installer un logiciel tel quie WireS et configurer votre adaptateur WiFi en mode Promiscuous. En captant les trames WiFI avec un logiciel (WirShark ou Ethereal) : le pirate se réjouit ! (récupération mots de passe, document se numéros de carte bancaires, etc…) pour toutes les communications non cryptées.

Pour se protéger : il est indispensable de crypter les communications avec un algorithme puissant tel que WPA et WPA2

6.1.3. Intrusion :

L'intrusion est trivial si il n'ya pas de sécurisation du AP, un pirate peut s'associer au rés normalement. En revanche, si l'association impose un mécanisme d'identification avant d'auto l'ouverture d'une session sur le réseau, le pirate aura essentiellement deux options :

-Ouvrir une nouvelle session en se faisant passer pour un utilisateur légitime.

-Détourner une session existante (Hijacking).

6.1.4. Ouverture d'une session :

Nous avons vue que les stations doivent être authentifiées, avant de s'associer au résea Pour les AP qui utilisent des une authentification par un nom d'utilisateur et un mot des passes pirate a plusieurs options :

1- Si les mots de passes sont échangés en clair, il suffit d'attendre qu'un utilisateur légit se connecte et d'espionner l'envoi de son mot de passe.
2- Si le mot de passe est crypté, on peut essayer de s'attaquer à l'algorithme de crypta utilisé, certains étant beaucoup plus faible que d'autres.

Une autre technique, plus brutale, consiste à essayer des millions de mots de passe jusq trouver le bon ! Certain logiciels permettent d'essayer les mots de passe les plus probable en u les mots du dictionnaire, et en lis modifiant légèrement. On parle donc d'attaque du dictionnair

Exemple d'un logiciel permettant d'effectué cette attaque : **BruteForce**

Il existe deux variantes de l'attaque de dictionnaire :

L'attaque « en ligne »

Le pirate essaie successivement chaque mot de passe jusqu'à trouver le bon.

Cette attaque à plusieurs inconvénients (pour le pirate) :

- Elle prend beaucoup de temps car chaque mot de passe doit être vérifié par le système
- Le pirate risque d'être repéré, surtout si le système est configuré pour détecter les tentatives d'intrusion.

Une bonne façon de se prémunir contre les attaques de dictionnaire en ligne est donc de configurer le système pour qu'il prévienne un administrateur lorsqu'un utilisateur essaie de nombreux mots de passe d'affilée, et que cet utilisateur soit automatiquement bloqué.

L'attaque « hors ligne ».

Le pirate enregistre le dialogue d'une authentification réussie. Il possède alors le défi et réponse, correcte, de l'utilisateur. Rien ne l'empêche alors « hors connexion » d'essayer des m de mot de passes (avec le même défi et le même algorithme), jusqu'à trouvé jusqu'à trouvé ce donne la même réponse avec l'utilisateur. Méthode rapide et le pirate ne sera pas bannie.

Ce prémuni : obliger les utilisateurs à utiliser des mots de passe long et complexe.

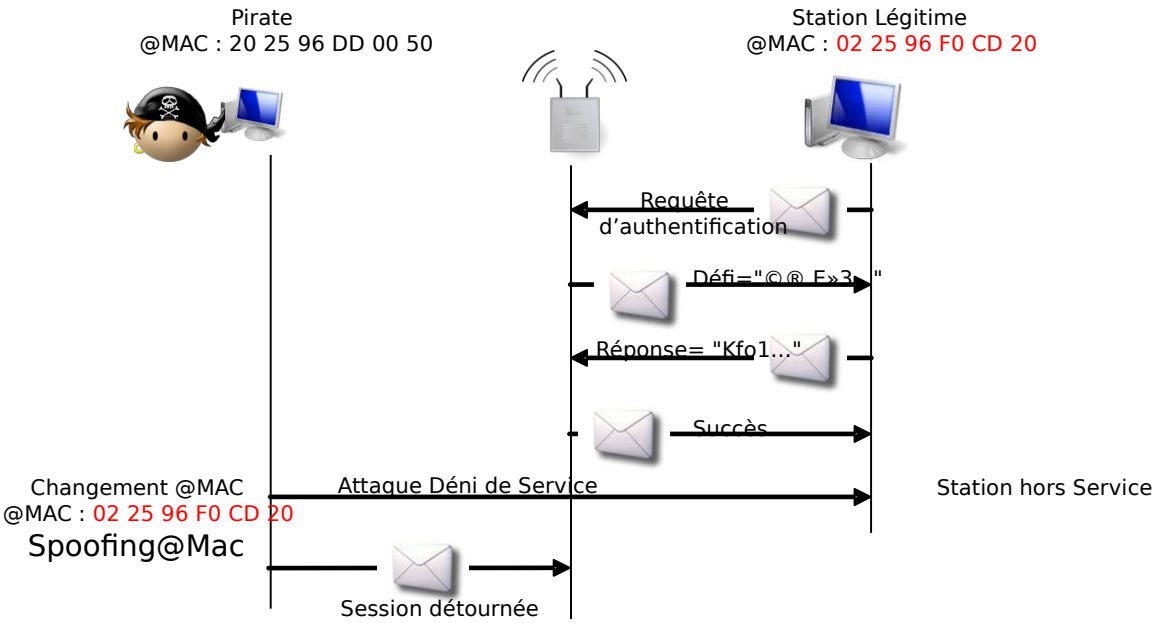
6.1.5. Attaque de relecture

Une autre façon d'ouvrir une nouvelle session consiste à enregistrer les paquets émis pa
station légitime au moment ou elle se connecte, puis des les remettre à l'identique un peu plus

Ceci peut s'appliquer pour tout type de requêtes (réécriture d'une requtee d'insertion da
une BDD par exemple)

Solution une façon d'éviter les risques de relectures consiste à imposer qu'un compteur
soit incrémenté à chaque paquet échangé : on dit qu'on rajouté du sel (SALT) dans chaque paq
Ce cette façon, un paquet contenant un compteur ancien sera rejeté. Le WEP n'offre aucune
protection contre la relecture, mais en revanche le WPE et le WPE2 son immunisés contre ce ge
d'attaque.

6.1.6. Détourner une session existante : (Hijacking en Wifi)



Hijacking

Solution

Crypter les communications
Utiliser le WPA ou WPA2.

6.1.7. Déni de service : (DoS) empêcher le réseau de fonctionner :

Une alternative, est de casser carrément le AP, et le réseau s'écoule.

Une autre est d'émettre des ondes radio sur la même fréquence que celle de votre AP ave
brouilleur.

But :

-le vandalisme gratuit ou intéressé ;

-assouvissement d'une vengeance ;

-le pirate peut également demander une rançon pour rétablir le service.

-le pirate peut faire une attaque DoS assez brève dans le but de déconnecter des utilisateurs pour les forcer à se reconnecter quelques instants après. Le but est alors d'essayer de subtiliser leurs mots de passes pour pouvoir faire plus tard un attaque d'intrusion.

6.1.8. Faiblisse du protocole MAC et le déni de Service:

Pour la couche MAC, une attaque consiste à émettre sans arrêt des paquets pour saturer l réseau. Pire, absolument rien n'est prévu dans le standard wifi pour sécuriser les paquets de gestion(tels que les trame Balise, les Trames d'authentification, et les trames d'association et désassociassions) ni pour sécuriser les paquets de contrôles (Paquet RTS, CTS, ACK). Conclusio n'empêche à un pirate d'envoyer un paquet de désassociassions à tous les utilisateurs connect en se faisant passer pour l'AP, un simple Spoofing d'adresse MAC suffit, alors de déconnecter L utilisateurs de l'AP !

Autre option :

le pirate peut sans arrêt envoyer des paquets CTS en se faisant passer pour l'AP : tous les utilisateurs croient que l'AP a donné le droit à un autre utilisateur d'envoyer son paquet de don et ils se mettront donc en attente.

Solution aucune !!!!!!!

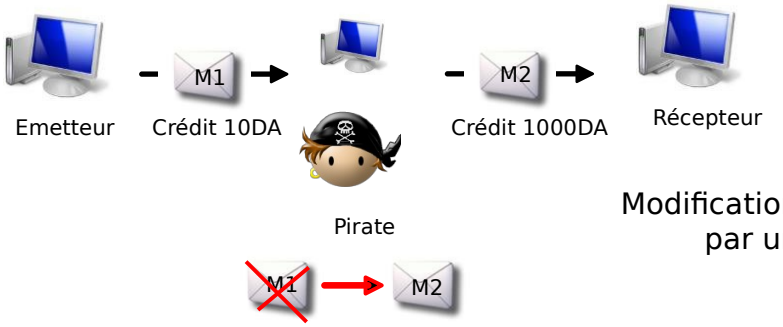
Aucune pour se prémunir contre le DoS en WiFi.

Le minimum est d'essayer de trouver la source qui doit se situer non loin du réseau attaq éventuellement appelé les autorités.

Autre alternative consiste à riposter, c.-à-d. reprendre le poste du pirate. Pour le faire des logiciels existent (tels que AirMargnet) qui permettent de faire une audite du réseau.

6.1.9. La modification des messages :

Un autre type d'attaque est la modification des messages échangé à l'insu des interlocute
Cette modification peut s'effectué bien sur les messages en clair que sur les messages cryptés
que avec les massages cryptés la modification sera à l'aveuglette, le pirate ne saura pas qu'es
qu'il a modifié, espérant que ceci ait un sens pour le récepteur).



Modification d'un message
par un pirate

Le pirate Intercepte le message et il le modifie
puis il le renvoie(en recalculant le CRC)

Solution :

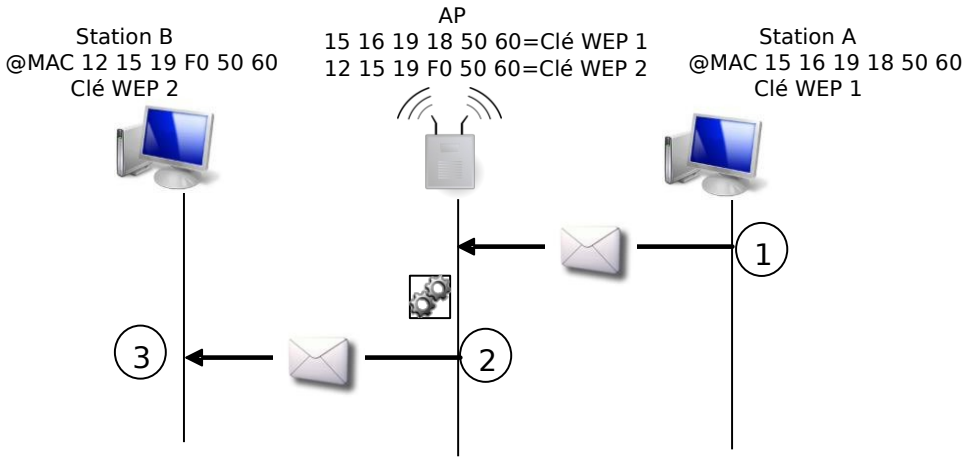
1. Le cryptage avec la clé WEP, WPA ou WPA2.
2. Limiter les débordements : une première mesure de protection contre les attaque
   du réseau sans fil consiste à s'assurer que les ondes radio ne débordent pas(ou pe
   sur l'extérieur de l'entreprise. Ça permet aussi de baisse la consommation et
   optimise le réseau en étudiant les positionnements des APs.
3. Réseaux privés Virtuels (VPN)

6.2 La mise en œuvre de WEP :

WEP (Wired Equivalent Privacy) est algorithme de cryptage symétrique, à une seule clé se de (40 ou 104 bits). Il suffit de configurer chaque adaptateur WiFi (Ordinateur, PDA, AP) avec la même clé pour qu'ils puisent communiquer.

6.2.1. Les clés individuelles et clés partagées:

Le standard 802.11 définit deux types de clés WEP : la clé WEP partagée par tous (Shared K et les clés WEP individuelles. Les clés WEP individuelles sont propres à chaque station. AU nive l'AP on a une table de correspondance des clés.



1. La stationA crypte un message avec sa propre clé WEP pour l'envoyer à la StationB
2. L'AP Décrypte le message reçu en utilisant la clé WEP associée à @MAC puis le crypt avec la clé WEP de la stationB
3. La stationB décrypte le message avec sa propre clé WEP.

Les clés individuelles ont un avantage important : chaque employé possède sa propre clé, ses communications ne peuvent pas être espionnées par les autres collègues.

Pour la clé Partagée, la même clé WEP est utilisée par toutes les stations pour crypter ou décrypter les messages.

6.2.2. L’algorithme RC4

Le WEP repose sur un algorithme appelé RC4. Cet algorithme a été conçu par l’un des gra
noms de la sécurité informatique : Ron Rivest.

En 1977, il décrit avec Adi Shamir et Len Adleman le premier algorithme de chiffrement à clé publique, nommé RSA selon leurs initiales. Ils reçoivent en 2002 pour cette découverte le Prix Turing de l'Association for Computing Machinery.

RC4 Rivest Cipher 4 c’est-à-dire « code de Rivest numéro 4 ».

Principe de RC4 :

RC4 ne crypte rien, son rôle est de produire une série de bits pseudo-aléatoires R. Un tab
de 256 octets (2048bits) est d’abord initialisé avec la clé RC4, répétée autant de fois que néces
pour remplir le tableau. Par la suite, des opérations très simples sont réalisées pour mélanger a
que possible le tableau et obtenir R.

6.2.3. Procédure du cryptage :

Avec la clé WEP, on peut générer un code pseudo-alétoire (R) de la même longueur que le
message à crypter(M). On applique ou pour obtenir le message crypté (MesCry).

MesCry=MR

Pour le décryptage, la station régénère le même code pseudo-aléatoire avec la même clé
et applique le pour obtenir le message décrypté (M)

M= MesCryR

XOR	1 1=0	0 1=1	1 0=1	0 0=0

1001 0011 1110 1001=0111 1010 (147 233 = 122)

Un aspect très important de est qu’en répétant la même opération deux fois, on revient à la valeur initiale :

a b b = a donc (122 233 = 147).

6.2.4. Vulnérabilité

Eviter la répétions de la clé RC4 :

Imaginons deux messages (M1 et M2) cryptés avec le même code RC4 (R)

$$C1 = M1 \oplus R$$

$$C2 = M2 \oplus R$$

Un espion intercepte les deux messages cryptés, il peut alors réaliser l'opération suivante :

$$C1 \oplus C2 = (M1 \oplus R) \oplus (M2 \oplus R) = (M1 \oplus M2) \oplus (R \oplus R) = (M1 \oplus M2)$$

On voit qu'en calculant C1 C2 l'espion parvient à éliminer R de l'équation ! Or ce R qui donnait au message crypté son aspect aléatoire.

A vrai dire, l'espion n'a pas encore les messages en clair, mais il n'en est pas loin. Pour vo convaincre, admettons par exemple que le message M2 soit entièrement rempli de zéro : dans cas, l'espion aura M1 M2 = M1 0=M1 : le message M1 lui apparait en clair, comme par enchantement. Si le message M2 contient des séquences nulles à certains endroits, cela laisse apparaitre en clair des portions du message M1, aux endroits correspondants et vise versa bien

Solution :

Il faut éviter à tout prix de réutiliser la même séquence pseudo-aléatoire dans les paquets distincts. C'est pour ça une clé WEP est précédée par un Vecteur d'initialisation (appelé **nonce** permet généré des clés RC4 différentes.

Donc une clé de cryptage est la suivante

IV (variable)	Clé WEP(fixe)
3 octets (24bits)	5 ou 13 octets(40 ou 104 bits)

Bien entendu, pour pouvoir décrypter le message, le récepteur doit connaitre la clé RC4 a complet. Il connait déjà la clé WEP, puisqu'elle est configurée dans chaque poste et chaque AP réseau, mais comment connaitre l'IV ?

La réponse est simple : l'IV est envoyé, en clair, au début de chaque paquet (après l'en-tê MAC). Voici le format d'un paquet crypté avec le WEP :

IV	ID	Données cryptées	ICV crypté
3 octets	1octet	0 à 2304	4octets

Le vecteur d’initialisation (IV) est un nonce (un nombre sensé n’être utilisé qu’une seule f
généré pour chaque paquet. Il est rajouté avant la clé WEP pour former la clé RC4 qui sert à cr
le paquet. Pour que le récepteur puisse décrypter le paquet, l’IV est envoyé avec le paquet.

Inconvénient, IV est trop cours donc une même clé RC4 sera réutilisée tôt ou tard

6.2.5. Le contrôle d’intégrité :

L’ICV Pour résoudre ce problème, le WEP a défini un mécanisme assez simple: un code de
vérification de l’intégrité du message (Integrity Check Value ICV) est calculé de façon similaire
habituel, sur 32 bits également. Toutefois, l’ICV est calculé non pas à partir du paquet « prêt à
partir » (c.-à-d. crypté) comme le CRC, mais à partir du message original (En clair). L’ICV et ins
fin du message, et le tout est crypté par l’algorithme RC4.

6.2.6. Casser la clé WEP, Les clés faibles :

En août 2001, un article fut publié par Scott Fluhrer, Itsik Mantin et Adi Shamir : Weakness
the Key Scheduling Algorithm of RC4. Cet article démontre qu’il existe une faiblesse dans l’algo
RC4: pour certains types de clés RC4, les premiers bits produits par l’algorithme ont une forte
probabilité de correspondre à quelques bits de la clé ! C’est clé sont donc appelées des clés fai
(Weak keys).

Peu de temps après la parution de cet article, les outils furent créés, mettant en œuvre ce
attaque : AirSnort, WEPCrack, dweputils … disponibles gratuitement sur Internet !

Devant l’ampleur du désastre, des constructeurs ont réagi en créant des adaptateurs WiFi
capables d’éviter les IV qui produisent des clés Faible.

7. Sécurité du WiFi avancée : WPA (Wi-Fi Protected Access)

Nous allons étudier dans cette partie le WPA (WPA et WPA2, en particulier la version personnel la plus utilisée, mais aussi la version Enterprise utilisant un serveur d'authentificatio type radius donc plus compliquée) son fonctionnement (protocole de cryptage, authentificatior ses faiblesses et ensuite quels sont les moyens utilisés pour le craquer.

Le Wi-Fi Protected Access (WPA et WPA2) est un mécanisme pour sécuriser les réseaux sa de type Wifi.

7.1. Origine du WPA

7.1.1. Wi-Fi Alliance (WPA) :

La Wi-Fi Alliance est une association d'entreprises, qui possède les droits sur le sigle Wi-fi qui certifie le matériel portant ce sigle. Les certifications des implantations du WPA ont comme en avril 2003 et sont devenues obligatoires en novembre 2003.

Le WEP faisant l'objet de trop nombreuses faiblesses, la Wi-Fi Alliance et l'IEEE ont donc d de garantir plus de sécurité tant pour le transfert des données que pour l'authentification des utilisateurs en créant une nouvelle solution de sécurisation de réseau WiFi.
La norme IEEE 802.11i a tardé à être validée. Du coup, en fin 2002, la Wi-Fi Alliance a défi sous-ensemble de ce qu'allait être 802.11i, sous la désignation de WPA.

7.1.2. 2. 802.11i (WPA2) :

La norme IEEE 802.11i, est un amendement à la norme IEEE 802.11 ratifié le 24 juin 2004 connu sous le nom de WPA2, traite du renforcement de la sécurité des échanges au niveau des réseaux informatiques locaux utilisant une liaison sans fil (WLAN). La norme IEEE 802.11i (ou W fournit un chiffrement plus élaboré que celui de la solution intérimaire WPA (Wi-Fi Protected Access).

Pour la mise en place de ces nouvelles sécurités, il faut faire attention au matériel (point d'accès) utilisé car le WPA ne nécessite qu'une mise jour du firmware du point d'accès tandis q WPA2 nécessite un matériel adéquat. De nos jours, tous les nouveaux matériels disposent de la sécurité WPA2.

Il existe 2 types de WPA, la version personal la plus utilisée, mais aussi la version enterpri utilisant un serveur d'authentification.

7.2. WPA personal : clés partagées (PSK)

7.2.1. Schéma et explication de connexion, d'authentification :

Le mode personal permet de mettre en œuvre une infrastructure sécurisée basée sur le W sans utiliser de serveur d'authentification. Le WPA personal repose sur l'utilisation d'une clé partagée, appelées PSK pour Pre-shared Key, renseignée dans le point d'accès ainsi que dans le postes clients. En effet, le WPA permet de saisir une « passphrase » (phrase secrète), traduite par un algorithme de hachage.

Voici le schéma d'une connexion WiFi de base, c'est-à-dire que le client envoie une requête d'authentification au point d'accès, celui-ci lui répond et en cas d'authentification réussi, le clie renvoie une requête pour s'associer au point d'accès. Si celui-ci accepte, le client est connecté point d'accès.

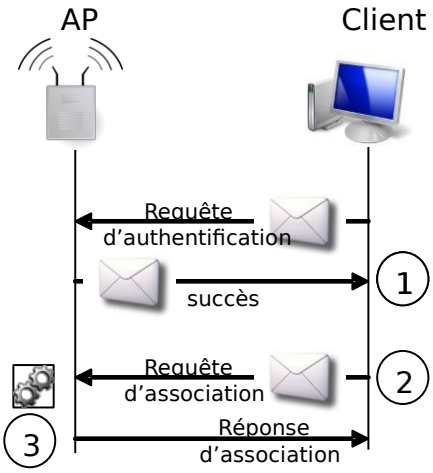


Figure 1 Association WiFi

7.2.2. Explication des différentes clés utilisées

Voici le schéma de la négociation des clés durant la phase de la connexion au point d'acc

Tout d'abord le client et le point d'accès se mettent d'accord sur une clé PTK (Pairwise Transient Key) dérivée de la PMK (Pairwise Master Key). Désormais les échanges sont cryptés a clé PTK dans un tunnel sécurisé.

Ce qui permet au point d'accès d'envoyer la clé GTK (Group Transient Key) utilisée pour cr le trafic broadcast et multicast avec une requête EAPol-Key. Avec cette clé le client peut dorén décrypter le trafic de groupe et ensuite accéder au réseau en ayant des communications crypt

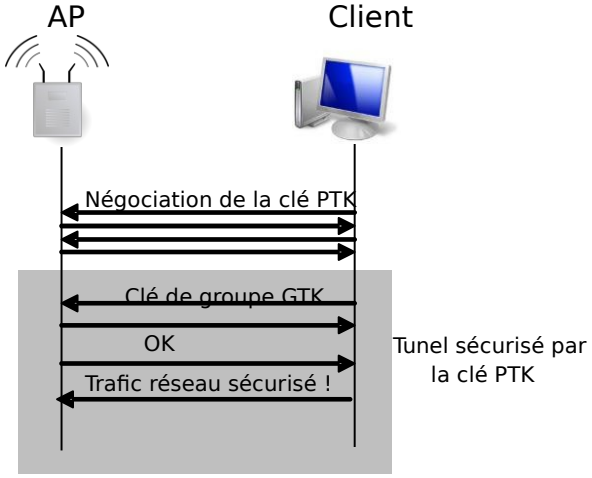


Figure 2 : Négociation des clés temporaires

Un moment important de la communication est le four-way handshake, c'est-à-dire 4 messages non cryptés donc vulnérables aux attaques car ils contiennent les échanges permett négocier la clé PTK.

Ces messages sont d'ailleurs utilisés au moment du craquage de la clé WPA (cf V Test).

Voici le schéma du four-way handshake :

- Tout d'abord le point d'accès envoie son nonce (numéro utilisé qu'une seule fois) au clie
clair.
- Ensuite le client génère la clé PTK avec ses éléments, et envoie son propre nonce au poi
d'accès en rajoutant un code de contrôle d'intégrité.
- Puis le point d'accès génère la clé PTK à l'aide du nonce du client. Il utilise la clé générée
vérifier le code d'intégrité envoyé par le client et si le code est bon (sinon il y a échec de la
connexion), il envoie un message au client pour lui dire en rajoutant un code d'intégrité.
- Pour finir, le client vérifie le code d'intégrité et si le code est bon c'est qu'ils ont la bonne
même clé PMK. Il envoie ensuite un message au client pour lui dire qu'il est prêt à démarrer la
session. Le tunnel sécurisé est donc créé ce qui permet désormais de réaliser des échanges cry

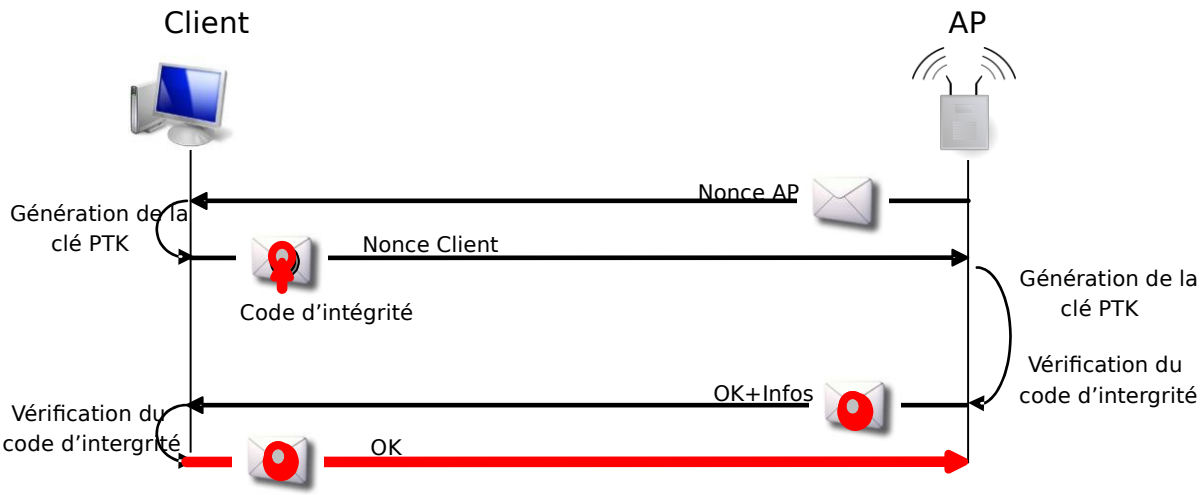


Figure 3 : Négociation de la clé temporaire PTK avec le four-way handshake

Plusieurs clés sont donc utilisées pour se connecter à un réseau. Tout d'abord la première clé (
EAP suivant le protocole utilisé) devient la clé maitresse appelé PMK.
Ensuite, la clé PTK, c'est la dérivée avec une fonction de hashage de la clé PMK. La clé de grou
quant à elle est générée par le point d'accès après hashage de la clé GMK.

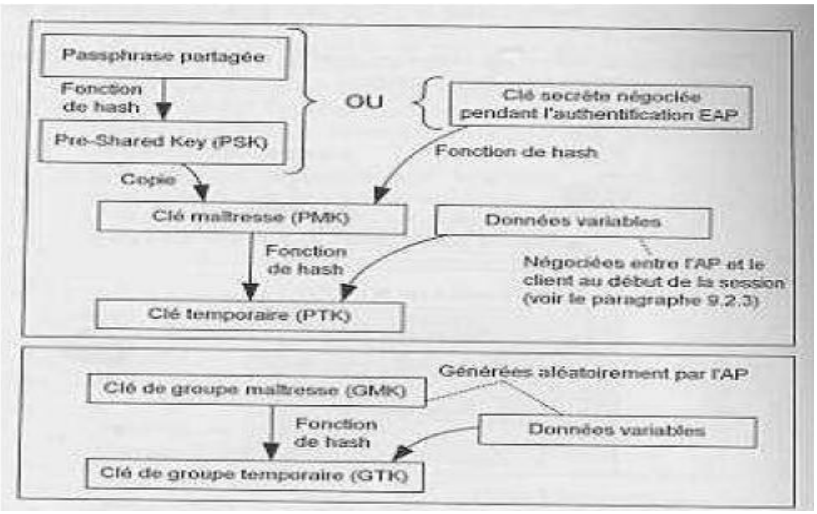


Figure 4 : Hiérarchie des clés du WPA et du WPA2

7.3. WPA Enterprise : architecture 802.1x (RADIUS avec EAP)

7.3.1. Schéma et explication de connexion, authentification :

Le mode enterprise impose l'utilisation d'une infrastructure d'authentification 802.
basée sur l'utilisation d'un serveur d'authentification, généralement un serveur RADIUS
(Remote Authentication Dial-in User Service), et d'un contrôleur réseau (le point d'accè

Le but du protocole EAP utilisé ici est d'identifier les utilisateurs avant de les laisse
rentrer sur le réseau à l'aide de multiples méthodes d'authentification : mot de passe,
à puce, certificats électroniques, ...

Voici le schéma expliquant comment marche la connexion WiFi avec un serveur
d'authentification (version WPA enterprise). Ici les clients sont reliés au point d'accès m
ensuite pour accéder au réseau il faut s'authentifier sur un serveur d'authentification.

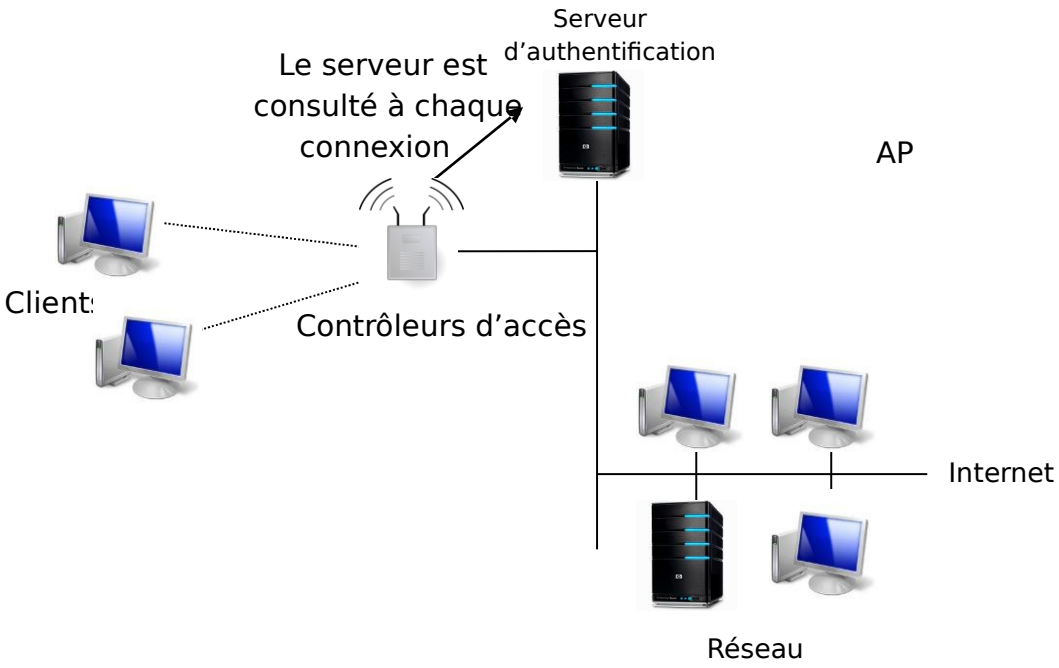


Figure 5 : Vue d'ensemble du protocole EAP

Le schéma suivant est celui d'une connexion WiFi avec 802.1x. Tout d'abord le clie
envoie une requête EAPol Start pour démarrer l'échange ayant pour but l'authentificati
point d'accès qui vérifie l'identité du client à l'aide d'un serveur d'authentification.

Au cours de l'authentification, le client et le serveur s'accorde sur le protocole de
cryptage des données et la clé de 256 bits utilisée (PMK). Après l'échange des clés entr
serveur, l'AP et le client, l'échange continue désormais dans un tunnel sécurisé.

L'authentification réussie, le serveur envoie une requête de succès EAP au client p
son association au point d'accès.

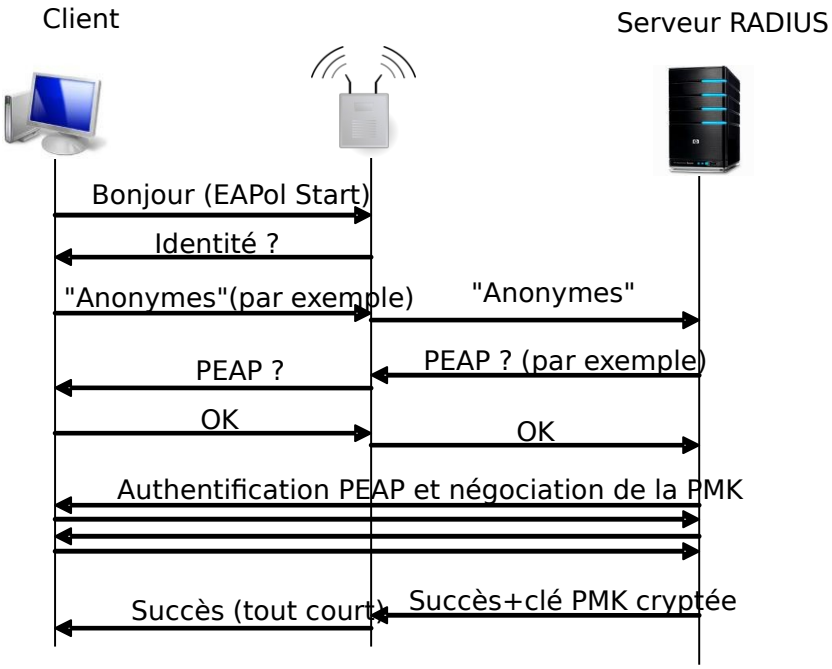


Figure 6 : Authentification 802.1x

Ce schéma est celui d'une connexion WiFi via un serveur d'authentification EAP av
un certificat.

Tout d'abord le serveur envoie une requête d'authentification au client, celui-ci lui
répond soit avec un mot de passe soit avec une carte à jeton soit avec un certificat (ici
client ne disposant pas de carte à jeton, il propose au serveur une autre alternative
d'authentification et celui-ci choisit le certificat).

Après vérification par le serveur, le client renvoie une requête pour s'associer au p
d'accès. Si le serveur accepte, le client est connecté au réseau.

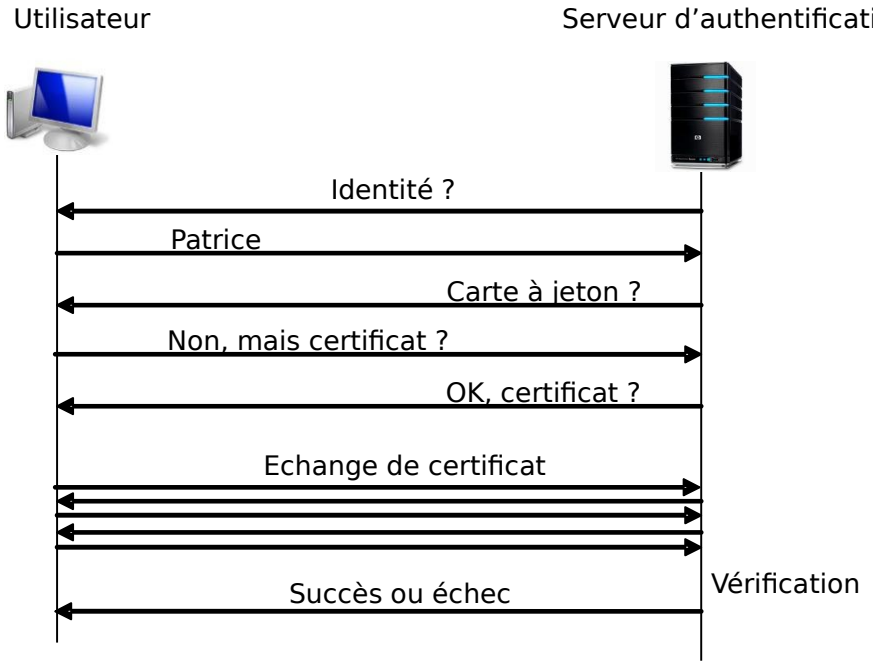


Figure 7 : Dialogue avec EAP

7.3.2. Types EAP

EAP (Extensible Authentication Protocol) est un protocole d'identification très soup
(mots de passe, carte à puce, certificats électroniques, ...) utilisé dans différents contex
pas seulement dans le cadre du WiFi et qui est défini par IEFT (Internet Engineering Tas
Force) en mars 1998 (RFC 2284) puis corrigé en juin 2004 (RFC 3748).

Le principe est basé sur 3 acteurs, c'est-à-dire que si un client cherche à accéder a
réseau, un contrôleur d'accès lui barrera le chemin jusqu'à ce qu'il s'identifie auprès du
serveur d'authentification.

Le contrôleur d'accès du type point d'accès sert d'intermédiaire pour la communication entre le client et le serveur d'authentification.

Il existe une multitude de méthodes d'authentification avec EAP qui se diffèrent pa
l'utilisation d'un certain protocole d'authentification (ex : CHAP), fonction de hachage (e
MD5), protocole de sécurisation des échanges (ex : TLS),... mais les principales sont
répertoriées dans le tableau suivant.

Ce Tableau récapitulatif des types EAP les plus courants.

Types EAP

	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP
Authentification du serveur	Aucune	Password Hash	Clé publique (certificat)	Clé publique (certificat)	Clé publique (certificat)
Authentification du client	Password Hash	Password Hash	Clé publique (Certificat , carte à puce)	CHAP, PAP, MS-CHAP(v2), EAP	EAP(EAP-MS-CHAPv2 ou clé publique)
Distribution dynamique des clés	Non	Oui	Oui	Oui	Oui
Risques sécurité	Vol de session. Attaque dictionnaire. Obtention du login client et Attaque MiM	Attaque dictionnaire et obtention du login client	Obtention de l'identité client	Attaque MiM	Attaque MiM

Figure 8 : Tableau récapitulatif des types EAP

7.4. Cryptages

Il existe 2 types de cryptage, le protocole TKIP pour le WPA, et le protocole AES po
WPA2.

7.4.1. WPA : TKIP

1. Présentation

TKIP (Temporal Key Integrity Protocol) est un protocole de communication utilisé p
la protection et l'authentification des données transitant sur un réseau WiFi. WPA spécif
notamment l'utilisation de ce chiffrement qui recourt au même algorithme (RC4) que W
mais renouvelle la clé tous les dix mille paquets. TKIP est donc plus performant que le

2. Nouveautés par rapport au WEP (clé RC4)

On utilise le même algorithme de cryptage RC4 que le WEP seulement il est plus
performant.

Un mécanisme a été mis en place pour éviter d'utiliser des clés RC4 faibles, l'utilis
du contrôle d'intégrité Michael est plus puissant que le contrôle d'intégrité IVC du WEP,
vecteur d'initialisation est plus long (48 bits au lieu de 24 bits pour le WEP) et est aussi
pour contrer les attaques de relecture et enfin les clés de cryptage sont différentes à ch
paquet, et sont distribuées suivant un mécanisme plus souple et plus sûr que celui du

7.4.2. WPA2 : TKIP et AES (CCMP)

1. Présentation

CCMP (Counter-Mode/CBC-Mac protocol) est une méthode de chiffrement qui utilise
AES (Advanced Encryption Standard), un algorithme de chiffrement. La combinaison de
deux est la sécurité la plus performante.

2. Nouveautés d'AES par rapport au TKIP

Le cryptage AES est le plus sécurisé, mais provoque certains problèmes de compatibilité avec quelques matériels. C'est le plus fort standard de chiffrage autorisé Wi-Fi.

Il dispose comme avantages d'une authentification forte reposant sur le protocole 802.1X, d'un mécanisme de distribution automatique des clés, d'un contrôle d'intégrité puissant et d'un mécanisme empêchant toute attaque de relecture. Si on choisit de se connecter en réseau mixte TKIP+AES alors le cryptage sera utilisé
avec l'algorithme le moins fort des deux, soit TKIP. Ce n'est donc pas une bonne solution de sécurité.

Tableau récapitulatif des protocoles, algorithmes de cryptages et algorithmes de contrôle d'intégrité des différentes solutions de sécurités WiFi.

Solution	Protocole	Cryptage	Intégrité
WEP	WEP	RC4	CRC
WPA	TKIP	RC4	Michael
WPA2	TKIP	RC4	Michael
WPA2	CCMP	AES	CBC

Solution Protocole Cryptage Intégrité
WEP WEP RC4 CRC
WPA TKIP RC4 Michael
WPA2 TKIP RC4 Michael
WPA2 CCMP AES CBC

3. Récapitulatif
Tableau récapitulatif des solutions de chiffrement plus précis que le précédent.

	WEP	*TKIP*	*CCMP*
Chiffrement	RC4	RC4	AES
Taille de la clé	40 ou 104 bits	128 bits (chiffrement) 64 bits (authentification)	128 bits
Taille IV	24 bits	48 bits	48 bits
Clé par paquet	Non (seul l'IV fait varier la suite chiffrante)	Oui	Pas nécessaire
Intégrité de l'en-tête du paquet	Non	SA et DA protégés par Michael	CCM
Intégrité des données du paquet	CRC32	Michael	CCM
Détection des rejeux	Non	Sequencement des IV obligatoire et rejeu impossible	Sequencement des IV obligatoire et rejeu impossible
Gestion des clés	Aucune	IEEE 802.1X	IEEE 802.1X

Figure 9 : Récapitulatif des solutions de chiffrement

7.5. Faiblesses :

- **Celles du PSK :**

C'est la solution la plus simple mais elle ne convient qu'aux petits réseaux infrastructure ou les réseaux Ad Hoc. Ces défauts sont dus aux mots de passe trop cou partage de la clé avec tous les utilisateurs ce qui diminue la sécurité et le fait que tous utilisateurs peuvent espionner le trafic des autres et dans le cas où le nombre d'utilisat est grand, le système devient lourd à gérer.

- **Celles de TKIP :**

Par exemple celle du protocole Michael qui dispose d'un code d'intégrité MIC (Message Integrity Protocol) trop court et donc qui peut être attaquable en quelques he

- **Celles d'EAP :**

La sécurité du 802.1x peut être compromise de 3 façons différentes : en attaquant méthode EAP utilisée (contre la méthode d'authentification il existe l'attaque de diction en ligne ou hors ligne), en détournant une session après sa création ou encore en s'interposant entre le client et le serveur d'authentification (attaque MiM).

7.6. Solutions :

- Celles pour PSK :

Il faut utiliser un mot de passe long, une vingtaine de caractères est recommandé au moins une douzaine si c'est des lettres aléatoires et aussi ne pas avoir trop d'utilisat gérer sur un même point d'accès.

- Celles pour TKIP :

La contre mesure de Michael est que si un paquet est modifié par un pirate le cont d'intégrité Michael le détectera et l'AP sera bloquée pendant 60 secondes. Ceci permet d'éviter qu'un pirate modifie des millions de paquets dans l'espoir que l'un d'entre eux passera le contrôle d'intégrité.

- **Celles pour EAP :**

Il faut créer un tunnel sécurisé, améliorer la validité du certificat (exemple : un par poste) et avoir une bonne sécurité interne du type carte à jeton en utilisant un cryptage puissant du type WPA et WPA2.

IV Types de craquage existant

Les principales failles utilisées pour le craquage sont celle de l'authentification ave MAC spoofing pour détourner une session, les failles ARP utilisées pour une attaque MiM (Man in the Middle) et les attaques DoS (déni de service).

- **Le MAC Spoofing**

C'est une technique d'attaque qui permet de changer son adresse MAC par une au pour pouvoir accéder à un routeur ou un serveur qui dispose d'une restriction d'accès p adresse MAC soit en se cachant du réseau soit en usurpant l'identité d'un autre ordinate

- **Attaques MiM** (Man in the Middle)

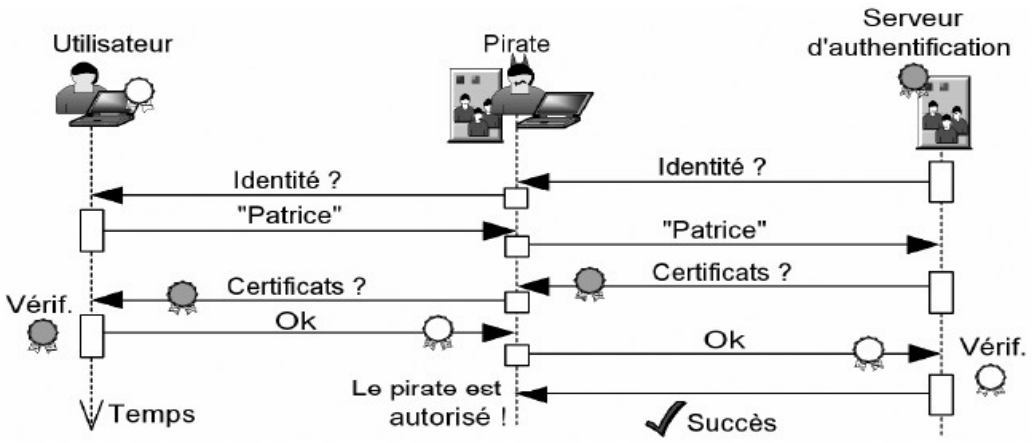


Figure 10 : Exemple d'attaque MiM contre l'authentification EAP

La principale attaque man in the middle consiste à exploiter une faiblesse du proto ARP (*Address Resolution Protocol*) dont l'objectif est de permettre de retrouver l'adress d'une machine connaissant l'adresse physique (adresse MAC) de sa carte réseau.

L'objectif consiste à s'interposer entre deux machines du réseau et de transmettre chacune un paquet ARP falsifié indiquant que l'adresse ARP (adresse MAC) de l'autre machine a changé, l'adresse ARP fournie étant celle de l'attaquant.

Les deux machines cibles vont ainsi mettre à jour leur table dynamique appelée Ca ARP. On parle ainsi de « ARP spoofing».

De cette manière, à chaque fois qu'une des deux machines souhaitera communiqu avec la machine distante, les paquets seront envoyés à l'attaquant, qui les transmettra manière transparente à la machine destinatrice. Cette attaque fait intervenir trois acteu le client, le serveur et l'attaquant. Le but de l'attaquant est de se faire passer pour le cl auprès du serveur et de se faire passer pour le serveur auprès du client. Il devient ainsi l'homme du milieu. Cela permet de surveiller tout le trafic réseau entre le client et le serveur, et de le modifier à sa guise pour l'obtention d'informations (mots de passe, ac système, etc.).

- **Attaques DoS**

Le déni de service ou Denial of Service (DoS) est, d'une manière générale, l'attaqu vise à rendre pendant un temps indéterminé une application informatique tel qu'un ser incapable de répondre aux requêtes de ses utilisateurs.

Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise, qu'ils ne puissent être utilisés et consultés. Les attaques de type DoS peuvent être évit repérant l'adresse de la machine

hostile, dans le cas d'une attaque à distance, et de bannir celle-ci. Les paquets IP provenant de cette machine seront donc désormais rejetés directement sans être traité

- **Attaques par dictionnaire** (en ligne et hors ligne)

L'attaque par dictionnaire est une méthode utilisée en cryptanalyse pour trouver u
mot de passe ou une clé. Elle consiste à tester une série de mots de passe potentiels, e
utilisant des fichiers externes contenant des phrases, mots, nombres, noms ou citation
uns à la suite des autres, en espérant que le mot de passe utilisé pour le chiffrement so
contenu dans les dictionnaires. Ce type d'attaque est très rapide. Un mot de passe mal
est vite découvert.

- **Attaques par force brute**

L'attaque par force brute est une méthode utilisée en cryptanalyse pour trouver un
mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons de cara
possibles. Cette méthode de recherche exhaustive ne réussit que dans les cas où le mo
passe cherché est constitué de peu de caractères. Ces programmes tentent toutes les
possibilités de mot de passe dans un ordre aléatoire afin de berner les logiciels de sécu
qui empêchent de tenter tous les mots de passe dans l'ordre.

Cette méthode garantit de trouver un mot de passe mais prend du temps. La solut
est d’avoir un mot de passe complexe.

8. Conclusion

La démocratisation des réseaux Wi-Fi a grandement simplifié le déploiement des infrastructures domestiques et professionnelles. Même si cette évolution est extrêmem positive, gardons-nous de penser que cette technologie est exempte de défauts. Contrairement aux réseaux filaires qui ne peuvent être attaqué que de façon distante, depuis Intente, un réseau sans fil pourra toujours être pénétré localement. Aussi, pour conserver que les bénéfices du Wi-Fi, il est fortement recommandé de sécurisé sans Wi prendre en considération toute les suggestions qu'on exposé pour augmenter la sa séc

Ces opérations ne s'effectuent pas sans douleur : bien sécuriser son réseau sans une opération contraignante à mettre en place. L'inconvénient ne s'arrête pas à l'étape paramétrages puisque ces nombreux verrouillages compliqueront également l'arrivée d nouvelles machines légitimes sur votre réseau Wi-Fi.

En résumé, il est bien évident que vous serez la première personne à être importu par vos propres sécurités. On remarque également que la sécurité quasi totale est pour l'instant réservée au monde professionnel (serveur radius etc.). Bien sûr, ces nombreus complications ne s'adresseront pas forcément à tout le monde. Les personnes allergiqu aux configurations dont la couverture Wi-Fi n'excèdent pas celle de leur propriété, pour être dispensées de paramétrages contraignants en supprimant toutes sécurités.

Sommaire