Le WI-FI

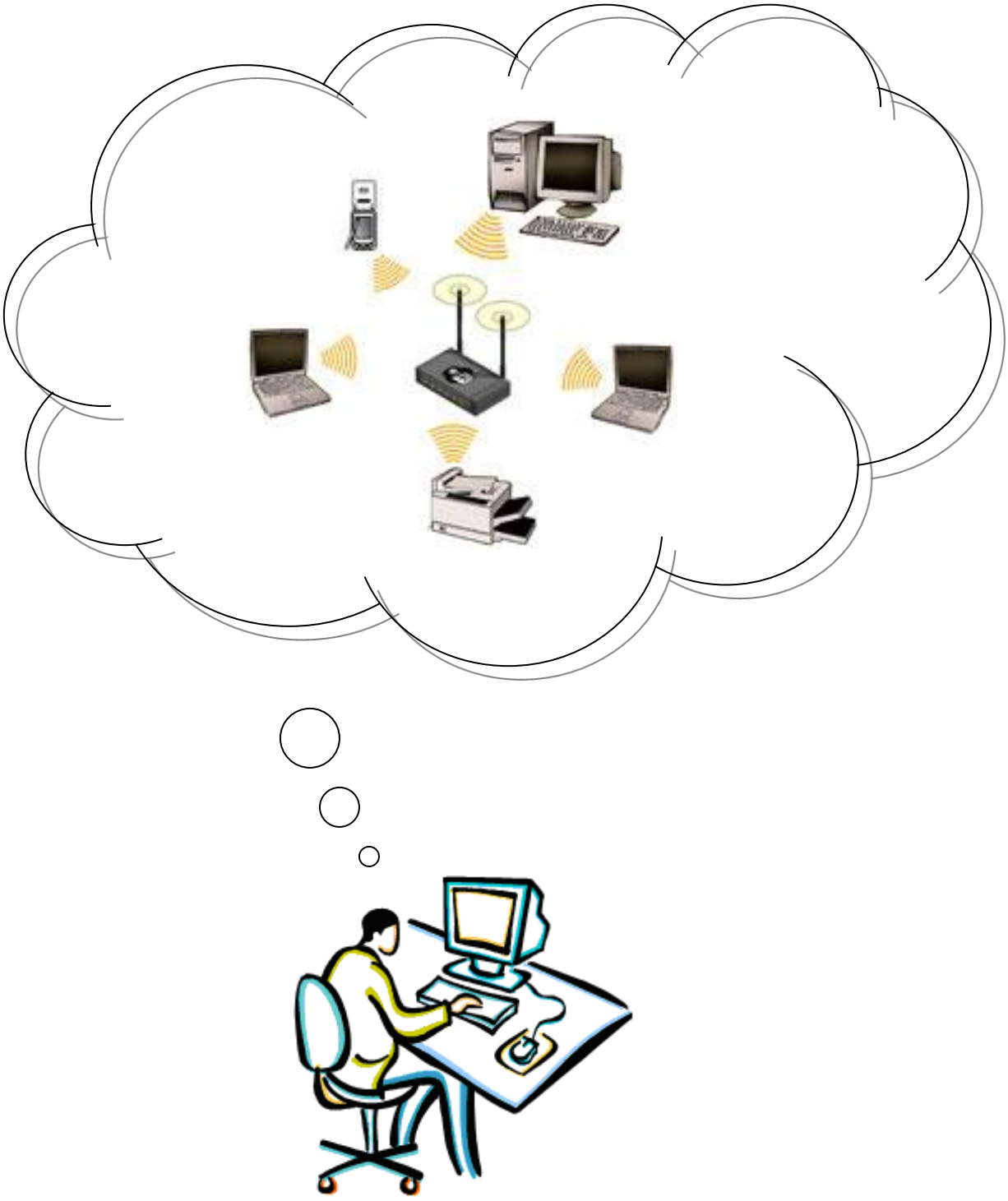


Table des matières

1 INTRODUCTION

Présentation du Wi-Fi (802.11)
La norme IEEE 802.11 (ISO/IEC 8802-11) est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN). Le nom Wi-Fi correspond initialement au nom donné à la certification délivrée par la Wi-Fi Alliance, anciennement 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 Wi-Fi est en réalité un réseau répondant à la norme 802.11.

Grâce au Wi-Fi, il est possible de créer des réseaux locaux sans fils à haut débit pour peu que l'ordinateur à connecter ne soit pas trop distante par rapport au point d'accès. Dans la pratique, le Wi-Fi permet de relier des ordinateurs portables, des ordinateurs de bureau, des assistants personnels (PDA) ou tout type de périphérique à une liaison haut débit (11 Mbps ou supérieur) sur un rayon de plusieurs dizaines de mètres en intérieur (généralement entre une vingtaine et une cinquantaine de mètres) à plusieurs centaines de mètres en environnement ouvert.

Ainsi, des opérateurs commencent à irriguer des zones à fortes concentration d'utilisateurs (gares, aéroports, hôtels, trains, ...) avec des réseaux sans fils. Ces zones d'accès sont appelées « hot spots ».

La norme 802.11
La norme 802.11 s'attache à définir les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques, c'est-à-dire :

- la **couche physique** (notée parfois couche PHY), proposant trois types de codages de l'information.
- la **couche liaison de données**, constitué de deux sous-couches : le contrôle de la liaison logique (Logical Link Control, ou LLC) et le contrôle d'accès au support (Media Access Control, ou MAC)

La couche physique définit la modulation des ondes radioélectriques et les caractéristiques de la signalisation pour la transmission de données, tandis que la couche liaison de données définit l'interface entre le bus de la machine et la couche physique, notamment une méthode d'accès proche de celle utilisée dans le standard Ethernet et les règles de communication entre les différentes stations. La norme 802.11 propose en réalité trois couches physiques, définissant des modes de transmission alternatifs :

Il est possible d'utiliser n'importe quel protocole de haut niveau sur un réseau sans fil Wi-Fi au même titre que sur un réseau Ethernet.

Les différentes normes Wi-Fi
La norme IEEE 802.11 est en réalité la norme initiale offrant des débits de 1 ou 2 Mbps. Des révisions ont été apportées à la norme originale afin d'optimiser le débit (c'est le cas des normes 802.11a, 802.11b, 802.11g, 802.11n et 802.11ac, appelées normes 802.11 physiques) ou bien préciser des éléments afin d'assurer une meilleure sécurité ou une meilleure interopérabilité.

Voici un tableau présentant les différentes révisions de la norme 802.11 et leur signification :

Nom de la norme	Nom	Description
802.11a	Wi-Fi5	La norme 802.11a (baptisé *Wi-Fi 5*) permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). La norme 802.11a spécifie 8 canaux radio dans la bande de fréquence des 5 GHz.
802.11b	Wi-Fi	La norme 802.11b est la norme la plus répandue actuellement. Elle propose un débit théorique de 11 Mbps (6 Mbps réels) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2.4 GHz, avec 3 canaux radio disponibles.
802.11c	Pontage 802.11 vers 802.1d	La norme 802.11c n'a pas d'intérêt pour le grand public. Il s'agit uniquement d'une modification de la norme 802.1d afin de pouvoir établir un pont avec les trames 802.11 (niveau *liaison de données*).
802.11d	Internationalisation	La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11. Elle consiste à permettre aux différents équipements d'échanger des informations sur les plages de fréquence et les puissances autorisées dans le pays d'origine du matériel.
802.11e	Amélioration de la qualité de service	La norme 802.11e vise à donner des possibilités en matière de qualité de service au niveau de la couche *liaison de données*. Ainsi cette norme a pour but de définir les besoins des différents paquets en terme de bande passante et de délai de transmission de telle manière à permettre notamment une meilleure transmission de la voix et de la vidéo.
802.11f	Itinérance (roaming)	La norme 802.11f est une recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole *Inter-Access point roaming protocol* permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau. Cette possibilité est appelée *itinérance* (ou *roaming en anglais*)
802.11g		La norme 802.11g offre un haut débit (54 Mbps théoriques, 30 Mbps réels) sur la bande de fréquence des 2.4 GHz. La norme 802.11g a une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b
802.11h		La norme *802.11h* vise à rapprocher la norme 802.11 du standard Européen (HiperLAN 2, d'où le *h* de 802.11h) et être en conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie.
802.11i		La norme *802.11i* a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'*AES* (*Advanced Encryption Standard*) et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
802.1n	WWiSE (World-Wide Spectrum Efficiency) ou TGn Sync	La norme 802.11n. Le débit théorique atteint les 540 Mbit/s (débit réel de 100 Mbit/s dans un rayon de 90 mètres) grâce aux technologies **MIMO** (Multiple-Input Multiple-Output) et OFDM (Orthogonal Frequency Division Multiplexing). En avril 2006, des périphériques à la norme 802.11n commencent à apparaître basés sur le Draft 1.0 (brouillon 1.0). le Draft 2.0 est sorti en mars 2007, les périphériques basés sur ce brouillon seront compatibles avec la version finale attendue pour avril 2009. Le 802.11n utilisera simultanément les fréquences 2,4 et 5GHz. Il saura combiner jusqu'a 8 canaux non superposés.
802.1ac	Amélioration du débit	IEEE 802.11ac est la dernière évolution du standard de transmission sans fil 802.11, qui permet une connexion sans fil haut débit dans la bande de fréquences inférieure à 6 GHz (communément appelée bande des 5 GHz). Le 802.11ac offre jusqu'à 1 300 Mbit/s de débit théorique, en utilisant des canaux de 80 MHz, soit jusqu'à 7 Gbit/s de débit global dans la bande des 5 GHz (de 5170 MHz à 5835 MHz).

Il est intéressant de noter l'existence d'une norme baptisée «802.11b+». Il s'agit d'une norme propriétaire proposant des améliorations en termes de débits. En contrepartie cette norme souffre de lacunes en termes de garantie d'interopérabilité dans la mesure où il ne s'agit pas d'un standard IEEE.

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

Standard	Bande de fréquence	Débit	Portée
Wi-Fi a (802.11a)	5 GHz	54 Mbit/s	10 m
Wi-Fi b (802.11b)	2.4 GHz	11 Mbit/s	100 m
Wi-Fi g (802.11g)	2.4 GHz	54 Mbit/s	100 m
Wi-Fi n (802.11n)	2.4 GHz ou 5 GHz	300 Mbit/s	125 m
Wi-Fi n (802.11ac)	5 GHz	433 à 1300 Mbps	125 m

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

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

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

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

802.11n
La norme 802.11n permet d'obtenir un débit théorique de 300 Mbps, pour une portée d'environ 50 de mètres en intérieur et jusqu'à 125 mètres en extérieur. Cette norme utilise la technologie MIMO, l'abréviation de *Multiple Input Multiple Output* (réceptions et émissions multiples) permet à une unité sans fil de transmettre de façon plus efficace les données à l'intérieur de locaux.
802.11ac
La norme 802. 802.11ac est un standard de transmission sans fil de la famille Wi-Fi, normalisé par l'IEEE le 8 janvier 20141, qui permet une connexion sans fil haut débit à un réseau local et utilise exclusivement une bande de fréquence comprise entre 5 et 6 GHz2, avec des variations selon les pays3.
Les canaux agrégés permettent, dans des conditions radio idéales, un débit théorique pouvant atteindre 1,3 Gbit/s et un débit utile de 910 Mbit/s (en utilisant quatre canaux occupant une sous-bande de 80 MHz)4,5, soit jusqu'à 7 Gbit/s de débit global, grâce à l'agrégation de canaux, au codage OFDM/OFDMA, à l'utilisation de la technique multi-antennes MIMO1 et au plus grand nombre de canaux disponibles dans la bande des 5 GHz par rapport à ceux autorisés dans la bande des 2,4 GHz utilisée par les normes 802.11 plus anciennes

Il existe différents types d'équipement pour la mise en place d'un réseau sans fil Wi-Fi :

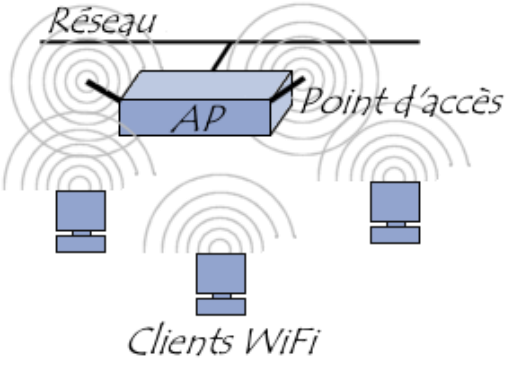
- Les **adaptateurs sans fils** ou cartes d'accès (en anglais Wireless adapters ou network interface controller, noté NIC) : il s'agit d'une carte réseau à la norme 802.11 permettant à une machine de se connecter à un réseau sans fil. Les adaptateurs Wi-Fi sont disponibles dans de nombreux formats (carte PCI, carte PCMCIA, adaptateur USB, carte Compact Flash, ...). On appelle station tout équipement possédant une telle carte.
- Les **points d'accès** (notés AP pour Access point, parfois appelés bornes sans fils) permettant de donner un accès au réseau filaire (auquel il est raccordé) aux différentes stations avoisinantes équipées de cartes Wi-Fi.

Le standard 802.11 définit deux modes opératoires :

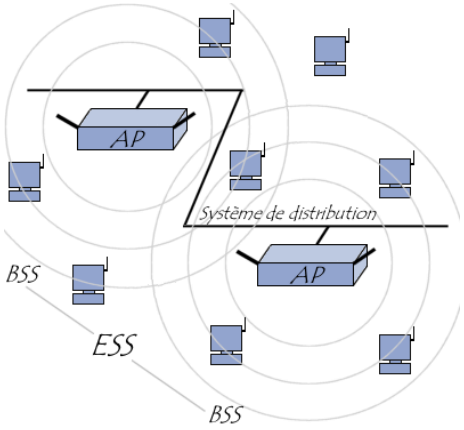
- Le **mode infrastructure** dans lequel les clients sans fils sont **connectés à un point d'accès**. Il s'agit généralement du mode par défaut des cartes 802.11b.
- Le **mode ad hoc** dans lequel les clients sont connectés les uns aux autres **sans aucun point d'accès**.

2 FONCTIONNEMENT DU WI-FI

Le mode infrastructure
En mode infrastructure chaque ordinateur station (notée STA) se connecte à un point d'accès via une liaison sans fil. L'ensemble formé par le point d'accès et les stations situés dans sa zone de couverture est appelé ensemble de services de base (en anglais basic service set, noté BSS) et constitue une cellule. Chaque BSS est identifié par un BSSID, un identifiant de 6 octets (48 bits). Dans le mode infrastructure, le BSSID correspond à l'adresse MAC du point d'accès.



Il est possible de relier plusieurs points d'accès entre eux (ou plus exactement plusieurs BSS) par une liaison appelée système de distribution (notée DS pour Distribution System) afin de constituer un ensemble de services étendu (extended service set ou ESS). Le système de distribution (DS) peut être aussi bien un réseau filaire, qu'un câble entre deux points d'accès ou bien même un réseau sans fil !



Un ESS est repéré par un ESSID (Service Set Identifier), c'est-à-dire un identifiant de 32 caractères de long (au format ASCII) servant de nom pour le réseau. L'ESSID, souvent abrégé en SSID, représente le nom du réseau et représente en quelque sort un premier niveau de sécurité dans la mesure où la connaissance du SSID est nécessaire pour qu'une station se connecte au réseau étendu.

Lorsqu'un utilisateur nomade passe d'un BSS à un autre lors de son déplacement au sein de l'ESS, l'adaptateur réseau sans fil de sa machine est capable de changer de point d'accès selon la qualité de réception des signaux provenant des différents points d'accès. Les points d'accès communiquent entre eux grâce au système de distribution afin d'échanger des informations sur les stations et permettre le cas échéant de transmettre les données des stations mobiles. Cette caractéristique permettant aux stations de « passer de façon transparente » d'un point d'accès à un autre est appelé itinérance (en anglais roaming).

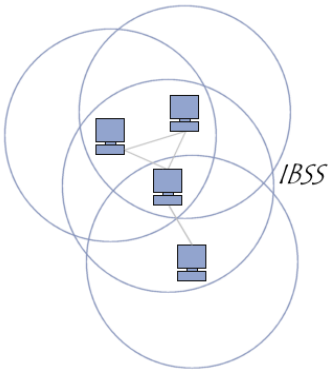
La communication avec le point d'accès
Lors de l'entrée d'une station dans une cellule, celle-ci diffuse sur chaque canal une requête de sondage (probe request) contenant l'ESSID pour lequel elle est configurée ainsi que les débits que son adaptateur sans fil supporte. Si aucun ESSID n'est configuré, la station écoute le réseau à la recherche d'un SSID.

En effet chaque point d'accès diffuse régulièrement (à raison d'un envoi toutes les 0.1 secondes environ) une trame balise (nommée beacon en anglais) donnant des informations sur son BSSID, ses caractéristiques et éventuellement son ESSID. L'ESSID est automatiquement diffusé par défaut, mais il est possible (et recommandé) de désactiver cette option.

A chaque requête de sondage reçue, le point d'accès vérifie l'ESSID et la demande de débit présent dans la trame balise. Si l'ESSID correspond à celui du point d'accès, ce dernier envoie une réponse contenant des informations sur sa charge et des données de synchronisation. La station recevant la réponse peut ainsi constater la qualité du signal émis par le point d'accès afin de juger de la distance à laquelle il se situe. En effet d'une manière générale, plus un point d'accès est proche, meilleur est le débit.

Une station se trouvant à la portée de plusieurs points d'accès (possédant bien évidemment le même SSID) pourra ainsi choisir le point d'accès offrant le meilleur compromis de débit et de charge.

Le mode ad hoc
En mode ad hoc les machines sans fils clientes se connectent les unes aux autres afin de constituer un réseau point à point (peer to peer en anglais), c'est-à-dire un réseau dans lequel chaque machine joue en même temps le rôle de client et le rôle de point d'accès.



L'ensemble formé par les différentes stations est appelé ensemble de services de base indépendants (en anglais independant basic service set, abrégé en IBSS).

Un IBSS est ainsi un réseau sans fil constitué au minimum de deux stations et n'utilisant pas de point d'accès. L'IBSS constitue donc un réseau éphémère permettant à des personnes situées dans une même salle d'échanger des données. Il est identifié par un SSID, comme l'est un ESS en mode infrastructure.

Dans un réseau ad hoc, la portée du BSS indépendant est déterminée par la portée de chaque station. Cela signifie que si deux des stations du réseau sont hors de portée l'une de l'autre, elles ne pourront pas communiquer, même si elles « voient » d'autres stations. En effet, contrairement au mode infrastructure, le mode ad hoc ne propose pas de système de distribution capable de transmettre les trames d'une station à une autre. Ainsi un IBSS est par définition un réseau sans fil restreint.

3 LES LIMITES DU WI-FI

Propagation des ondes radio
Il est nécessaire d'avoir une culture minimum sur la propagation des ondes hertziennes afin de pouvoir mettre en place une architecture réseau sans fil, et notamment de disposer les bornes d'accès (point d'accès) de telle façon à obtenir une portée optimale.

Les ondes radio (notées RF pour Radio Frequency) se propagent en ligne droite dans plusieurs directions. La vitesse de propagation des ondes dans le vide est de 3.108 m/s.

Dans tout autre milieu, le signal subit un affaiblissement dû à

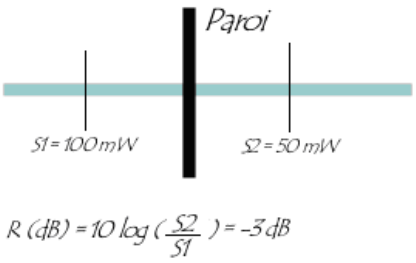
- **la réflexion :** *phénomène qui se produit lorsque des rayons lumineux (ondes) rencontrent un obstacle qui le force de suivre une autre direction*
- **la réfraction :** *c'est la déviation des rayons lumineux (ondes) passant obliquement d'un milieu transparent dans un autre*
- **la diffraction :** *phénomène de déviation des ondes (lumineuses, acoustiques...) lorsqu'elles passent au voisinage d'un obstacle physique*
- **l'absorption :** *processus par lequel l'énergie d'un photon est prise par une autre entité, par exemple, un atome qui fait une transition entre deux niveaux d'énergie électronique*

Absorption des ondes radio
Lorsqu'une onde radio rencontre un obstacle, une partie de son énergie est absorbée et transformée en énergie, une partie continue à se propager de façon atténuée et une partie peut éventuellement être réfléchie.

On appelle atténuation d'un signal la réduction de la puissance de celui-ci lors d'une transmission. L'atténuation est mesurée en bels (dont le symbole est B) et est égale au logarithme en base 10 de la puissance à la sortie du support de transmission, divisée par la puissance à l'entrée. On préfère généralement utiliser le décibel (dont le symbole est dB) correspondant à un dixième de la valeur en Bels. Ainsi un Bel représentant 10 décibels la formule devient :

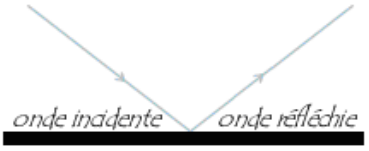
$$\mathbf{R\ (dB) = (10) * \log\ (P2/P1)}$$

Lorsque R est positif on parle d'amplification, lorsqu'il est négatif on parle d'atténuation. Dans le cas des transmissions sans fil il s'agit plus particulièrement d'atténuations.

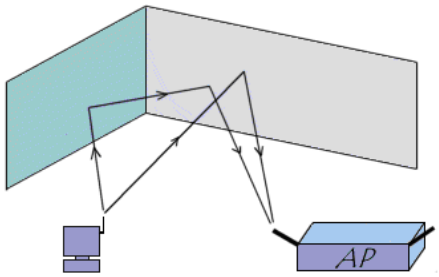


L'atténuation augmente avec l'augmentation de la fréquence ou de la distance. De plus lors de la collision avec un obstacle, la valeur de l'atténuation dépend fortement du matériau composant l'obstacle. Généralement les obstacles métalliques provoquent une forte réflexion, tandis que l'eau absorbe le signal.

Réflexion des ondes radio
Lorsqu'une onde radio rencontre un obstacle, tout ou partie de l'onde est réfléchie, avec une perte de puissance. La réflexion est telle que l'angle d'incidence est égal à l'angle de réflexion.



Par définition une onde radio est susceptible de se propager dans plusieurs directions. Par réflexions successives un signal source peut être amené à atteindre une station ou un point d'accès en empruntant des chemins multiples (on parle de « multipath » ou en français cheminements multiples).



La différence de temps de propagation (appelées délai de propagation) entre deux signaux ayant emprunté des chemins différents peut provoquer des interférences au niveau du récepteur car les données reçues se chevauchent. Ces interférences deviennent de plus en plus importantes lorsque la vitesse de transmission augmente car les intervalles de temps entre les données sont de plus en plus courts. Les chemins de propagations multiples limitent ainsi la vitesse de transmission dans les réseaux sans fil.

Pour remédier à ce problème les cartes Wi-Fi et points d'accès embarquent deux antennes par émetteur. Ainsi, grâce à l'action de l'AGC (Aquisition Gain Controller), qui commute immédiatement d'une antenne à l'autre suivant la puissance des signaux, le point d'accès est capable de distinguer deux signaux provenant de la même station. Les signaux reçus par ces deux antennes sont dit décorrélés (indépendants) s'ils sont séparés de Lambda/2 (6,25 cm à 2.4GHz).

Propriétés des milieux
L'affaiblissement de la puissance du signal est en grande partie du aux propriétés des milieux traversés par l'onde. Voici un tableau donnant les niveaux d'atténuation pour différents matériaux :

Matériaux	Affaiblissement	Exemples
Air	Aucun	Espace ouvert, cour intérieure
Bois	Faible	Porte, plancher, cloison
Plastique	Faible	Cloison
Verre	Faible	Vitres non teintées
Verre teinté	Moyen	Vitres teintées
Eau	Moyen	Aquarium, fontaine
Etres vivants	Moyen	Foule, animaux, humains, végétation
Briques	Moyen	Murs
Plâtre	Moyen	Cloisons
Céramique	Elevé	Carrelage
Papier	Elevé	Rouleaux de papier
Béton	Elevé	Murs porteurs, étages, piliers
Verre blindé	Elevé	Vitres pare-balles
Métal	Très élevé	Béton armé, miroirs, armoire métallique, cage d'ascenseur

3.1 MIMO

Comment ça marche ?
Equipant déjà les produits Wi-Fi de dernière génération, la technologie **Mimo** améliore les performances des réseaux sans fil en multipliant les signaux.

Comme d'autres systèmes de communication sans fil, le Wi-Fi utilise des ondes radio pour transmettre des informations. Le problème, c'est que ces signaux se dégradent avec la distance et avec les obstacles, limitant ainsi la portée et le débit de la liaison. D'où les piètres performances des déclinaisons actuelles du Wi-Fi (les normes 802.11b et 802.11g), notamment en intérieur, entre différentes pièces d'un bâtiment.

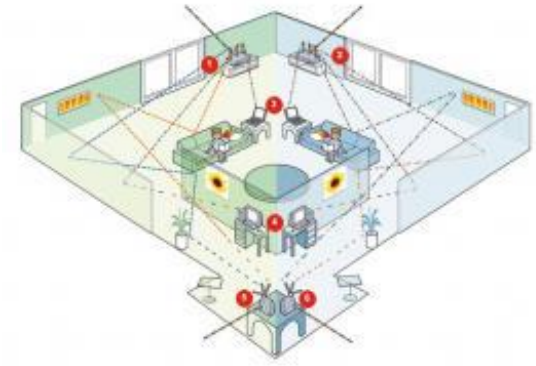
C'est justement pour améliorer les performances de ces liaisons sans fil que des fabricants spécialisés (Linksys, Netgear, Belkin ou D-Link, par exemple) exploitent depuis quelque temps dans leurs produits Wi-Fi une nouvelle technique baptisée **Mimo**. Le principe du **Mimo** (Multiple In, Multiple Out, soit multiples entrées, multiples sorties) est simple : il consiste à multiplier les signaux pour transmettre une même information. Peu importe que les ondes radio se dégradent avec la distance ou à cause des obstacles : les paquets de données qu'elles véhiculent sont réorganisés à l'arrivée pour reconstituer l'information d'origine.

Pour multiplier les signaux, les produits estampillés **Mimo** utilisent ainsi plusieurs antennes (jusqu'à huit). Mais ces antennes ne fonctionnent pas toutes de la même manière. De fait, deux méthodes coexistent actuellement, chacune défendue par un constructeur de circuit Wi-Fi (Airgo et Atheros).

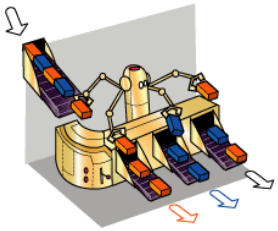
Deux techniques concurrentes
La technique d'Airgo consiste à envoyer simultanément des signaux fragmentés et complémentaires (partie gauche de l'illustration). De son côté, le système Atheros (partie droite de l'illustration) utilise la réplication : des signaux identiques voyagent simultanément, ce qui facilite la reconstruction des informations à l'arrivée.

Ces deux techniques n'offrent pas les mêmes performances. Avec la réplication (Atheros), c'est surtout la portée qui est augmentée, jusqu'à 120 mètres (contre seulement de 50 mètres avec du 802.11g). Avec la fragmentation (Airgo), c'est principalement le débit qui est amélioré (576 Mbit/s, contre 54 Mbit/s avec du 802.11g), davantage d'informations transitant simultanément. Un débit proche de celui d'une liaison filaire Ethernet classique (100 Mbit/s), plus que confortable pour partager une connexion à Internet, et même suffisant pour transmettre une vidéo en haute définition entre un ordinateur et un décodeur relié à un téléviseur, par exemple.

Pour l'heure, selon la technique utilisée, les produits estampillés **Mimo** sont incompatibles entre eux d'une marque à une autre. C'est la norme 802.11n, appellation officielle du futur « super Wi-Fi », qui mettra un terme à cette confrontation en adoptant, au second semestre 2007, l'une de ces deux techniques.

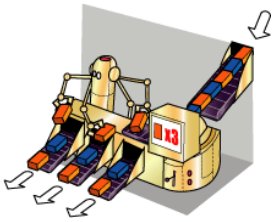


1 - Le signal d'origine est découpé par la borne Mimo



Avec le système préconisé par le fabricant de processeurs Airgo, la puce de la borne **Mimo** scinde le signal à transmettre en deux ou trois flux complémentaires de paquets de données. Chacun est envoyé, sous forme d'ondes, via une antenne distincte. Pour garantir la compatibilité avec les matériels Wi-Fi de génération précédente, cette borne diffuse en même temps, via une antenne spécifique, le signal d'origine dans son intégralité. Il contient donc tous les paquets de données à transmettre.

2 - Le signal d'origine est répliqué par la borne Mimo



Avec le système préconisé par le fabricant de processeurs Atheros, la puce de la borne **Mimo** réplique le signal d'origine en plusieurs flux de données, diffusés simultanément via plusieurs antennes. Cette technique permet de garantir la compatibilité des bornes **Mimo** avec les matériels Wi-Fi de générations précédentes (802.11b et 802.11g), incapables de reconstituer un signal fragmenté.

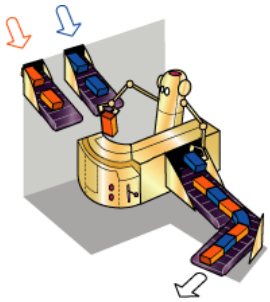
3 - Un seul signal est compris par un module 802.11g

Si aucun obstacle ne vient brouiller sa transmission, le signal complet (non fragmenté) émis par une ou plusieurs antennes de la borne **Mimo** peut être intercepté et interprété par un matériel Wi-Fi classique.

4 - Aucun signal n'est reçu par un module 802.11g éloigné

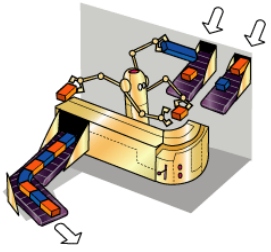
Placé derrière un obstacle filtrant les ondes radio (mur épais ou un meuble métallique, par exemple), un module Wi-Fi classique (à la norme 802.11b ou 802.11g) demeure incapable d'interpréter les signaux altérés ou atténués émis avec la technique **Mimo**.

5 - Le signal d'origine est reconstitué



Même altérés par des obstacles, les signaux demeurent interprétables à leur réception. Le processeur du module **Mimo** reconstitue le signal d'origine grâce à un algorithme. Comme s'il s'agissait d'un puzzle, il remet dans le bon ordre les paquets de données reçus.

6 - Le signal d'origine est reconstitué



Même altérés par des obstacles, les signaux demeurent interprétables à leur réception. Le processeur du module **Mimo** utilise un algorithme pour reconstituer le signal d'origine en superposant les différents flux de données reçus.

4 LA SÉCURITÉ

Le manque de sécurité
Les ondes radioélectriques ont intrinsèquement une grande capacité à se propager dans toutes les directions avec une portée relativement grande. Il est ainsi très difficile d'arriver à confiner les émissions d'ondes radio dans un périmètre restreint. La propagation des ondes radio doit également être pensée en trois dimensions. Ainsi les ondes se propagent également d'un étage à un autre (avec de plus grandes atténuations).

La principale conséquence de cette « propagation sauvage » des ondes radio est la facilité que peut avoir une personne non autorisée d'écouter le réseau, éventuellement en dehors de l'enceinte du bâtiment où le réseau sans fil est déployé.

Là où le bât blesse c'est qu'un réseau sans fil peut très bien être installé dans une entreprise sans que le service informatique ne soit au courant ! Il suffit en effet à un employé de brancher un point d'accès sur une prise réseau pour que toutes les communications du réseau soient rendues « publiques » dans le rayon de couverture du point d'accès !

Le War-driving
Etant donné qu'il est très facile d' « écouter » des réseaux sans fils, une pratique venue tout droit des Etats-Unis consiste à circuler dans la ville avec un ordinateur portable équipé d'une carte réseau sans fil à la recherche de réseaux sans fils, il s'agit du « **war driving** » (parfois noté wardriving ou war-Xing pour « war crossing »). Des logiciels spécialisés dans ce type d'activité permettent même d'établir une cartographie très précise en exploitant un matériel de géolocalisation (GPS, Global Positionning System).

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

Les risques en matière de sécurité
Les risques liés à la mauvaise protection d'un réseau sans fil sont multiples :

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

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

L'intrusion réseau
Lorsqu'un point d'accès est installé sur le réseau local, il permet aux stations d'accéder au réseau filaire et éventuellement à internet si le réseau local y est relié. Un réseau sans fil non sécurisé représente de cette façon un point d'entrée royal pour le pirate au réseau interne d'une entreprise ou une organisation.

Outre le vol ou la destruction d'informations présentes sur le réseau et l'accès à internet gratuit pour le pirate, le réseau sans fil peut également représenter une aubaine pour ce dernier dans le but de mener des attaques sur Internet. En effet étant donné qu'il n'y a aucun moyen d'identifier le pirate sur le réseau, l'entreprise ayant installé le réseau sans fil risque d'être tenue responsable de l'attaque.

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

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

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

Une infrastructure adaptée
La première chose à faire lors de la mise en place d'un réseau sans fil consiste à positionner intelligemment les points d'accès selon la zone que l'on souhaite couvrir. Il n'est toutefois pas rare que la zone effectivement couverte soit largement plus grande que souhaitée, auquel cas il est possible de réduire la puissance de la borne d'accès afin d'adapter sa portée à la zone à couvrir.

Eviter les valeurs par défaut
Lors de la première installation d'un point d'accès, celui-ci est configuré avec des valeurs par défaut, y compris en ce qui concerne le mot de passe de l'administrateur. Un grand nombre d'administrateurs en herbe considèrent qu'à partir du moment où le réseau fonctionne il est inutile de modifier la configuration du point d'accès. Toutefois les paramètres par défaut sont tels que la sécurité est minimale. Il est donc impératif de se connecter à l'interface d'administration (généralement via une interface web sur un port spécifique de la borne d'accès) notamment pour définir un mot de passe d'administration.

D'autre part, afin de se connecter à un point d'accès il est indispensable de connaître l'identifiant du réseau (SSID). Ainsi il est vivement conseillé de modifier le nom du réseau par défaut et de désactiver la diffusion (broadcast) de ce dernier sur le réseau. Le changement de l'identifiant réseau par défaut est d'autant plus important qu'il peut donner aux pirates des éléments d'information sur la marque ou le modèle du point d'accès utilisé.

Le filtrage des adresses MAC
Chaque adaptateur réseau (nom générique pour la carte réseau) possède une adresse physique qui lui est propre (appelée adresse MAC). Cette adresse est représentée par 12 chiffres hexadécimaux groupés par paires et séparés par des tirets.

Les points d'accès permettent généralement dans leur interface de configuration de gérer une liste de droits d'accès (appelée ACL) basée sur les adresses MAC des équipements autorisés à se connecter au réseau sans fil.

Cette précaution un peu contraignante permet de limiter l'accès au réseau à un certain nombre de machines. En contrepartie cela ne résout pas le problème de la confidentialité des échanges.

Le cryptage des réseaux sans fils
Les réseaux sans fils peuvent être cryptés de plusieurs manières :

- **WEP** (Wired Equivalent Privacy)
- **WPA** (Wi-Fi Protected Access)
- **WPA2** (Wi-Fi Protected Access, seconde generation)

WEP - Wired Equivalent Privacy
Pour remédier aux problèmes de confidentialité des échanges sur les réseaux sans fils, le standard 802.11 intègre un mécanisme simple de chiffrement des données, il s'agit du WEP, Wired equivalent privacy.

Le WEP est un protocole chargé du chiffrement des trames 802.11 utilisant l'algorithme symétrique RC4 avec des clés d'une longueur de 64 bits ou 128 bits. Le principe du WEP consiste à définir dans un premier temps une clé secrète de 40 ou 128 bits. Cette clé secrète doit être déclarée au niveau du point d'accès et des clients. La clé sert à créer un nombre pseudo-aléatoire d'une longueur égale à la longueur de la trame. Chaque transmission de donnée est ainsi chiffrée en utilisant le nombre pseudo-aléatoire comme masque grâce à un OU Exclusif entre le nombre pseudo-aléatoire et la trame.

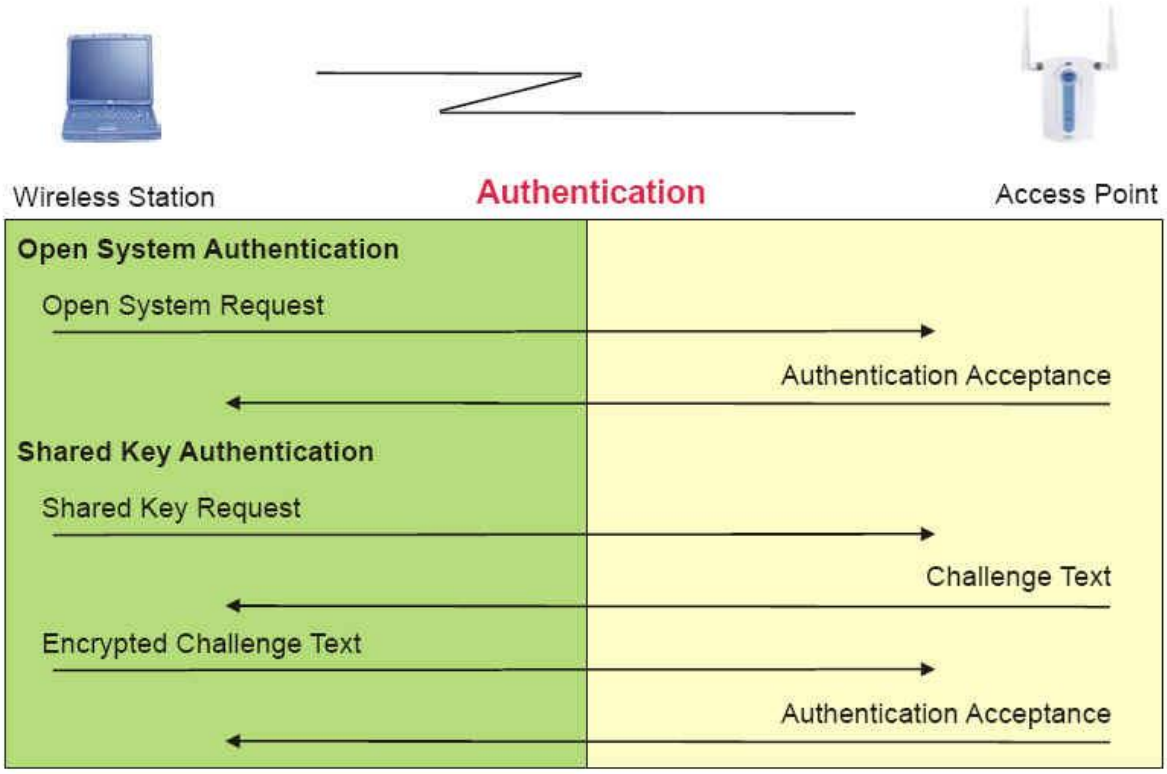
La clé de session partagée par toutes les stations est statique, c'est-à-dire que pour déployer un grand nombre de stations Wi-Fi il est nécessaire de les configurer en utilisant la même clé de session. Ainsi la connaissance de la clé est suffisante pour déchiffrer les communications.

De plus, 24 bits de la clé servent uniquement pour l'initialisation, ce qui signifie que seuls 40 bits de la clé de 64 bits servent réellement à chiffrer et 104 bits pour la clé de 128 bits.

Dans le cas de la clé de 40 bits, une attaque par force brute (c'est-à-dire en essayant toutes les possibilités de clés) peut très vite amener le pirate à trouver la clé de session. De plus une faille décelée par Fluhrer, Mantin et Shamir concernant la génération de la chaîne pseudo-aléatoire rend possible la découverte de la clé de session en stockant 100 Mo à 1 Go de trafic créés intentionnellement.

Le WEP n'est donc pas suffisant pour garantir une réelle confidentialité des données. Pour autant, il est vivement conseillé de mettre au moins en œuvre une protection WEP 128 bits afin d'assurer un niveau de confidentialité minimum et d'éviter de cette façon 90% des risques d'intrusion.

Fonctionnement d'un authentification WEP



Système d'authentification ouvert
Le système d'authentification implique une procédure de deux messages non-encryptés.

1. Une station envoie une demande ouverte d'authentification au point d'accès.
2. Le point d'accès va automatiquement accepter et connecter la station au réseau.

En effet, un système ouvert n'authentifie pas les stations.

Clé d'authentification partagée
L'authentification de clé partagée implique une procédure en quatre étapes.

1. Une station envoie une demande d'authentification à clé partagée au point d'accès.
2. Le point d'accès va ensuite répondre avec un message de texte défi.
3. La station doit utiliser la clé WEP du point d'accès pour encrypter le message de texte défi et le retourner au point d'accès.
4. Le point d'accès va essayer de décrypter le message en utilisant la clé WEP.

Si le message décrypté correspond au message de texte défi, la station est authentifiée.

Améliorer l'authentification
Afin de gérer plus efficacement les authentifications, les autorisations et la gestion des comptes utilisateurs (en anglais AAA pour Authentication, Authorization, and Accounting) il est possible de recourir à un serveur RADIUS (Remote Authentication Dial-In User Service). Le protocole RADIUS (défini par les RFC 2865 et 2866), est un système client/serveur permettant de gérer de façon centralisée les comptes des utilisateurs et les droits d'accès associés.

Mise en place d'un VPN
Pour toutes les communications nécessitant un haut niveau de sécurisation, il est préférable de recourir à un chiffrement fort des données en mettant en place un réseau privé virtuel (VPN).

WPA - Wi-Fi Protected Access
Le WPA est une version « allégée » du protocole 802.11i, reposant sur des protocoles d'authentification et un algorithme de cryptage robuste : TKIP (Temporary Key Integrity Protocol). Le protocole TKIP permet la génération aléatoire de clés et offre la possibilité de modifier la clé de chiffrement plusieurs fois par secondes, pour plus de sécurité.

Le fonctionnement de WPA repose sur la mise en œuvre d'un serveur d'authentification (la plupart du temps un serveur RADIUS), permettant d'identifier les utilisateurs sur le réseau et de définir leurs droits d'accès.

Le WPA (dans sa première mouture) ne supporte que les réseaux en mode infrastructure, ce qui signifie qu'il ne permet pas de sécuriser des réseaux sans fil d'égal à égal (mode ad hoc).

WPA-PSK – Wi-Fi Protected Access Pre Shared Key
Une variante du WPA est le WPA-PSK (Pre Shared Key). WPA-PSK est une version simplifiée pour une utilisation personnelle. La configuration du WPA-PSK commence par la détermination d'une clé statique ou « passphrase » tout comme le WEP. Mais à la différence du WEP, le WPA va utiliser TKIP pour faire une rotation des clés.

WPA est une solution de sécurisation de réseau Wi-Fi proposé par la « Wi-Fi Alliance », afin de combler les lacunes du WEP.

WPA2 - Wi-Fi Protected Access, seconde génération
La seconde version du « Wi-Fi Protected Access » vient renforcer la sécurité des réseaux sans-fil sans pour autant remiser la version précédente. Seule amélioration visible dans WPA2 : la présence du chiffrement par AES, le nouvel algorithme de chiffrement standard du gouvernement américain. Mais c'est de la présence d'AES que découle tout le reste.

Le support de ce protocole, requis par la norme 802.11i à laquelle obéit WPA2, lui permet ainsi de prétendre à la certification FIPS-140-2. Cette dernière est exigée dans le cadre des marchés gouvernementaux américains et par de nombreuses entreprises internationales dans leurs appels d'offre sécurité. WPA2 est donc la déclinaison du très attendu protocole 802.11i, ratifié en juin dernier par l'association Electrical and Electronics Engineers (IEEE). Ce protocole était attendu comme la pierre fondatrice des réseaux Wi-Fi sécurisés.

Fonctionnement d'une authentification WPA2 (4 way handshake)

Lorsqu'un client se connecte à un point d'accès protégé par le protocole WPA2, il y a un échange de 4 messages qui est effectué afin de pouvoir ensuite échanger des informations en les chiffrant dans le but de les rendre illisibles pour toute personne aux oreilles un peu trop pendues n'appartenant pas au réseau.

Pour pouvoir construire une clé qui chiffrera tout, chaque partie aura besoin du SSID, de la clé du point d'accès, des adresses MAC des deux parties, ainsi qu'un nombre aléatoire généré par chacun (ANonce-Client et SNonce-Point d'accès).

Si nous francisons ce handshake, ça ressemble à ça :

[Message 1] Point d'accès - Je t'envoie un numéro aléatoire (Anonce) et mon adresse MAC. Moi j'ai déjà mon SSID et la clé du réseau, me permettant de calculer une clé commune à tous (PMK)

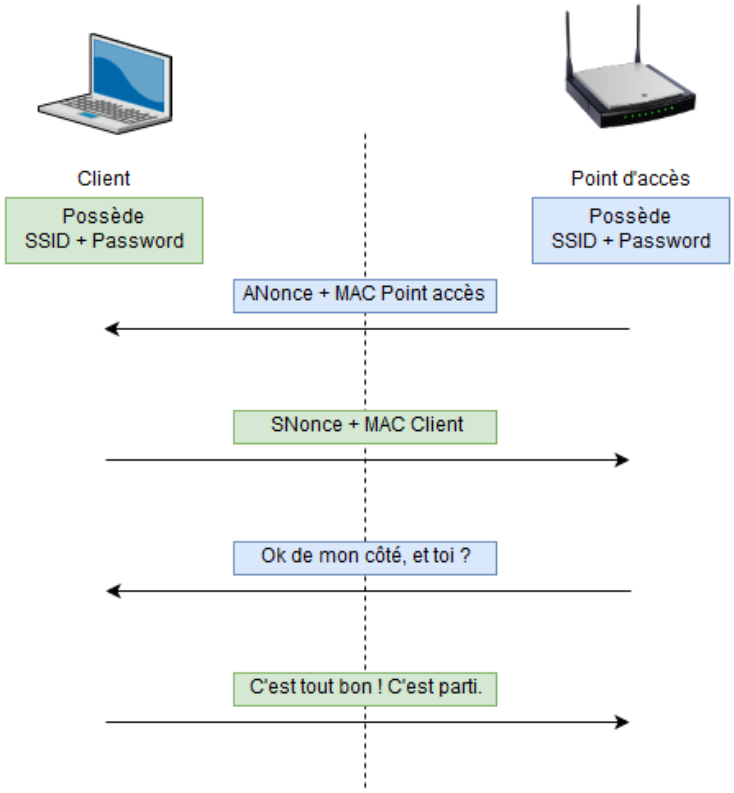
[Message 2] Client - Reçus ! J'ai fait une tambouille avec ton numéro (Anonce), un numéro que j'ai généré (Snonce), ton adresse MAC, mon adresse MAC, ton SSID et la clé (qui me donnent aussi la PMK), ça m'a donné la clé de chiffrement (PTK). Et du coup, je t'envoie mon numéro généré (Snonce) et mon adresse MAC pour que tu fasses la même tambouille.

[Message 3] Point d'accès - Reçus aussi. J'ai fait la même tambouille, donnant la clé de chiffrement (PTK). Thanks !

[Message 4] Client - Parfait ! Allez, discutons.

Une fois ce handshake effectué, une clé est partagée entre le client et le point d'accès sans jamais être passée sur le réseau, clé qui permettra de chiffrer le reste de la communication. Si jamais le client n'avait pas la bonne clé pour se connecter au point d'accès, alors la PMK était différente, ce qui entraine que la clé de chiffrement (PTK) n'est pas la même, et le client ne pourra pas communiquer avec le point d'accès.

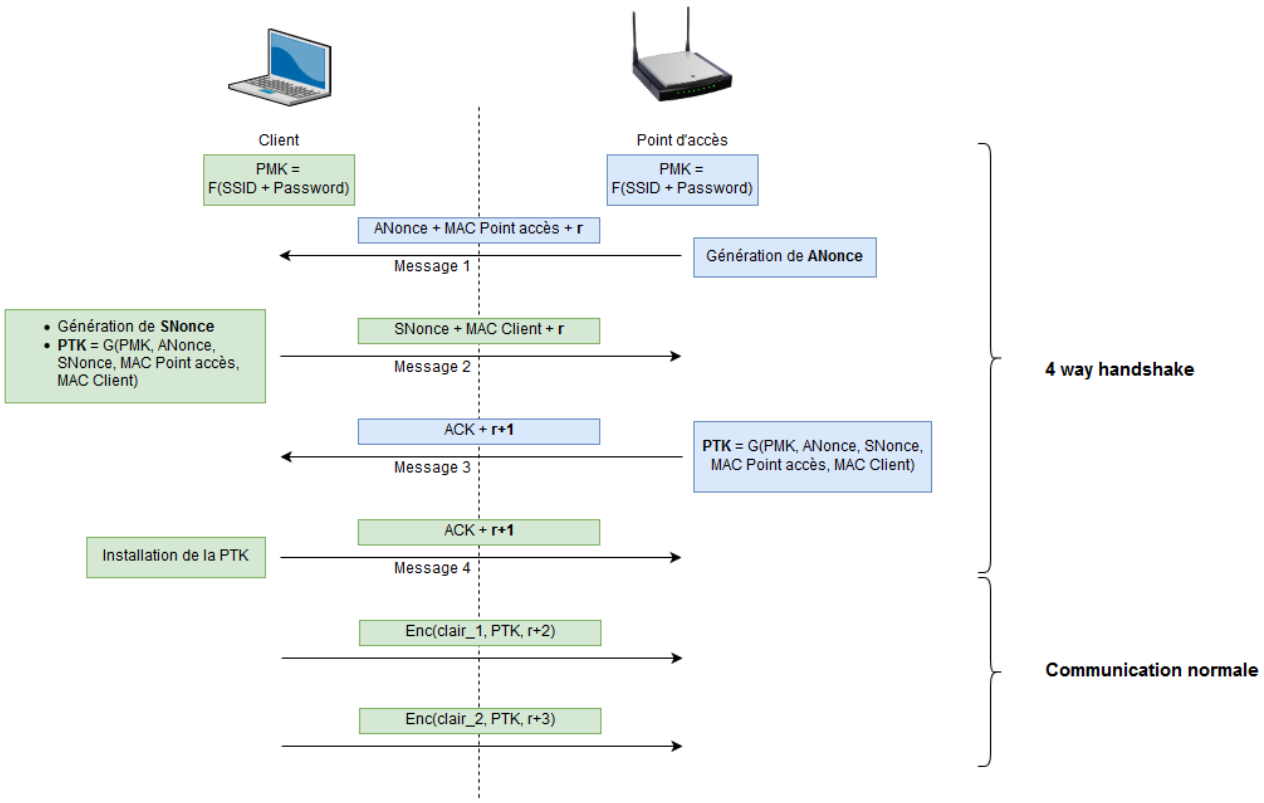
Voici un schéma qui résume cette communication



Il faut enfin ajouter un dernier élément, le compteur (Key Replay Counter). Celui-ci est généré au début du 4 way handshake et s'incrémente au fur et à mesure du handshake ainsi que dans toutes les communications qui suivront. Lorsque le premier message est envoyé, le point d'accès envoie une première valeur KRC. Le client répondra avec la même valeur, permettant au point d'accès de savoir à quel message 1 le client répond (plusieurs clients peuvent se connecter en même temps). Puis lors de l'envoi du deuxième message, le point d'accès l'incrémente, et le client répond avec cette nouvelle valeur.

Ensuite, pour les autres communications, ce compteur sera incrémenté à chaque message envoyé au point d'accès, on l'appelle d'ailleurs le PN (Packet Number) et ce compteur sera utilisé dans le chiffrement en tant que Nonce, ou IV (Initialization Vector), en garantissant une unicité pour chaque message. Si jamais deux messages sont chiffrés en utilisant le même Nonce, alors la solidité cryptographique tombe.

Voilà donc un schéma plus complet



Pour la culture, la fonction G qui permet de dériver la PMK afin de donner la PTK est une fonction pseudo aléatoire (Pseudo Random Function - PRF) basée sur HMAC utilisant SHA1 comme méthode de hachage.

Attaque : Key Reinstallation

Contexte et normes

Nous avons donc une vision assez claire de ce qu'il se passe lorsqu'un client tente de communiquer avec un point d'accès protégé via le protocole WPA2. Il y a un 4 way handshake qui permet aux deux entités de se mettre d'accord sur une clé de chiffrement temporaire qui a deux buts: Le premier est d'assurer au point d'accès que le client possède son mot de passe. En effet, si ce n'est pas le cas, les deux clés de chiffrement seront différentes et les deux entités ne pourront pas communiquer. Deuxièmement, cette clé de chiffrement temporaire permet aux deux entités de communiquer de manière chiffrée afin qu'un attaquant qui écoute sur le réseau ne puisse pas déchiffrer ou décrypter les communications.

Différents protocoles existent pour le chiffrement et la vérification d'intégrité des données une fois que la clé partagée a été calculée, par exemple TKIP (Temporal Key Integrity Protocol), qui est déprécié aujourd'hui, (AES-) CCMP (Counter-mode/CBC-Mac Protocol), largement utilisé de nos jours, ou encore GCMP (Galios/Counter Mode Protocol) également très utilisé.

Les deux derniers (CCMP et GCMP) sont deux protocoles très robustes tant que les règles sont suivies, notamment le fait de ne jamais réutiliser un même Nonce pour chiffrer deux messages.

C'est cette condition qui entre en jeu dans l'attaque KRACK.

Dans la partie précédente, nous avons vu que le Nonce utilisé pour chiffrer les communications est le PN (Packet Number), qui est incrémenté à chaque message. Jusqu'ici, pas de problème puisque cela garanti son unicité pour chacun des messages. Si un message se perd et que le client doit le renvoyer, il le renverra avec un PN incrémenté afin de continuer de garantir l'unicité du Nonce dans le protocole de chiffrement.

Il y a cependant un point un peu gris dans la norme IEEE 802.11 (avec l'amendement 802.11i - WPA2) sur la gestion des messages retransmis dans le 4 way handshake. Heureusement l'amendement 802.11r (FT - Fast Basic Service State Transition, qui précise et améliore la bascule de point d'accès quand une personne se déplace) a donné un schéma d'états précisant tout cela. Les deux points importants sont les suivants :

- Le point d'accès doit retransmettre les messages 1 et 3 s'il n'a pas reçu de réponse de la part du client, impliquant que le client doit gérer ces retransmissions.
- Le client doit installer la PTK suite à la réception du message 3, ce qui a pour effet de mettre à jour le compteur, égal à celui reçu dans ce 3ème message

Là où ça coince

Grâce aux deux idées du paragraphe précédent :

- Les deux protocoles CCMP et GCMP sont très robustes tant que les règles sont suivies, notamment le fait de ne jamais réutiliser un même Nonce pour chiffrer deux messages;
- Le client doit installer la PTK suite à la réception du message 3, ce qui a pour effet de mettre à jour le compteur, égal à celui reçu dans ce message.

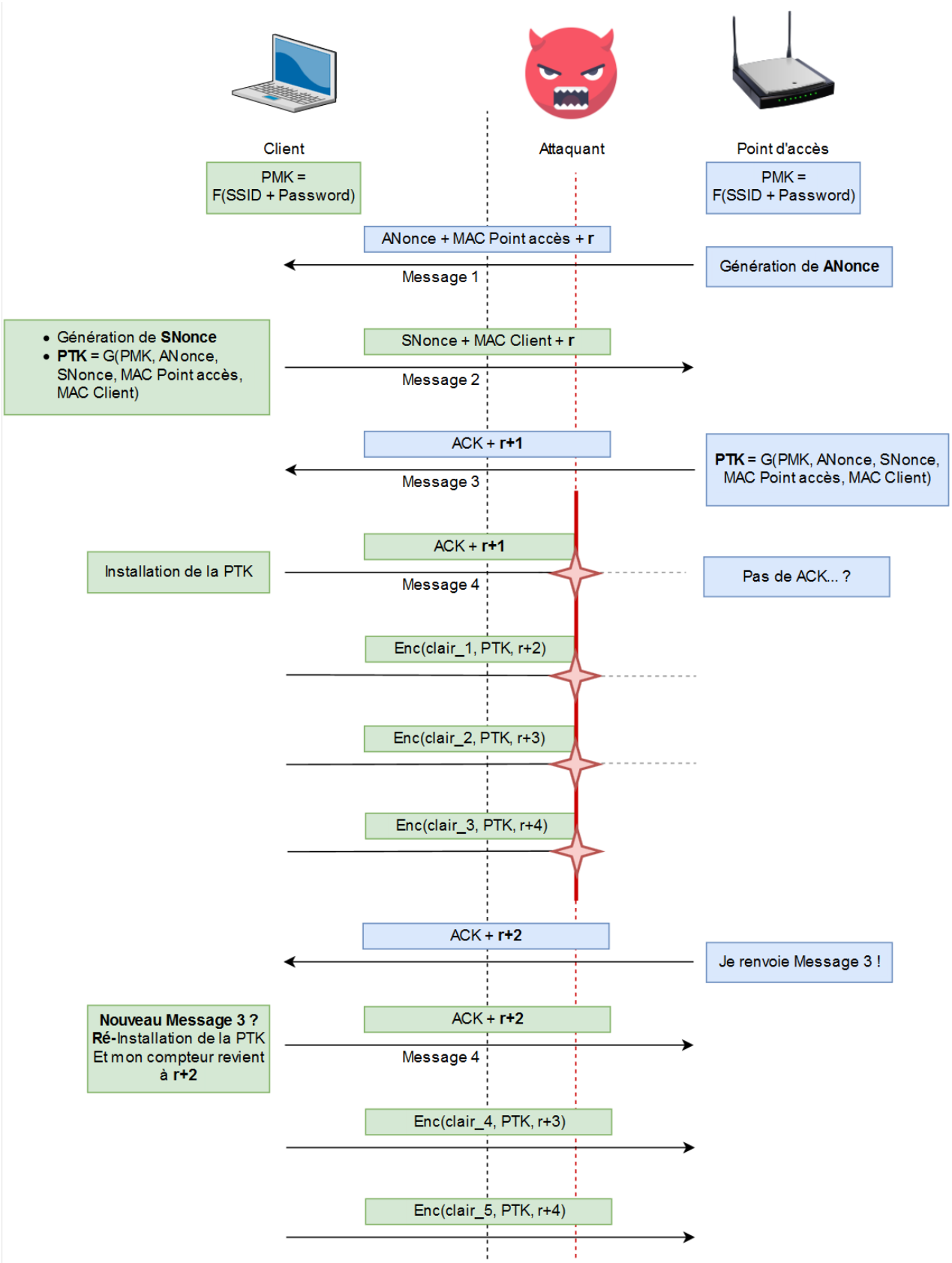
Nous pouvons maintenant bien comprendre comment peut se dérouler une attaque. Si l'attaquant se place entre le client et le point d'accès, et laisse passer les 3 premiers messages, mais qu'il bloque le 4ème message, c'est à dire l'acquittement du client envoyé au point d'accès, on se trouve dans la situation suivante :

Le client a envoyé son acquittement, donc de son point de vue, le 4 way handshake est terminé, et il peut commencer à communiquer en envoyant différents messages chiffrés avec la PTK, et avec le compteur qui s'incrémente, compteur qui joue le rôle de Nonce.

Le point d'accès quant à lui n'a pas reçu l'acquittement. Ainsi, pour lui, le 4 way handshake n'est pas complet. Après un certain timeout, il va donc renvoyer le 3ème message au client. Comme le client doit réinstaller la PTK suite à la réception du message 3, même s'il a terminé le 4 way handshake, il va recevoir une nouvelle fois ce 3ème message, et il va réinstaller la PTK (qui n'a pas changé) puis renvoyer un acquittement, pour enfin continuer de communiquer avec le point d'accès, en recommençant avec le compteur égal à celui du 3ème message, qu'il incrémente à nouveau pour la suite.

C'est ici que nous avons le souci. De nouveaux messages vont être chiffrés et envoyés par le client, mais ils vont être chiffrés avec un Nonce qu'il a déjà utilisé. Et là, c'est le drame, toute la force cryptographique tombe, comme nous avons pu le voir rapidement dans le premier paragraphe. Il devient possible de décrypter des messages reçus par le client alors que nous n'avons pas la clé permettant de nous connecter au réseau, ce qui est exactement l'inverse du principe de WPA2.

Voici un petit schéma qui résume ce principe



Nous avons donc les ***clair_1, clair_2, clair_3*** qui ont été chiffrés avec les Nonces ***r+2, r+3, r+4***, puis suite à la réinstallation de la PTK, les ***clair_4, clair_5*** ont été à nouveau chiffrés avec les ***Nonce r+3, r+4***. Il ne faut alors plus longtemps pour casser le protocole cryptographique qui doit protéger les messages, comme vu dans le début de cet article.

En effet, dans cet exemple nous avons :

msg_chiffré_2 = clair_2 XOR F(PTK, r+3)
msg_chiffré_4 = clair_4 XOR F(PTK, r+3)

Le même Nonce r+3 est utilisé pour chiffrer deux messages différents. Si nous connaissons clair_2 par exemple, nous pouvons réduire ces deux égalités à la suivante :

msg_chiffre_2 XOR clair_2 XOR msg_chiffré_4 = clair_4

Ainsi, sans connaissance de la clé PTK, nous pouvons déduire le ***clair_4***.

Comment s'en protéger
Si vous avez bien compris le principe de l'attaque, vous devriez alors déjà imaginer différentes solutions pour se protéger de celle-ci. Il est possible de se protéger à deux niveaux.

Protection au niveau du point d'accès
Ce paragraphe explique une manière de protéger les clients en configurant le point d'accès, cependant l'attaquant peut rejouer manuellement le message 3 en incrémentant le compteur, ce qui aura tout de même pour effet de réinstaller la PTK et réinitialiser le compteur chez le client. Ainsi, je ne pense pas que la solution que j'avais proposée soit fonctionnelle. Par ailleurs, il existe plusieurs variantes de l'attaque, visant parfois les points d'accès, parfois les clients. Il convient alors de mettre à jour les deux acteurs.

C'est la partie qui semble la plus efficace à protéger puisque si nous y arrivons, alors l'ensemble des clients qui se connecteront à ce point d'accès ne sont plus vulnérables. Cependant c'est également celle qui a le plus gros impact. L'attaque reposant sur le fait que le client ne réponde pas suite au message 3, et que le point d'accès renvoie ce message, il est possible de corriger le problème en décidant que si le point d'accès ne reçoit pas de réponse, alors celui-ci déconnecte le client. Le client devra alors recommencer un 4 way handshake afin de se connecter. C'est cependant un changement assez radical dans l'implémentation du protocole.

Protection au niveau du client
Il est également possible de faire en sorte que la procédure du client lors du 4 way handshake soit à états, c'est à dire que le client se souvienne des actions précédentes. Ainsi, s'il a déjà installé une clé, et que le point d'accès lui renvoie le message 3, alors le client peut tout à fait décider que sa clé est déjà installée, et que par conséquent il ne la réinstallera pas, et ne réinitialisera pas son compteur, utilisé comme Nonce pour le principe cryptographique. C'est la manière la plus propre de se protéger du problème, cependant cela implique qu'il faut changer le comportement de tous les clients.

5 BIBLIOGRAPHIE

5.1 LIVRES

Jean-François Pillou, *Tout sur la sécurité informatique*, Dunod, Paris, 2005
Jean-François Pillou, *Tout sur les réseaux et Internet*, Dunod, Paris, 2006

5.2 SUPPORTS DE COURS

5.3 LIENS INTERNET

http://www.commentcamarche.net
http://fr.wikipedia.org
http://www.dslvalley.com
http://www.alcatel.com
http://www.towercast.fr/
http://surpinsat.com/actualite/nokia9902.htm
http://www-isis.enst.fr/Documents/RapportsGDR/OP62/CR62_JJMM.html
http://www.zyxel.fr/ratgeber.cfm?action=detail&id=10047&area=3&lang=f
http://beta.hackndo.com/krack/
http://www.01net.com/article/323148.htm
(Jean-Marie Portal , L'Ordinateur Individuel, le 02/08/2006 à 07h00)