

de A à Z

Présentation du WiFi (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** (contraction de *Wireless Fidelity*, parfois notée à tort *WiFi*) correspond initialement au nom donnée 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 (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 répondant à la norme 802.11. Les matériels certifiés par la Wi-Fi Alliance bénéficient de la possibilité d'utiliser le logo suivant :

Grâce au Wi-Fi il est possible de créer des réseaux locaux sans fils à haut débit pour peu que la station 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 machines 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, hotels, trains, ...) avec des réseaux sans fils. Ces zones d'accès sont appelées "**hot spots**".

Présentation du WiFi (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 radio-électriques 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 :

Couche Liaison de données (MAC)	802.2
	802.11
Couche Physique (PHY)	DSSS FHSS Infrarouges

Il est possible d'utiliser n'importe quel protocole de haut niveau sur un réseau sans fil WiFi au même titre que sur un réseau *ethernet*.

Les différentes normes WiFi

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 et 802.11g, 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	Wifi5	La norme 802.11a (baptisé <i>WiFi 5</i>) 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	Wifi	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 <i>liaison de données</i>).
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 <i>liaison de données</i> . 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 <i>Inter-Access point roaming protocol</i> 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 <i>itinérance</i> (ou <i>roaming en anglais</i>)
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 <i>802.11h</i> vise à rapprocher la norme 802.11 du standard Européen (HiperLAN 2, d'où le <i>h</i> de 802.11h) et être en conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie.
802.11i		La norme <i>802.11i</i> a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l' <i>AES (Advanced Encryption Standard)</i> et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
802.11r		La norme <i>802.11r</i> a été élaborée de telle manière à utiliser des signaux infra-rouges. Cette norme est désormais dépassée techniquement.
802.11j		La norme <i>802.11j</i> est à la réglementation japonaise ce que le 802.11h est à la réglementation européenne.

Il est intéressant de noter l'existence d'une norme baptisée «*802.11b+*». Il s'agit d'une norme propriétaire proposant des améliorations en terme 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, 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.

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 le équipements 802.11b. Il existe toutefois des matériels intégrant des puces 802.11a et 802.11b, on parle alors de matériels «**dual band**».

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

802.11b

La norme 802.11b permet d'obtenir un débit théorique de 11 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).

Débit théorique	Portée (en intérieur)	Portée (à l'extérieur)
11 Mbits/s	50 m	200 m
5,5 Mbits/s	75 m	300 m
2 Mbits/s	100 m	400 m
1 Mbit/s	150 m	500 m

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.

Débit théorique	Portée (en intérieur)	Portée (à l'extérieur)
54 Mbits/s	27 m	75 m
48 Mbits/s	29 m	100 m
36 Mbits/s	30 m	120 m
24 Mbit/s	42 m	140 m
18 Mbit/s	55 m	180 m
12 Mbit/s	64 m	250 m
9 Mbit/s	75 m	350 m
6 Mbit/s	90 m	400 m

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

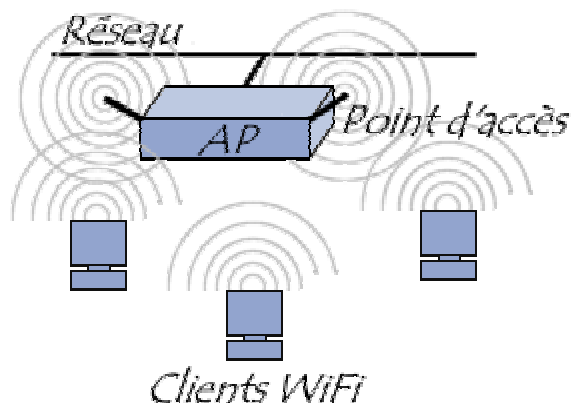
- Les **adaptateurs sans fils** ou **cartes d'accès** (en anglais *wireless adapters* ou *network interface controller*, noté *NIC*) : il s'agit d'une carte réseau à la norme 802.11 permettant à une machine de se connecter à un réseau sans fil. Les adaptateurs WiFi sont disponibles dans de nombreux formats (carte PCI, carte PCMCIA, adaptateur USB, carte CompactFlash, ...). 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 wifi.

Le standard 802.11 définit deux modes opératoires :

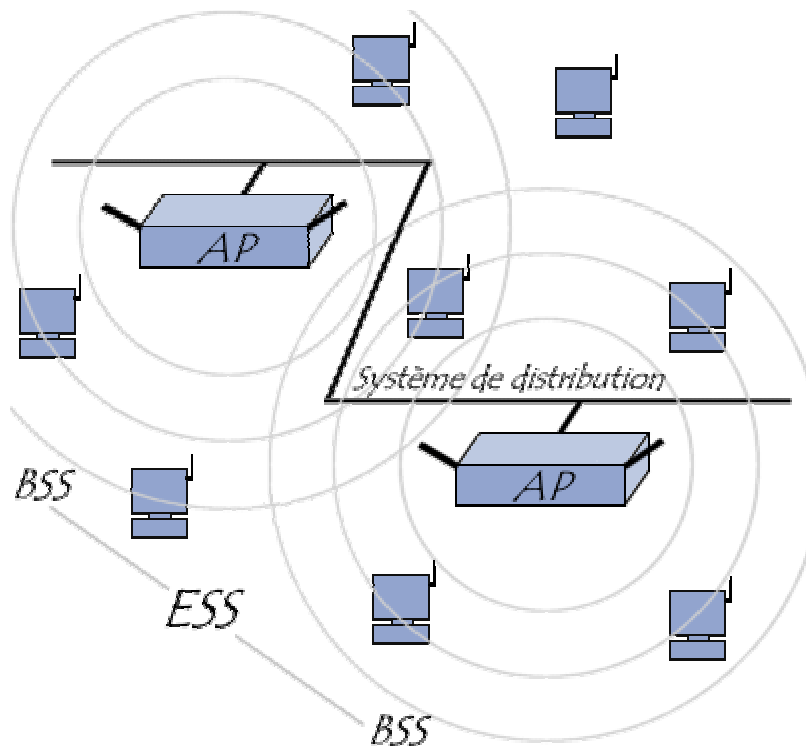
- Le mode infrastructure dans lequel les clients sans fils sont connectés à un point d'accès. Il s'agit généralement du mode par défaut des cartes 802.11b.
- Le mode ad hoc dans lequel les clients sont connectés les uns aux autres sans aucun point d'accès.

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 sorte 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 un 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 présents 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.

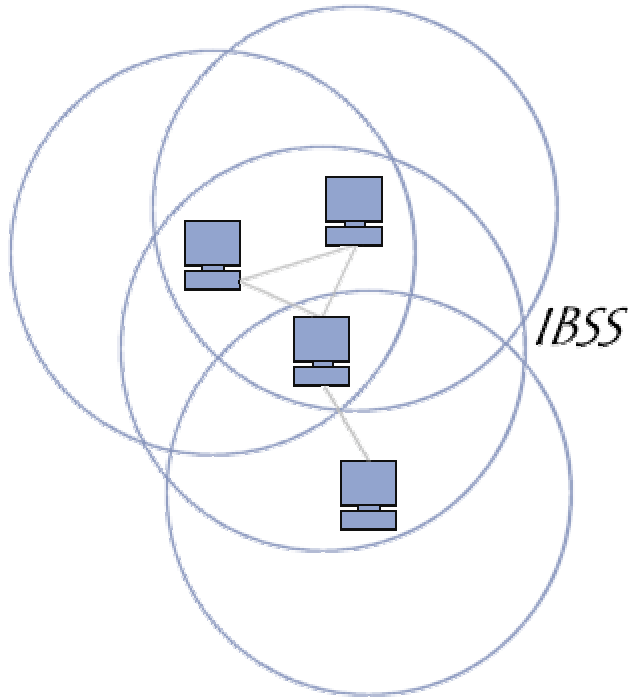
Une station se trouvant à la portée de plusieurs points d'accès (possédant bien évidemment le même SSID) pourra ainsi **choisir** le point d'accès offrant le meilleur compromis de débit et de charge.



Lorsqu'une station se trouve dans le rayon d'action de plusieurs points d'accès, c'est elle qui choisit auquel se connecter !

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 **independent 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 déterminé par la portée de chaque station. Cela signifie que si deux des stations du réseaux 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.

Les canaux de transmission

On appelle *canal de transmission* une bande étroite de fréquence utilisable pour une communication. Dans chaque pays, le gouvernement est en général le régulateur de l'utilisation des bandes de fréquences, car il est souvent le principal consommateur pour des usages militaires.

Toutefois les gouvernements proposent des bandes de fréquence pour une utilisation libre, c'est-à-dire ne nécessitant pas de licence de radiocommunication. Les organismes chargés de réguler l'utilisation des fréquences radio sont :

- l'ETSI (*European Telecommunications Standards Institute*) en Europe
- la FCC (*Federal Communications Commission*) aux Etats-Unis
- le MKK (*Kensa-kentei Kyokai*) au Japon

En 1985 les Etats-Unis ont libéré trois bandes de fréquence à destination de l'Industrie, de la Science et de la Médecine. Ces bandes de fréquence, baptisées *ISM (Industrial, Scientific, and Medical)*, sont les bandes 902-928 MHz, 2.400-2.4835 GHz, 5.725-5.850 GHz.

En Europe la bande s'étalant de 890 à 915 MHz est utilisée pour les communications mobiles (*GSM*), ainsi seules les bandes 2.400 à 2.4835 GHz et 5.725 à 5.850 GHz sont disponibles pour une utilisation radio-amateur.

Les technologies de transmission

Les réseaux locaux radio-électriques utilisent des ondes radio ou infrarouges afin de transmettre des données. La technique utilisée à l'origine pour les transmissions radio est appelé transmission en bande étroite, elle consiste à passer les différentes communications sur des canaux différents. Les transmissions radio sont toutefois soumises à de nombreuses contraintes rendant ce type de transmission non suffisantes. Ces contraintes sont notamment :

- Le partage de la bande passante entre les différentes stations présentes dans une même cellule.
- La propagation par des chemins multiples d'une onde radio. Un onde radio peut en effet se propager dans différentes direction et éventuellement être réfléchié ou réfractés par des objets de l'environnement physique, si bien qu'un récepteur peut être amené recevoir à quelques instants d'intervalles deux mêmes informations ayant emprunté des cheminements différents par réflexions successives.

La couche physique de la norme 802.11 définit ainsi initialement plusieurs techniques de transmission permettant de limiter les problèmes dûs aux interférences :

- La technique de l'étalement de spectre à saut de fréquence,
- La technique de l'étalement de spectre à séquence directe,
- La technologie infrarouge.

La technique à bande étroite

La technique à bande étroite (*narrow band*) consiste à utiliser une fréquence radio spécifique pour la transmission et la réception de données. La bande de fréquence utilisée doit être aussi petite que possible afin de limiter les interférences sur les bandes adjacentes.

Les techniques d'étalement de spectre

La norme *IEEE 802.11* propose deux techniques de modulation de fréquence pour la transmission de données issues des technologies militaires. Ces techniques, appelées *étalement de spectre* (en anglais *spread spectrum*) consistent à utiliser une bande de fréquence large pour transmettre des données à faible puissance. On distingue deux techniques d'étalement de spectre :

- La technique de l'étalement de spectre à saut de fréquence,
- La technique de l'étalement de spectre à séquence directe

La technique de saut de fréquence

La technique **FHSS** (*Frequency Hopping Spread Spectrum*, en français *étalement de spectre par saut de fréquence* ou *étalement de spectre par évacion de fréquence*) consiste à découper la large bande de fréquence en un minimum de 75 canaux (*hops* ou *sauts* d'une largeur de 1MHz), puis de transmettre en utilisant une combinaison de canaux connue de toutes les stations de la cellule. Dans la norme 802.11, la bande de fréquence 2.4 - 2.4835 GHz permet de créer 79 canaux de 1 MHz. La transmission se fait ainsi en émettant successivement sur un canal puis sur un autre pendant une courte période de temps (d'environ 400 ms), ce qui permet à un instant donné de transmettre un signal plus facilement reconnaissable sur une fréquence donnée.

L'*étalement de spectre par saut de fréquence* a originalement été conçu dans un but militaire afin d'empêcher l'écoute des transmissions radio. En effet, une station ne connaissant pas la combinaison de

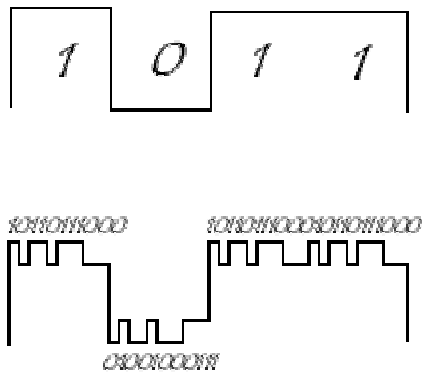
fréquence à utiliser ne pouvait pas écouter la communication car il lui était impossible dans le temps imparti de localiser la fréquence sur laquelle le signal était émis puis de chercher la nouvelle fréquence.

Aujourd'hui les réseaux locaux utilisant cette technologie sont standards ce qui signifie que la séquence de fréquences utilisées est connue de tous, l'étalement de spectre par saut de fréquence n'assure donc plus cette fonction de sécurisation des échanges. En contrepartie, le FHSS est désormais utilisé dans le standard 802.11 de telle manière à réduire les interférences entre les transmissions des diverses stations d'une cellule.

Etalement de spectre à séquence directe

La technique **DSSS** (*Direct Sequence Spread Spectrum, étalement de spectre à séquence directe*) consiste à transmettre pour chaque bit une séquence *Barker* (parfois appelée *bruit pseudo-aléatoire* ou en anglais *pseudo-random noise*, noté *PN*) de bits. Ainsi chaque bit valant 1 est remplacé par une séquence de bits et chaque bit valant 0 par son complément.

La couche physique de la norme 802.11 définit une séquence de 11 bits (*10110111000*) pour représenter un 1 et son complément (*01001000111*) pour coder un 0. On appelle *chip* ou *chipping code* (en français *puce*) chaque bit encodé à l'aide de la séquence. Cette technique (appelée *chipping*) revient donc à moduler chaque bit avec la séquence *barker*.



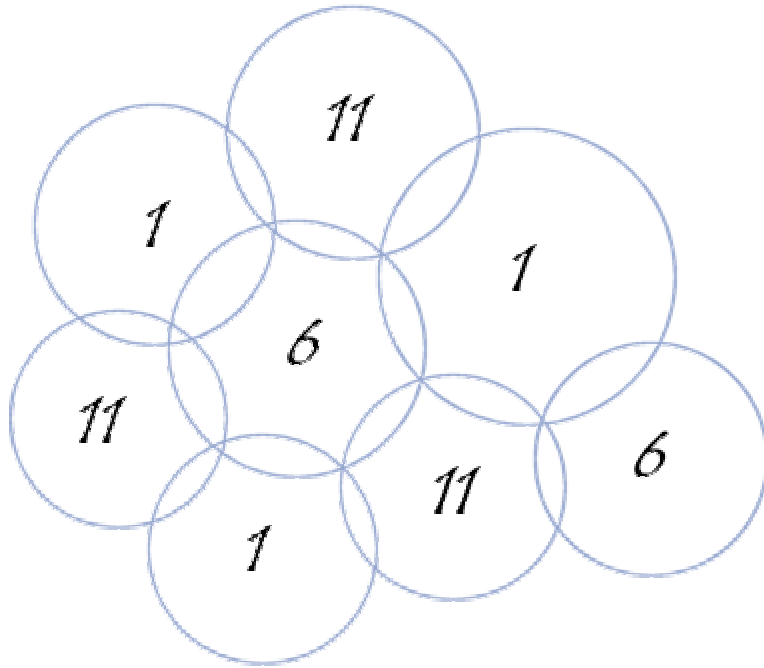
Grâce au *chipping*, de l'information redondante est transmise, ce qui permet d'effectuer des contrôles d'erreurs sur les transmissions, voire de la correction d'erreurs.

Dans le standard 802.11b, la bande de fréquence 2.400-2.4835 GHz (d'une largeur de 83.5 MHz) a été découpée en 14 canaux séparés de 5MHz, dont seuls les 11 premiers sont utilisables aux Etats-Unis. Seuls les canaux 10 à 13 sont utilisables en France. Voici les fréquences associées aux 14 canaux :

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

Toutefois, pour une transmission de 11 Mbps correcte il est nécessaire de transmettre sur une bande de 22 MHz car, d'après le théorème de Shannon, la fréquence d'échantillonnage doit être au minimum égale au double du signal à numériser. Ainsi certains canaux recouvrent partiellement les canaux adjacents, c'est la raison pour laquelle des canaux isolés (les canaux 1, 6 et 11) distants les uns des autres de 25MHz sont généralement utilisés.

Ainsi, si deux points d'accès utilisant les mêmes canaux ont des zones d'émission qui se recoupent, des distorsions du signal risquent de perturber la transmission. Ainsi pour éviter toute interférence il est recommandé d'organiser la répartition des points d'accès et l'utilisation des canaux de telle manière à ne pas avoir deux points d'accès utilisant les mêmes canaux proches l'un de l'autre.



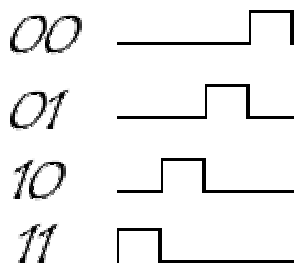
Le standard 802.11a utilise la bande de fréquence 5.15GHz à 5.35GHz et la bande 5.725 GHz à 5.825 GHz, ce qui permet de définir 8 canaux distincts d'une largeur de 20Mhz chacun, c'est-à-dire une bande suffisamment large pour ne pas avoir de parasitage entre canaux.

La technologie infrarouge

Le standard IEEE 802.11 prévoit également une alternative à l'utilisation des ondes radio : la lumière infrarouge. La technologie infrarouge a pour caractéristique principale d'utiliser une onde lumineuse pour la transmission de données. Ainsi les transmissions se font de façon uni-directionnelle, soit en "vue directe" soit par réflexion. Le caractère non dissipatif des ondes lumineuses offre un niveau de sécurité plus élevé.

Il est possible grâce à la technologie infrarouge d'obtenir des débits allant de 1 à 2 Mbit/s en utilisant une modulation appelé **PPM** (*pulse position modulation*).

La modulation *PPM* consiste à transmettre des impulsions à amplitude constante, et à coder l'information suivant la position de l'impulsion. Le débit de 1 Mbps est obtenu avec une modulation de *16-PPM*, tandis que le débit de 2 Mbps est obtenu avec une modulation *4-PPM* permettant de coder deux bits de données avec 4 positions possibles :



Les techniques de modulation

Tandis que la radio classique utilise une modulation de fréquence (*radio FM* pour *Frequency Modulation*) ou bien une modulation d'amplitude (*radio AM* pour *Amplitude Modulation*), le standard 802.11b utilise une technique de modulation de phase appelée *PSK* pour *Phase Shift Keying*. Ainsi chaque bit produit une rotation de phase. Une rotation de 180° permet de transmettre des débits peu élevés (technique

appelé *BPSK* pour *Binary Phase Shift Keying*) tandis qu'une série de quatre rotations de 90° (technique appelé *QPSK* pour *Quadrature Phase Shift Keying*) permet des débits deux fois plus élevés.

Optimisations

La norme 802.11b propose d'autres types d'encodage permettant d'optimiser le débit de la transmission. Les deux séquences Barker ne permettent de définir que deux états (0 ou 1) à l'aide de deux mots de 11 bits (compléments l'un de l'autre).

Une méthode alternative appelée *CCK* (*complementary code keying*) permet d'encoder directement plusieurs bits de données en une seule puce (*chip*) en utilisant 8 séquences de 64 bits. Ainsi en codant simultanément 4 bits, la méthode *CCK* permet d'obtenir un débit de 5.5 Mbps et elle permet d'obtenir un débit de 11 Mbps en codant 8 bits de données.

La technologie *PBCC* (*Packet Binary Convolutionary Code*) permet de rendre le signal plus robuste vis-à-vis des distorsions dues au cheminement multiple des ondes hertziennes. Ainsi la société *Texas Instrument* a réussi à mettre au point une séquence tirant avantage de cette meilleure résistance aux interférences et offrant un débit de 22Mbit/s. Cette technologie baptisée *802.11b+* est toutefois non conforme à la norme *IEEE 802.11b* ce qui rend les périphériques la supportant non compatibles avec les équipements 802.11b.

La norme 802.11a opère dans la bande de fréquence des 5 GHz, qui offre 8 canaux distincts, c'est la raison pour laquelle une technique de transmission alternative tirant partie des différents canaux est proposée. L'*OFDM* (*Orthogonal Frequency Division Multiplexing*) permet d'obtenir des débits théoriques de 54 Mbps en envoyant les données en parallèle sur les différentes fréquences. De plus la technique *OFDM* fait une utilisation plus rationnelle du spectre.

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

La couche liaison de données

La couche *Liaison de données* de la norme 802.11 est composée de deux sous-couches : la couche de *contrôle de la liaison logique* (*Logical Link Control*, notée **LLC**) et la couche de *contrôle d'accès au support* (*Media Access Control*, ou **MAC**).

La couche *MAC* définit deux méthodes d'accès différentes :

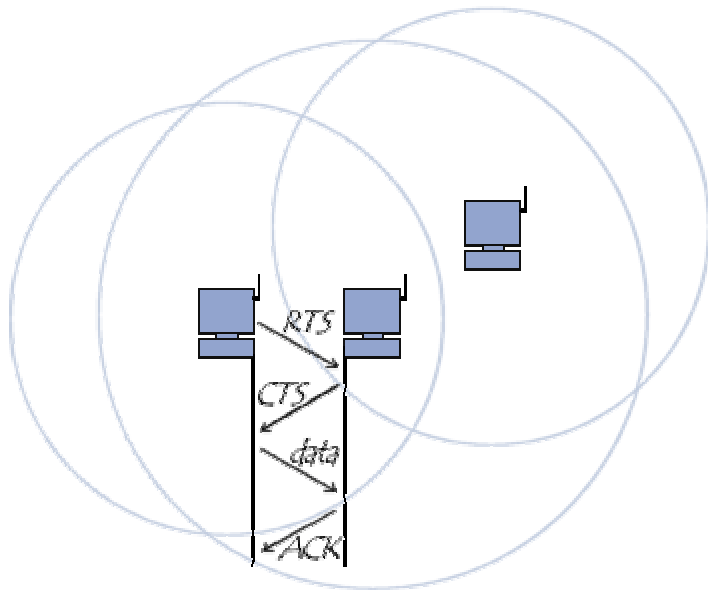
- La méthode *CSMA/CA* utilisant la *Distributed Coordination Function* (*DCF*)
- La *Point Coordination Function* (*PCF*)

La méthode d'accès CSMA/CA

Dans un réseau local Ethernet classique, la méthode d'accès utilisée par les machines est le *CSMA/CD* (*Carrier Sense Multiple Access with Collision Detect*), pour lequel chaque machine est libre de communiquer à n'importe quel moment. Chaque machine envoyant un message vérifie qu'aucun autre message n'a été envoyé en même temps par une autre machine. Si c'est le cas, les deux machines patientent pendant un temps aléatoire avant de recommencer à émettre.

Dans un environnement sans fil ce procédé n'est pas possible dans la mesure où deux stations communiquant avec un récepteur ne s'entendent pas forcément mutuellement en raison de leur rayon de portée. Ainsi la norme 802.11 propose un protocole similaire appelé **CSMA/CA** (*Carrier Sense Multiple Access with Collision Avoidance*).

Le protocole CSMA/CA utilise un mécanisme d'esquive de collision basé sur un principe d'accusé de réceptions réciproques entre l'émetteur et le récepteur :



La station voulant émettre écoute le réseau. Si le réseau est encombré, la transmission est différée. Dans le cas contraire, si le média est libre pendant un temps donné (appelé *DIFS* pour *Distributed Inter Frame Space*), alors la station peut émettre. La station transmet un message appelé *Ready To Send* (noté *RTS* signifiant *prêt à émettre*) contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission. Le récepteur (généralement un point d'accès) répond un *Clear To Send* (*CTS*, signifiant *Le champ est libre pour émettre*), puis la station commence l'émission des données.

A réception de toutes les données émises par la station, le récepteur envoie un accusé de réception (*ACK*). Toutes les stations avoisinantes patientent alors pendant un temps qu'elle considère être celui nécessaire à la transmission du volume d'information à émettre à la vitesse annoncée.

Somme de contrôle

La couche MAC du protocole 802.11 offre un mécanisme de contrôle d'erreur permettant de vérifier l'intégrité des trames. Il s'agit là d'une différence fondamentale avec le standard Ethernet. En effet Ethernet ne propose aucun système de détection ou de correction d'erreurs, cette tâche étant laissée aux protocoles de transports de niveau supérieur (TCP).

Dans un réseau sans fil le taux d'erreur est plus élevé, c'est la raison pour laquelle un contrôle d'erreur a été intégré au niveau de la couche liaison de données. Le contrôle d'erreur est basé sur le polynôme de degré 32 suivant :

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

Fragmentation et réassemblage

D'autre part le taux d'erreur de transmission sur les réseaux sans fils augmente généralement avec des paquets de taille importante, c'est la raison pour laquelle la norme 802.11 offre un mécanisme de fragmentation, permettant de découper une trame en plusieurs morceaux (fragments).

Format des trames

Le standard 802.11 définit le format des trames échangées. Chaque trame est constituée d'un en-tête (appelé *MAC header*, d'une longueur de 30 octets), d'un corps et d'un *FCS* (*Frame Sequence Check*) permettant la correction d'erreur.

FC (2)	D/ID (2)	Adresse (4 octets)	1	Adresse (4 octets)	2	Adresse (4 octets)	3	SC (2)	Adresse (4 octets)	4
Corps (0 à 2312 octets)										
FCS (2)										

Voici la description de ces champs :

- **FC** (*Frame Control*, en français *contrôle de trame*) : ce champ de deux octets est constitué des informations suivantes :

Version de protocole (2 bits)		Type (2 bits)				Sous-Type (4 bits)						
To (1 bit)	DS (1 bit)	From (1 bit)	DS (1 bit)	More (1 bit)	Frag	Retry (1 bit)	Power (1 bit)	Mgt	More (1 bit)	Data	WEP (1 bit)	Order (1 bit)

- **Versión de protocole** : ce champs de 2 bits permettra de prendre en compte les évolutions de version du standard 802.11. La valeur est égale à zéro pour la première version
- **Type** et **Sous-type** : ces champs, respectivement de 2 et 4 bits, définissent le type et le sous-type des trames explicités dans le tableau ci-dessous. Le type *gestion* correspond aux demandes d'association ainsi qu'aux messages d'annonce du point d'accès. Le type *contrôle* est utilisé pour l'accès au média afin de demander des autorisations pour émettre. Enfin le type *données* concerne les envois de données (la plus grande partie du trafic).
- **To DS** : ce bit vaut 1 lorsque la trame est destinée au système de distribution (*DS*), il vaut zéro dans les autres cas. Toute trame envoyée par une station à destination d'un point d'accès possède ainsi un champ *To DS* positionné à 1.
- **From DS** : ce bit vaut 1 lorsque la trame provient du système de distribution (*DS*), il vaut zéro dans les autres cas. Ainsi, lorsque les deux champs *To* et *From* sont positionnés à zéro il s'agit d'une communication directe entre deux stations (mode *ad hoc*).
- **More Fragments** (*fragments supplémentaires*) : permet d'indiquer (lorsqu'il vaut 1) qu'il reste des fragments à transmettre
- **Retry** : ce bit spécifie que le fragment en cours est une retransmission d'un fragment précédemment envoyé (et sûrement perdu)
- **Power Management** (*gestion d'énergie*) : indique, lorsqu'il est à 1, que la station ayant envoyé ce fragment entre en mode de gestion d'énergie
- **More Data** (*gestion d'énergie*) : ce bit, utilisé pour le mode de gestion d'énergie, est utilisé par le point d'accès pour spécifier à une station que des trames supplémentaires sont stockées en attente.
- **WEP** : ce bit indique que l'algorithme de chiffrement WEP a été utilisé pour chiffrer le corps de la trame.
- **Order** (*ordre*) : indique que la trame a été envoyée en utilisant la classe de service strictement ordonnée (*Strictly-Ordered service class*)
- **Durée / ID** : Ce champ indique la durée d'utilisation du canal de transmission.
- **Champs adresses** : une trame peut contenir jusqu'à 3 adresses en plus de l'adresse de 48 bits
- **Contrôle de séquence** : ce champ permet de distinguer les divers fragments d'une même trame. Il est composé de deux sous-champs permettant de réordonner les fragments :
 - Le *numéro de fragment*
 - Le *numéro de séquence*
- **CRC** : une somme de contrôle servant à vérifier l'intégrité de la trame.

Le tableau ci-dessous récapitule les types et sous-type de trame encapsulés dans le champ de contrôle de trame de l'en-tête MAC :

Type	Description du type	Sous-type	Description du sous-type
------	---------------------	-----------	--------------------------

00	Management (gestion)	0000	Association request (requête d'association)
00	Management (gestion)	0001	Association response (réponse d'association)
00	Management (gestion)	0010	Reassociation request (requête ré-association)
00	Management (gestion)	0011	Reassociation response (réponse de ré-association)
00	Management (gestion)	0100	Probe request (requête d'enquête)
00	Management (gestion)	0101	Probe response (réponse d'enquête)
00	Management (gestion)	0110-0111	Reserved (réservé)
00	Management (gestion)	1000	Beacon (balise)
00	Management (gestion)	1001	Annoucement traffic indication message (ATIM)
00	Management (gestion)	1010	Disassociation (désassociation)
00	Management (gestion)	1011	Authentication (authentification)
00	Management (gestion)	1100	Deauthentication (désauthentification)
00	Management (gestion)	1101-1111	Reserved (réservé)
01	Control (contrôle)	0000-1001	Reserved (réservé)
01	Control (contrôle)	1010	Power Save (PS)-Poll (économie d'énergie)
01	Control (contrôle)	1011	Request To Send (RTS)
01	Control (contrôle)	1100	Clear To Send (CTS)
01	Control (contrôle)	1101	ACK
01	Control (contrôle)	1110	Contention Free (CF)-end
01	Control (contrôle)	1111	CF-end + CF-ACK
10	Data (données)	0000	Data (données)
10	Data (données)	0001	Data (données) + CF-Ack
10	Data (données)	0010	Data (données) + CF-Poll
10	Data (données)	0011	Data (données) + CF-Ack+CF-Poll
10	Data (données)	0100	Null function (no Data (données))
10	Data (données)	0101	CF-Ack
10	Data (données)	0110	CF-Poll
10	Data (données)	0111	CF-Ack + CF-Poll
10	Data (données)	1000-1111	Reserved (réservé)
11	Data (données)	0000-1111	Reserved (réservé)

Point Coordination Function (PCF)

La Point Coordination Function (PCF) appelée mode d'accès contrôlé. Elle est fondée sur l'interrogation à tour de rôle des stations, ou polling, contrôlée par le point d'accès. Une station ne peut émettre que si elle est autorisée et elle ne peut recevoir que si elle est sélectionnée. Cette méthode est conçue pour les applications temps réel (vidéo, voix) nécessitant une gestion du délai lors des transmissions de données.

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.

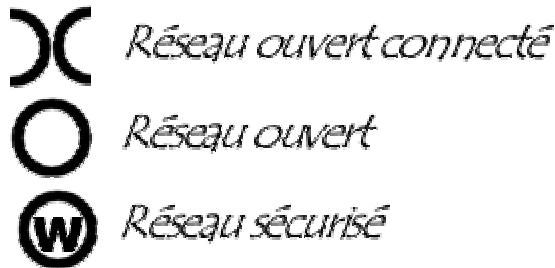
Là où le bât blesse c'est qu'un réseau sans fil peut très bien être installé dans une entreprise sans que le service informatique ne soit au courant ! Il suffit en effet à un employé de brancher un point d'accès sur une prise réseau pour que toutes les communications du réseau soient rendues "publiques"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

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 désassociation 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.

Éviter 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* 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 résoud pas le problème de la confidentialité des échanges.

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 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 partagé par toutes les stations est statique, c'est-à-dire que pour déployer un grand nombre de stations WiFi il est nécessaire de les configurer en utilisant la même clé de session. 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 traffic 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 oeuvre une protection *WEP* 128 bits afin d'assurer un niveau de confidentialité minimum et d'éviter de cette façon 90% des risques d'intrusion.

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).